УДК: 004.42

Арчаков Хасан Багаудинович
студент 4-го курса ИнгГУ,
г. Магас, РФ
Газдиев Ибрагим Муратович
студент 4-го курса ИнгГУ,
г. Магас, РФ
Кодзоев Умар Исмаилович
студент 4-го курса ИнгГУ,
г. Магас, РФ
Мациев Абуязит Ибрагимович
студент 4-го курса ИнгГУ,
г. Магас, РФ
Погоров Адам Муссаевич
студент 4-го курса ИнгГУ,
г. Магас, РФ

ЭЛЕКТРОННЫЙ УЧЁТ ЭЛЕКТРОННО-ЦИФРОВЫХ ПОДПИСЕЙ

АННОТАЦИЯ

В настоящей научно-исследовательской работе рассматривается проблема автоматизации учёта электронно-цифровых подписей (ЭЦП) в корпоративных информационных системах. Актуальность исследования обусловлена стремительным ростом числа субъектов электронного документооборота, обязательностью применения квалифицированной ЭЦП согласно Федеральному закону № 63-ФЗ «Об электронной подписи», а также высокими рисками, связанными с просроченными или ненадлежащим образом учтёнными сертификатами.

В ходе работы разработано прикладное программное средство «ECP Manager» — десктопное приложение на языке Python с использованием

фреймворка PyQt6. Средство реализует автоматическое сканирование сертификатов ЭЦП в форматах PFX, CER, PEM, DER и PKCS#7, шифрование хранилища данных на основе AES-256 (PBKDF2/SHA-256), систему уведомлений об истечении сроков действия подписей, а также экспорт данных в форматах CSV и Excel.

Ключевые слова

Электронно-цифровая подпись, ЭЦП, учёт сертификатов, автоматизация, информационная безопасность, PKCS#12, X.509, ГОСТ, КриптоПро, AES-256, PBKDF2.

Archakov Kh.B.
4th year student of IngSU,
Magas, Russian Federation
Gazdiev I.M.
4th year student of IngSU,
Magas, Russian Federation
Kodzoev U.I.
4th year student of IngSU,
Magas, Russian Federation
Matsiev A.I.
4th year student of IngSU,
Magas, Russian Federation
Pogorov A.M.
4th year student of IngSU,
Magas, Russian Federation
Scientific adviser: Fargieva Z. S.
Candidate of Pedagogical Sciences, Senior Lecturer
Magas, Russian Federation

ELECTRONIC ACCOUNTING OF ELECTRONIC DIGITAL SIGNATURES

ABSTRACT

This research paper examines the problem of automating the accounting of electronic digital signatures (EDS) in corporate information systems. The relevance of the research is due to the rapid growth of the number of electronic document management entities, the mandatory use of qualified EDS in accordance with Federal Law No. 63-FZ "On Electronic Signatures", as well as the high risks associated with expired or improperly accounted certificates.

During the research, the ECP Manager application software was developed, which is a desktop application written in Python using the PyQt6 framework. The tool implements automatic scanning of digital signature certificates in PFX, CER, PEM, DER, and PKCS#7 formats, AES-256 (PBKDF2/SHA-256) data storage encryption, a system for notifying about expired signatures, and data export in CSV and Excel formats.

Keywords

Digital signature, digital signature, certificate accounting, automation, information security, PKCS#12, X.509, GOST, KryptoPro, AES-256, PBKDF2.

Электронно-цифровая подпись является одним из ключевых инструментов обеспечения юридической значимости электронного документооборота. В условиях масштабной цифровизации государственного управления и корпоративных процессов количество сертификатов ЭЦП неуклонно возрастает. Типичное среднее предприятие оперирует несколькими десятками сертификатов, а крупные организации — сотнями и тысячами, принадлежащих различным сотрудникам, подразделениям и информационным системам.

Использование просроченных сертификатов влечёт широкий спектр негативных последствий: от отказа в приёме электронных документов государственными информационными системами до серьёзных правовых рисков и финансовых потерь. Ручной контроль сроков действия сертификатов неэффективен, трудозатратен и подвержен ошибкам человеческого фактора. Это

обусловливает необходимость создания специализированных автоматизированных средств учёта ЭЦП.

Целью данной работы является разработка программного средства для автоматизированного учёта электронно-цифровых подписей, обеспечивающего централизованное хранение, систематический мониторинг и своевременное оповещение об изменении статуса сертификатов. Практическая значимость состоит в создании готового к внедрению продукта, снижающего трудозатраты и повышающего уровень информационной безопасности организации.

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И АНАЛИЗ ПРОБЛЕМАТИКИ

Основу правового регулирования составляет Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», устанавливающий три вида электронной подписи: простую, усиленную неквалифицированную и усиленную квалифицированную. Квалифицированная электронная подпись (КЭП) признаётся равнозначной собственноручной подписи. Срок действия сертификата КЭП составляет, как правило, 15 месяцев, по истечении которых юридическая сила подписанных документов утрачивается.

Разработанное средство поддерживает все актуальные форматы сертификатов: PFX/PKCS#12 (хранение вместе с закрытым ключом), CER/X.509 (открытая часть), PEM (текстовый Base64-формат), DER (бинарный ASN.1) и PKCS#7 (цепочка сертификатов). Особое место занимают сертификаты на алгоритмах ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, автоматически идентифицируемые по OID-префиксу «1.2.643».

Анализ практики управления сертификатами выявляет три системные проблемы: децентрализованное хранение (сертификаты размещены в CertMgr, КриптоПро CSP, файловой системе и съёмных носителях без единого реестра); недостаточный контроль сроков (до 30% инцидентов с отказом в обработке электронных документов обусловлено просрочкой сертификатов); угрозы информационной безопасности хранилища учётных данных.

Существующие решения (Microsoft AD CS, Venafi, DigiCert CertCentral) ориентированы на крупный бизнес, не адаптированы к российской нормативной базе и не поддерживают алгоритмы ГОСТ. Электронные таблицы (Excel) не обеспечивают автоматического сканирования, уведомлений и надёжной защиты данных. Это обосновывает необходимость разработки специализированного средства «ECP Manager».

2. АРХИТЕКТУРА И РЕАЛИЗАЦИЯ «ECP MANAGER»

«ECP Manager» реализован как десктопное приложение на Python 3.x с использованием фреймворка PyQt6. Архитектура построена по принципу разделения ответственности и включает четыре логических модуля: криптографической защиты данных, сканирования и распознавания сертификатов, контроля сроков и уведомлений, экспорта данных. Хранилище данных располагается в папке %APPDATA%\ECP_Manager (Windows) или ~/.local/share/ECP_Manager (Linux/macOS).

Для защиты хранилища применяется симметричное шифрование AES-256 в режиме CBC. Ключ шифрования вычисляется при каждой аутентификации из пароля администратора посредством PBKDF2-SHA256 (100 000 итераций, случайная соль 128 бит). Структура зашифрованного файла: первые 16 байт — соль, следующие 16 байт — вектор инициализации (IV), далее — зашифрованные данные с PKCS#7-дополнением. При каждом сохранении генерируются новые соль и IV, что обеспечивает семантическую безопасность. Хэш пароля администратора хранится в bcrypt с автоматически генерируемой солью.

Модуль реализует многоуровневую стратегию обнаружения. Первый уровень — сканирование файловой системы: поддерживаются расширения .cer, .crt, .pem, .der, .pfx, .p12, .p7s, .p7b с каскадной стратегией распознавания формата. Второй уровень — интеграция с КриптоПро CSP через последовательные вызовы certmgr.exe, certutil и PowerShell Get-ChildItem. Дедупликация реализована через проверку уникальности SHA-1 отпечатка.

При каждом запуске приложения выполняется check_expiry_alerts(): формируются списки просроченных сертификатов и сертификатов с истекающим в течение 30 дней сроком. При наличии проблемных записей отображается модальное диалоговое окно. Порог 30 дней достаточен для прохождения процедуры получения нового сертификата в УЦ. Экспорт реализован в форматах CSV (кодировка UTF-8, разделитель-запятая) и Excel (.xlsx с форматированным заголовком через openpyxl).

3. ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС

Приложение открывается диалогом аутентификации (AuthDialog), в котором пользователь вводит пароль администратора СКЗИ для входа в существующую базу данных. Кнопка «Первый запуск» инициализирует новую зашифрованную базу данных при первоначальном развёртывании системы.

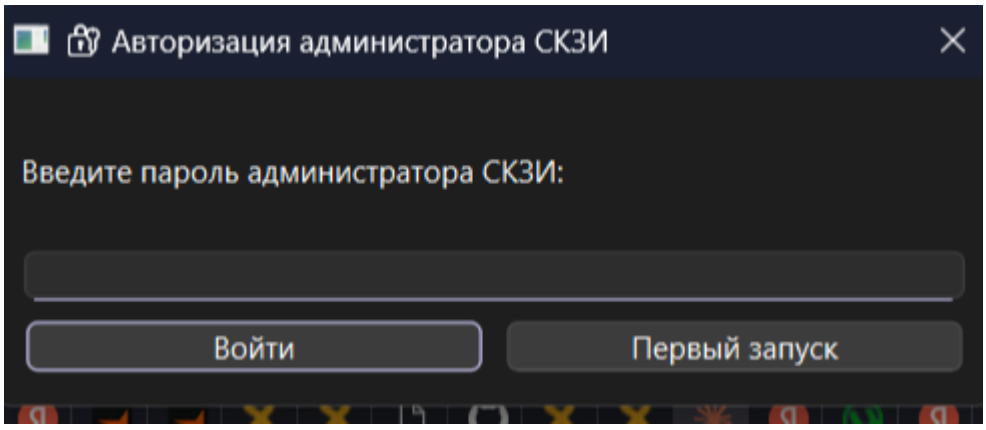

Рисунок 1 — Диалог авторизации администратора СКЗИ

После успешной аутентификации открывается главное окно «Учёт ЭЦП (автоматический сбор)» размером 1000×600 пикселей. Панель инструментов содержит кнопки: «Сканировать ЭЦП (КриптоПро)», «Загрузить файлы ЭЦП», «Экспорт в Excel», «Обновить». Таблица данных отображает восемь атрибутов: Владелец, Организация, Отпечаток, Действует до, ГОСТ?, Источник, Статус,

Добавлено. Записи с истёкшим сроком выделяются красным цветом, с истекающим в течение 30 дней — жёлтым.

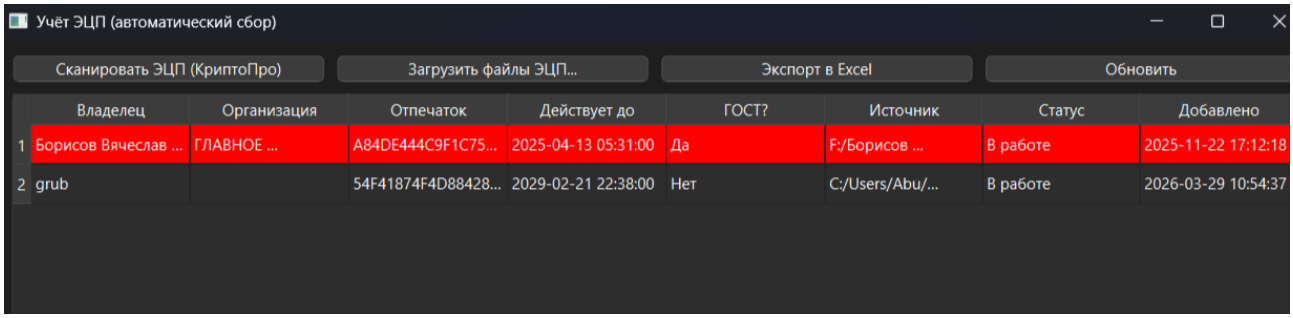

Рисунок 2 — Главное окно программы «ECP Manager»: цветовая индикация статуса сертификатов

4. ТЕСТИРОВАНИЕ, ЭФФЕКТИВНОСТЬ И ПЕРСПЕКТИВЫ

Функциональное тестирование подтвердило корректное распознавание сертификатов всех поддерживаемых форматов. Механизм дедупликации по SHA-1 отпечатку исключил дублирование записей при повторном сканировании. Цветовая индикация корректно отражает статус: истёкшие — красный, истекающие — жёлтый. Тестирование интеграции с КриптоПро CSP версий 4.0 и 5.0 провалилось.

Оценка защищённости показала высокую стойкость ключа: PBKDF2-SHA256 с 100 000 итерациями позволяет перебирать ~200–500 паролей в секунду. При пароле из 8 символов пространства ASCII гарантированный взлом потребует порядка 13 000 лет. Уникальность случайных соли и IV при каждом сохранении исключает атаки на основе повторного использования ключевого материала.

Сравнительное исследование трудозатрат показало: сокращение времени на ведение реестра ЭЦП — 70% по сравнению с ручным методом; скорость добавления сертификата — с нескольких минут (ручной ввод) до нескольких секунд (автосканирование). В компании с 50 сотрудниками ежемесячный аудит

сократился с 4–6 часов до 15–20 минут. Автоматические уведомления при запуске полностью исключают риск пропуска сроков.

Определены следующие направления развития продукта: мобильные приложения для iOS и Android с push-уведомлениями (Погоров А.М., Кодзоев У.И.); централизованный серверный API на FastAPI с RBAC и корпоративными уведомлениями (Газдиев И.М.); интеграция с ЕПГУ, 1С и LDAP/Active Directory; расширение криптографической поддержки до полного спектра ГОСТ-алгоритмов (Мациев А.И.); веб-интерфейс на React.js (Арчаков Х.Б.).

ЗАКЛЮЧЕНИЕ

В ходе настоящей работы разработано программное средство «ECP Manager» для автоматизации учёта электронно-цифровых подписей. Реализована надёжная криптографическая защита хранилища на основе AES-256-CBC с деривацией ключа по PBKDF2-SHA256 (100 000 итераций). Модуль сканирования поддерживает все актуальные форматы сертификатов и интегрируется со штатными инструментами КриптоПро CSP, certutil и PowerShell.

Практическая эффективность подтверждена: сокращение трудозатрат составляет порядка 70%, а автоматические уведомления при запуске исключают риск использования просроченных ЭЦП. Разработанное средство готово к практическому применению в организациях любого масштаба, использующих электронный документооборот с применением ЭЦП. Открытость кодовой базы (Python) обеспечивает возможность адаптации продукта под специфические требования конкретной организации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства РФ. — 2011. — № 15. — Ст. 2036.

2. ГОСТ Р 34.10-2012. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Стандартинформ, 2013. — 24 с.

3. ГОСТ Р 34.11-2012. Функция хэширования (Стрибог). — М.: Стандартинформ, 2013. — 20 с.

4. RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and CRL Profile / D. Cooper et al. — IETF, 2008. — 151 p.

5. RFC 7292 — PKCS #12: Personal Information Exchange Syntax v1.1. — IETF, 2014. — 44 p.

6. NIST SP 800-132. Recommendation for Password-Based Key Derivation. — NIST, 2010. — 26 p.

7. Горбатов В.С., Полянская О.Ю. Инфраструктура открытых ключей. — М.: ИНТУИТ, 2007. — 280 с.

8. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. — СПб.: БХВ-Петербург, 2005. — 288 с.

9. Python cryptography library documentation. — URL: https://cryptography.io/en/latest/

10. PyQt6 Reference Guide. — URL: https://doc.qt.io/qtforpython-6/

11. Руководство администратора КриптоПро CSP 5.0. — М.: КРИПТО-ПРО, 2024. — 145 с.

12. Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи».