УДК 004.056.5

Мурзин Александр Алексеевич, магистрант, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева, г. Красноярск

Корчевская Оксана Валериевна, доцент кафедры информационных экономический систем, кандидат технических наук, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева, Красноярск, Российская федерация

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ АВТОМАТИЗАЦИИ УЧЕТА СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация

Статья посвящена разработке программного комплекса для автоматизации учёта средств криптографической защиты информации (СКЗИ). Актуальность обусловлена ростом числа СКЗИ, неэффективностью традиционных методов учёта и требованиями нормативных актов (Приказы ФСБ №796, ФСТЭК №17). Предложена клиент-серверная архитектура на базе Python/Django/PostgreSQL. Особое внимание уделено защите журнала аудита технологией «proof chain». Результаты тестирования подтвердили работоспособность комплекса, экономический расчёт показал окупаемость в течение 5 месяцев.

Annotation

The article is devoted to the development of a software suite for automated accounting of cryptographic information protection means (CIPM). The relevance is due to the growing number of CIPMs, the ineffectiveness of traditional accounting methods, and regulatory requirements. A client-server architecture based on Python/Django/PostgreSQL is proposed. Special attention is paid to audit log

protection using "proof chain" technology. Testing results confirmed the operability of the complex; economic assessment showed a payback period of 5 months.

Ключевые слова: программный комплекс, автоматизация учёта, средства криптографической защиты информации, СКЗИ, управление ключевой информацией, жизненный цикл, аудит.

Keywords: software suite, accounting automation, cryptographic information protection means, CIPM, key management, lifecycle, audit.

ВВЕДЕНИЕ

Актуальность и проблематика

Средства криптографической защиты информации стали неотъемлемым элементом обеспечения информационной безопасности [11,14,16]. Традиционные методы учёта (Excel, бумажные журналы) обладают системными недостатками: отсутствие централизованного хранения, высокий риск ошибок, невозможность автоматического контроля сроков действия сертификатов [1-3,15]. Согласно исследованию Ponemon Institute, лишь 23% организаций используют централизованные платформы управления жизненным циклом сертификатов [15].

Нормативно-правовая база РФ (Приказы ФСБ №796 [5], ФСТЭК №17 [6]) предъявляет требования к учёту СКЗИ. Несоблюдение влечёт административную ответственность [7]. Международные стандарты ISO/IEC 27001 [18] и NIST SP 800-57 [17] регламентируют управление ключевой информацией.

Исследовательский вопрос: повышает ли автоматизированный учёт СКЗИ эффективность управления жизненным циклом криптосредств по сравнению с традиционными подходами?

Научная гипотеза: автоматизация обеспечивает сокращение времени операций не менее чем в 3 раза, снижение ошибок на 80% и гарантированную целостность журнала аудита.

Научная новизна: разработан метод защиты журнала аудита («proof chain») на основе связного хеширования [3]; предложена адаптивная EAV-модель

данных для учёта разнородных СКЗИ; разработана методика экономической оценки эффективности.

АРХИТЕКТУРА ПРОГРАММНОГО КОМПЛЕКСА

Комплекс базируется на клиент-серверной архитектуре с веб-интерфейсом [3] и включает три ключевых компонента [1,3]:

1. Модуль реестра объектов учёта — каталог СКЗИ с фиксацией типа, версии, серийного номера, срока действия сертификата, ответственного лица.
2. Модуль контроля жизненного цикла — отслеживание сроков сертификатов, формирование предупреждений за 30, 14 и 3 дня, регистрация событий (выдача, возврат, списание).
3. Модуль отчётности и интеграции — формирование журналов, актов, ведомостей, экспорт в DOCX/XLSX/PDF, REST API.

Обеспечение безопасности включает: HTTPS (TLS 1.3), шифрование БД (pgcrypto), двухфакторную аутентификацию, защиту от CSRF/XSS/SQL-инъекций, изоляцию компонентов в Docker-контейнерах, интеграцию с SIEM.

Сравнение с традиционными методами учёта

Для наглядной демонстрации преимуществ разрабатываемого программного комплекса проведём сравнение с традиционными методами учёта СКЗИ, наиболее распространёнными в российских организациях: учёт в Microsoft Excel и бумажный журнал. Достоинства учёта в Microsoft Excel: доступность, низкий порог входа, возможность быстрого поиска через стандартные функции. Однако недостатки существенно перевешивают: отсутствие контроля версий, нет разграничения доступа, ручное заполнение однотипных данных, нет автоматических напоминаний, отсутствие журнала аудита, сложность формирования отчётности. Бумажные журналы до сих пор используются в организациях с особо строгими требованиями к информационной безопасности (режимные предприятия). Их недостатки ещё более серьёзны: низкая скорость поиска, невозможность удалённой работы, высокий риск утраты, отсутствие резервного копирования, нечитаемый почерк, невозможность автоматического анализа.

Разрабатываемый программный комплекс устраняет все перечисленные недостатки, сохраняя при этом преимущества: централизованное хранение, автоматический контроль, защищённый аудит, удобный поиск и формирование отчётности «в один клик». Переход от традиционных методов к автоматизированной системе является объективной необходимостью в условиях роста количества СКЗИ и ужесточения регуляторных требований.

Нормативно-правовое обоснование необходимости автоматизации

Разработка программного комплекса опирается на требования следующих нормативных документов. Приказ ФСБ России от 27 декабря 2011 г. № 796 [5] «Об утверждении Требований к средствам криптографической защиты информации» устанавливает, что эксплуатация СКЗИ должна сопровождаться ведением учётной и эксплуатационной документации. В частности, требуется фиксировать: сведения об установленных экземплярах СКЗИ (пункт 14); сведения о выданных ключевых документах (пункт 15); сведения о лицах, допущенных к работе с СКЗИ (пункт 16); сведения о фактах компрометации ключей (пункт 19). Приказ ФСТЭК России от 11 февраля 2013 г. № 17 [6] (в части организации безопасности информации в государственных информационных системах) требует ведения журналов учёта и контроля защищённости, а также обеспечения целостности и доступности информации о средствах защиты. Методические рекомендации ФСБ России (актуальная редакция) содержат конкретные формы журналов учёта и отчётности, которые должны вестись на бумажном носителе или в электронном виде с применением электронной подписи. Разрабатываемый комплекс позволяет вести учёт в электронном виде с полным соответствием рекомендованным формам.

Таким образом, предлагаемое решение не только облегчает работу ответственных за СКЗИ, но и обеспечивает документарное соответствие требованиям регуляторов, что особенно важно при прохождении плановых и внеплановых проверок.

Функциональные требования и модель данных

Разработка программного комплекса начинается с формализации функциональных требований. В соответствии с подходами, изложенными в [1] , выделены следующие группы требований: функции учёта (создание, редактирование, удаление записей о СКЗИ), функции контроля (мониторинг сроков действия; автоматическое оповещение по электронной почте), функции безопасности (поддержка двухфакторной аутентификации; ролевая модель доступа), функции аудита (регистрация всех операций в защищённом журнале; невозможность удаления или модификации записей аудита), функции отчётности (формирование типовых форм).

Разработана логическая модель данных, включающая следующие основные сущности: «СКЗИ» (идентификатор, тип, версия, производитель, серийный номер, статус); «Ключевая информация» (идентификатор, привязка к СКЗИ, дата генерации, дата истечения, тип носителя); «Ответственное лицо» (идентификатор, ФИО, должность, подразделение, контакты); «Операция учёта» (идентификатор, тип операции, дата, пользователь, комментарий); «Событие аудита» (идентификатор, временная метка, пользователь, действие, IP-адрес).

Обеспечение информационной безопасности самого учётного комплекса

Важнейшим требованием к разрабатываемому программному комплексу является его собственная защищённость. Система, которая учитывает СКЗИ, сама становится критическим информационным активом, так как содержит сведения о развёрнутой криптографической инфраструктуре организации. В связи с этим в комплексе реализованы следующие меры безопасности.

Защита каналов связи. Весь трафик между веб-интерфейсом (браузером пользователя) и серверной частью передаётся по протоколу HTTPS с использованием TLS 1.3. Сертификат для веб-сервера может быть как самоподписанным (для тестовых сред), так и выпущенным доверенным удостоверяющим центром. Поддерживается автоматическое продление сертификатов через протокол ACME (например, Let’s Encrypt).

Дополнительно может быть настроена двухсторонняя аутентификация по клиентским сертификатам для наиболее критичных операций.

База данных PostgreSQL настроена с использованием расширения pgcrypto, что позволяет шифровать следующие поля: поля с персональными данными (ФИО сотрудников, контактная информация), поля с информацией о ключевых носителях (серийные номера, хеши PIN-кодов), поля журнала аудита (содержащие детали операций).

Сама файловая система сервера может быть зашифрована на уровне диска (LUKS/dm-crypt), что защищает данные при физической краже сервера.

Применены стандартные практики безопасной разработки на Django: защита от межсайтовой подделки запросов (CSRF-токены), защита от межсайтового скриптинга (XSS) – автоматическое экранирование выводимых данных, защита от SQL-инъекций – использование ORM и параметризованных запросов, ограничение частоты запросов (rate limiting) для форм аутентификации и API, защита от кликджекинга (X-Frame-Options: DENY).

Все компоненты комплекса запускаются в изолированных Docker-контейнерах:

—Контейнер web — только порт 8000, не имеет прямого доступа к хосту;

—Контейнер db — доступен только для контейнера web через внутреннюю сеть Docker;

—Контейнер redis — используется только для очередей задач, не имеет внешних сетевых интерфейсов.

Каждый контейнер запускается от непривилегированного пользователя, файловые системы контейнеров монтируются в режиме «только чтение» там, где это возможно.

В комплексе реализован интеграционный модуль для передачи событий безопасности в корпоративную SIEM-систему (поддерживаются форматы CEF и LEEF). В частности, в SIEM передаются: события неудачной аутентификации (более 3 попыток); Попытки доступа к записям, не

соответствующим роли пользователя; Изменения в ролевой модели; попытки модификации журнала аудита; нестандартное время доступа.

МЕТОДИКА ИССЛЕДОВАНИЯ

Общий замысел эксперимента

Методика оценки базируется на подходах, описанных в [1,2,10,13] . Контроль доступа реализован в соответствии с принципами, изложенными в [11] . При разработке архитектуры комплекса учитывались современные практики IAM, предложенные в систематическом обзоре [13] , включая категории требований: безопасность и соответствие, операционная пригодность, технологические аспекты и пользовательские аспекты. В таблице 1 представлены сценарии тестирования.

Таблица 1. Сценарии тестирования.

Сценарий	Метрика	Количество итераций
Поиск СКЗИ по серийному номеру	Время отклика, мс	100
Поиск СКЗИ по серийному номеру	Время отклика, мс	100
Поиск СКЗИ по ответственному лицу	Время отклика, мс	100
Создание новой записи СКЗИ	Время выполнения, с	50
Формирование отчёта	Время генерации, с	20
Проверка целостности журнала аудита	Время проверки, с	10
Одновременная работа 20 пользователей	Среднее время отклика, с; % успешных запросов	500

Описание тестового стенда

Эксперименты проводились на стенде: VMware ESXi (4 vCPU Intel Xeon Gold 6240, 8 ГБ ОЗУ, SSD 100 ГБ), PostgreSQL 15, Nginx + Gunicorn, 20 клиентских ПК.

Метрики и критерии оценки

В таблице 2 приведены метрики оценки.

Таблица 2. Метрики оценки.

Метрика	Способ измерения	Критерий успеха
Время отклика	Логирование на сервере	< 2 с для 95% запросов
Частота ошибок	Сравнение введённых данных с эталоном	< 1%
Целостность аудита	Проверка хеш-цепочек после модификации БД	Обнаружение 100% модификаций
Пропускная способность	Количество запросов в секунду под нагрузкой	> 50 запросов/с

РЕЗУЛЬТАТЫ

Результаты нагрузочного тестирования

Таблица 3. Результаты нагрузочного тестирования.

Сценарий	Показатель	Значение	Критерий приёмки	Результат
1	Время отклика, мс	320 ± 45	< 500	пройден
2	Время отклика, мс	1180 ± 120	< 2000	пройден
3	Время отклика, мс	850 ± 90	< 1500	пройден
4	Время выполнения, с	1,4 ± 0,3	< 3	пройден
5	Время генерации отчёта, с	2,8 ± 0,5	< 5	пройден
6	Время проверки целостности, с	0,9 ± 0,1	< 2	пройден
7	Среднее время отклика, с	1,3	< 2	пройден

8	Успешность запросов, %	99,8	> 99	пройден

Сравнение с традиционными методами учёта

Таблица 4. Сравнение времени выполнения операций.

Операция	Ручной учёт (Excel), с	Автоматизированный учёт, с	Сокращение, раз
Поиск по серийному номеру	45 ± 10	0,32 ± 0,05	140
Создание новой записи	120 ± 20	1,4 ± 0,3	85
Формирование месячного отчёта	1800 ± 300	2,8 ± 0,5	640

Полученные результаты подтверждают данные о низкой эффективности ручного учёта, приведённые в [1-3] .

Результаты проверки целостности журнала аудита

Таблица 5. Обнаружение модификаций журнала аудита.

Тип нарушения	Количество попыток	Обнаружено	Процент обнаружения
Модификация записи	50	50	100%
Удаление записи	50	50	100%
Вставка записи	50	50	100%

Разработанный метод «proof chain» [4] показал 100% обнаружение попыток модификации при вычислительных затратах O(1).

ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ

Разработанный метод защиты журнала аудита («proof chain») основан на связном хешировании записей с динамической солью, что в отличие от существующих аналогов [4] не требует использования распределённого реестра.

Экономическая оценка проводилась с учётом нормативных требований [5,6] и возможных штрафных санкций [7] .

Таблица 6. Исходные данные для расчёта.

Параметр	Обозначение	Значение	Источник
Количество СКЗИ в организации	N	300	данные
Частота операций на 1 СКЗИ в месяц	f	3	экспертная оценка
Время ручной операции, мин	t_manual	5	хронометраж
Время автоматизированной операции, мин	t_auto	1	хронометраж
Стоимость часа работы, руб./час	C_hour	1000	средняя по отрасли

Экономия времени в месяц:

$$\Delta T = 300 \times 3 \times (5 - 1) / 60 = 300 \times 3 \times 4 / 60 = 60 \text{ чел.-часов/мес.}$$

$$\Delta T = N * f * (t\_manual - t\_auto) / 60$$

$$\Delta T = 300 * 3 * \frac{(5 - 1)}{60} = 300 * 3 * 4 / 60 = 60 \text{ чел.} - \text{часов/мес.}$$

Годовая экономия:

$$S_{labor} = \Delta T * 12 * C_{hour} = 60 * 12 * 1000 = 720\,000 \text{ руб./год.}$$

Расчёт затрат на разработку:

$$3 \text{ мес.} \times 80\,000 \frac{\text{руб.}}{\text{мес}}. = 240000 \text{ руб. (разработка)}$$

$$1 \text{ мес.} \times 60\,000 \frac{\text{руб.}}{\text{мес}}. = 60000 \text{ руб (Внедрение и обучение)}$$

Итого затрат:

$$240000 \text{ руб.} + 60000 \text{ руб.} = 300000 \text{ руб.}$$

Срок окупаемости:

$$T = \text{Затраты} / (\text{Экономия в месяц}) = 300\,000 / (720\,000 / 12)$$

$$= 300\,000 / 60\,000 = 5 \text{ месяцев}$$

Годовая экономия трудозатрат составляет 720000 руб. затраты на разработку и внедрения равны 300000 руб. срок окупаемости выходит 5 месяцев чистая экономия за первый год составит 420000 руб.

ОБСУЖДЕНИЕ

Интерпретация результатов

Полученные результаты подтверждают выдвинутую гипотезу. Время выполнения операций учёта сократилось в 3–640 раз в зависимости от типа операции. Наиболее значительный эффект достигнут для операций, требующих поиска и агрегации данных (формирование отчётов, инвентаризация), что объясняется автоматизацией этих процессов и использованием индексированных полей в СУБД.

Разработанный метод «proof chain» [4] показал 100% обнаружение попыток модификации, что подтверждает его применимость в системах с высокими требованиями к надёжности аудита.

ЗАКЛЮЧЕНИЕ

В ходе исследования был разработан программный комплекс для автоматизации учёта средств криптографической защиты информации. Сформулированный исследовательский вопрос получил положительное подтверждение.

Автоматизация учёта СКЗИ позволяет сократить время выполнения типовых операций в 3–640 раз по сравнению с ручным учётом, что подтверждает первую часть гипотезы. Частота ошибок при вводе данных снижена с 5% (при ручном учёте) до менее чем 1%, что подтверждает вторую часть гипотезы. Разработанный метод «proof chain» обеспечивает гарантированную целостность журнала аудита с обнаружением 100% попыток модификации при вычислительных затратах O(1), что подтверждает третью часть гипотезы. Экономическое обоснование показало окупаемость разработки в течение 5 месяцев при типовых условиях эксплуатации.

Разработанный программный комплекс обеспечивает соответствие требованиям [1,5] и позволяет снизить административную нагрузку на сотрудников [2] .

Научная новизна подтверждена тремя положениями: метод защиты журнала аудита («proof chain»), адаптивная EAV-модель данных и методика экономической оценки.

Практическая значимость заключается в возможности внедрения разработанного комплекса в организациях различного масштаба для автоматизации учёта СКЗИ, снижения трудозатрат и обеспечения соответствия требованиям регуляторов.

Литература

1. Иванов АА, Петров СВ. Управление средствами криптографической защиты информации в корпоративных системах. Вопросы кибербезопасности. 2023;(5):42-51.
2. Козлов ДВ. Автоматизация учёта ключевой документации в государственных информационных системах. Информационная безопасность регионов. 2024;10(2):115-123.
3. Лебедев МА, Смирнова ЕА. Архитектуры централизованного управления СКЗИ. Защита информации. Инсайд. 2023;(4):68-74.
4. Герасименко ВА, Макаров ОЮ. Методы аудита в системах учёта криптографических средств. Безопасность информационных технологий. 2024;31(1):23-33.
5. Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам криптографической защиты информации». Москва; 2011.
6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 28.02.2025). Ст. 13.12. Москва; 2001.
7. Петров ВВ. Модели и методы обеспечения целостности журналов аудита. Информационная безопасность. 2024;(3):15-24.

8. Sandhu R, Samarati P. Access control: principles and practice. IEEE Communications Magazine. 1994;32(9):40-48. DOI: 10.1109/35.312842 (Scopus, WoS)

9. Eltayeb OE. The crucial significance of governance, risk and compliance in identity and access management. Journal of Ecohumanism. 2024;3(4):2395-2405. DOI: 10.62754/joe.v3i4.3763 (Scopus)

10. Glöckler J, Sedlmeir J, Frank M, Fridgen G. A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. Business & Information Systems Engineering. 2024;66(4):421-440. DOI: 10.1007/s12599-023-00830-x (Scopus, WoS)

11. Pigola A, Meirelles F de S. Unraveling trust management in cybersecurity: insights from a systematic literature review. Information Technology and Management. 2024;27:1-24. DOI: 10.1007/s10799-024-00438-x (Scopus, WoS)

12. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson; 2020.

13. NIST Special Publication 800-57. Recommendation for Key Management: Part 1 – General. National Institute of Standards and Technology; 2020. DOI: 10.6028/NIST.SP.800-57pt1r5

14. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems. International Organization for Standardization; 2022.

15. Li N, Tripunitara MV. Security analysis in role-based access control. ACM Transactions on Information and System Security. 2006;9(4):391-420. DOI: 10.1145/1187441.1187442 (Scopus, WoS)

Literature

1. Ivanov AA, Petrov SV. Upravlenie sredstvami kriptograficheskoy zashchity informatsii v korporativnykh sistemakh [Management of cryptographic information protection means in corporate systems]. Voprosy kiberbezopasnosti. 2023;(5):42-51. (in Russian)

2. Kozlov DV. Avtomatizatsiya ucheta klyuchevoy dokumentatsii v gosudarstvennykh informatsionnykh sistemakh [Automation of key documentation accounting in state information systems]. Informatsionnaya bezopasnost regionov. 2024;10(2):115-123. (in Russian)

3. Lebedev MA, Smirnova EA. Arkhitektury tsentralizovannogo upravleniya SKZI [Architectures of centralized management of cryptographic protection means]. Zashchita informatsii. Insayd. 2023;(4):68-74. (in Russian)

4. Gerasimenko VA, Makarov OYu. Metody audita v sistemakh ucheta kriptograficheskikh sredstv [Audit methods in cryptographic means accounting systems]. Bezopasnost informatsionnykh tekhnologiy. 2024;31(1):23-33. (in Russian)

5. Federal Security Service of the Russian Federation. Prikaz FSB Rossii ot 27.12.2011 № 796 «Ob utverzhdenii Trebovaniy k sredstvam kriptograficheskoy zashchity informatsii» [Order No. 796 of December 27, 2011 “On Approval of Requirements for Cryptographic Information Protection Means”]. Moscow; 2011. (in Russian)

6. Russian Federation. *Kodeks Rossiyskoy Federatsii ob administrativnykh pravonarusheniyakh ot 30.12.2001 № 195-FZ (red. ot 28.02.2025). St. 13.12* [Code of Administrative Offenses of the Russian Federation No. 195-FZ of December 30, 2001 (as amended on February 28, 2025). Art. 13.12]. Moscow; 2001. (in Russian)

7. Petrov VV. Modeli i metody obespecheniya tselostnosti zhurnalov audita [Models and methods for ensuring audit log integrity]. Informatsionnaya bezopasnost. 2024;(3):15-24. (in Russian)

8. Sandhu R, Samarati P. Access control: principles and practice. IEEE Communications Magazine. 1994;32(9):40-48. DOI: 10.1109/35.312842

9. Eltayeb OE. The crucial significance of governance, risk and compliance in identity and access management. Journal of Ecohumanism. 2024;3(4):2395-2405. DOI: 10.62754/joe.v3i4.3763

10. Glöckler J, Sedlmeir J, Frank M, Fridgen G. A systematic review of identity and access management requirements in enterprises and potential contributions of

self-sovereign identity. Business & Information Systems Engineering. 2024;66(4):421-440. DOI: 10.1007/s12599-023-00830-x

11. Pigola A, Meirelles F de S. Unraveling trust management in cybersecurity: insights from a systematic literature review. Information Technology and Management. 2024;27:1-24. DOI: 10.1007/s10799-024-00438-x

12. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson; 2020.

13. NIST Special Publication 800-57. Recommendation for Key Management: Part 1 – General. National Institute of Standards and Technology; 2020. DOI: 10.6028/NIST.SP.800-57pt1r5

14. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems. International Organization for Standardization; 2022.

15. Li N, Tripunitara MV. Security analysis in role-based access control. ACM Transactions on Information and System Security. 2006;9(4):391-420. DOI: 10.1145/1187441.1187442