УДК 004.9

АРХИТЕКТУРА СИСТЕМЫ УЧЕТА ТЕХНИЧЕСКИХ СРЕДСТВ СВЯЗИ С РАСПРЕДЕЛЕННЫМ ДОСТУПОМ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТОЙ

А. Ю. Савицкий, кандидат военных наук;
А. В. Аскерко, кандидат военных наук, доцент;
Е. В. Лейбук*

В статье представлен авторский подход и построение архитектуры системы иерархического доступа, в которой реализована модель документооборота с отложенной регистрацией, пошаговая криптографическая верификация целостности и привязка документов к учетной карточке оборудования по комплексу «модель, серийный номер, год выпуска». Маршрут согласования включает четыре обязательных уровня, что исключает попадание незавершенных документов в реестр. Система выполнена в виде трехуровневого клиент-серверного приложения с ролевым разграничением доступа, обеспечивающим видимость данных строго в соответствии с должностными обязанностями.

The article proposes an architecture for a hierarchical access system, which implements a document workflow model with deferred registration, step-by-step cryptographic verification of integrity, and linking of documents to the equipment record card using the combination 'model, serial number, year of manufacture'. The approval route includes four mandatory levels, which prevents unfinished documents from entering the registry. The system is implemented as a three-tier client-server application with role-based access control, ensuring data visibility strictly in accordance with job responsibilities.

Введение

В условиях наблюдающегося значительного повышения интенсивности циркуляции материальных и информационных потоков учет материально-технических ресурсов, контроль за их расходованием предъявляют повышенные требования достоверности и оперативности к учетным процессам. Несмотря на развитие информационных технологий, в области учета наличия и движения технических средств связи, сохраняется значительная зависимость от традиционных методов бумажного документооборота, оформление актов приема, технического состояния, списания, изменения качественного состояния и замены комплектующих изделий по-прежнему требует физического перемещения бумажных носителей между подразделениями для сбора подписей и ручной регистрации. Приходно-расходные операции приводят к значительным временным затратам, рассинхронизации данных и задержкам в утверждении документов. Разработка системы, которая исключает необходимость личного участия при передаче актов на подпись и автоматически фиксирует утвержденные документы в едином реестре, позволяет существенно ускорить деятельность подразделений и повысить достоверность учета. Автоматизирована должна быть не только форма, но и сам процесс согласования документов при учете технических средств связи.

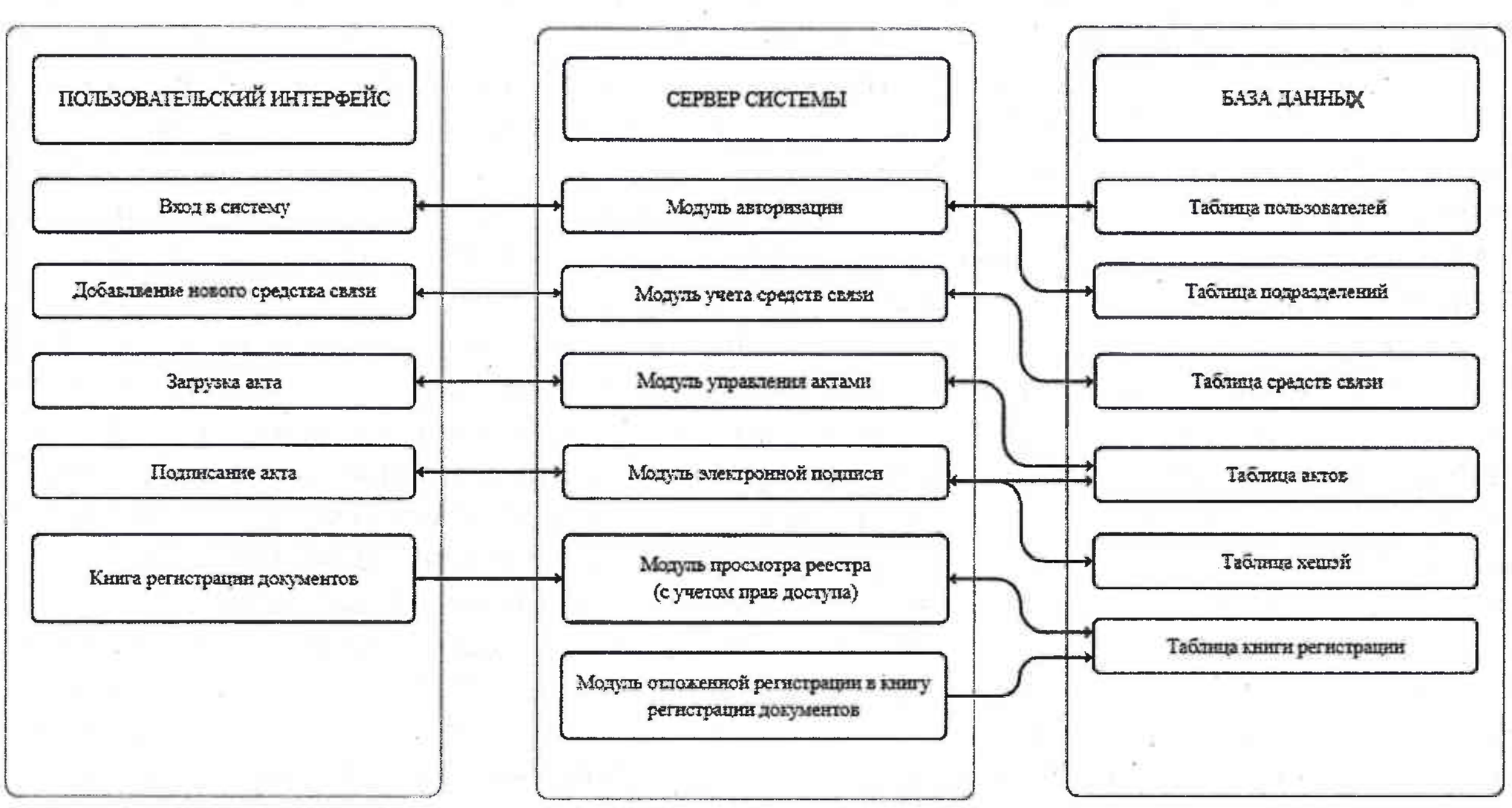
Проведенный анализ существующих систем учета оборудования и электронного документооборота (Odoo, «1С:Предприятие», Tunesoft, «Сова. ЕРКЦ») показал, что ни одна из них не реализует одновременно три ключевых механизма: иерархическое согласование документов по жесткой вертикали «комиссия → начальник отдела → начальник центра → командир», отложенную регистрацию актов в книге учета только после полного утверждения и сквозную криптографическую верификацию целостности на каждом этапе подписания. Таким образом, решаемая научная задача – разработка единой системы учета средств связи с распределенным доступом и криптографической защитой документов – соответствует современному уровню исследований в области автоматизации документооборота для организаций с иерархической структурой и не имеет прямых аналогов.

Основная часть

Архитектура системы. Общий подход к решению задачи заключается в разработке системы, объединяющей учет наличия и движения технических средств связи и электронный документооборот в едином цифровом контуре. Процесс инициируется пользователем путем привязки создаваемого документа к учетной карточке образца технических средств связи, идентифицируемого по уникальным характеристикам: модель, серийный номер и год выпуска. Процесс согласования реализуется через последовательное наложение электронных подписей, криптографические хеши которых хранятся в базе данных для обеспечения неизменности и верификации подлинности.

Ключевой особенностью подхода является принцип отложенной регистрации: запись в книгу учета производится автоматически только после прохождения всех уровней иерархического утверждения вплоть до командира воинской части (соединения). Разграничение прав доступа обеспечивает видимость данных строго в соответствии с должностными обязанностями. Такой подход позволяет интегрировать привычные форматы документов с высоким контролем доступа и отслеживать их статусы на всех этапах создания и утверждения единого документа, исключая промежуточные документы. Для технической реализации описанного подхода и обеспечения бесперебойного функционирования цифровой системы была спроектирована соответствующая многоуровневая архитектура системы. Она построена в соответствии с принципами организации распределенных программных систем на основе модели «клиент/сервер» [1].

Такая декомпозиция системы позволяет распределить функции между независимыми ее компонентами, где каждый уровень решает специфические задачи: клиентская часть отвечает за взаимодействие с пользователем, сервер приложений обеспечивает обработку запросов и реализацию логики, база данных гарантирует целостность и сохранность информации (рисунок 1).



В представленной трехзвенной организации системы взаимодействие между уровнями осуществляется последовательно: пользовательский интерфейс инициирует запросы. Сервер системы трансформирует их в соответствии с заданными алгоритмами обработки, а база данных обеспечивает персистентное хранение информации. Такое разделение ответственности соответствует рекомендуемым практикам разработки распределенных систем, позволяя модифицировать каждый компонент независимо от других при сохранении общей функциональности системы [1].

База данных системы (рисунок 2) представляет собой централизованное реляционное хранилище, служащее основным источником достоверных данных для всех компонентов системы учета технических средств связи. Реляционные базы данных обеспечивают структурированное хранение информации в виде связанных таблиц, где каждый элемент описывается набором уникальных атрибутов, а связи между таблицами поддерживаются через внешние ключи [2].

В основе организации данных лежит принцип ссылочной целостности. При этом каждая единица технических средств связи идентифицируется уникальным набором атрибутов: моделью, серийным номером и годом выпуска и выступает в качестве центрального объекта таблицы средств связи, вокруг которой формируется история ее эксплуатации. Сведения о сотрудниках и подразделениях нормализованы и связаны через отношения «один-ко-многим», что исключает дублирование информации и обеспечивает согласованность данных при любых операциях. Таблица «Сотрудники» хранит сведения об учетных записях и правах доступа: при авторизации эти данные определяют профиль пользователя и его принадлежность к конкретному подразделению. В «Средствах связи» содержится ссылка на соответствующий отдел или центр, что позволяет формировать выборки данных строго в соответствии с иерархической структурой организации, обеспечивая конфиденциальность информации на уровне запросов и разграничение доступа в зависимости от должностных полномочий.

Документооборот отражен через таблицы «Акты», «Согласование» и «Подписи», связанные с центральным объектом последовательной цепочкой отношений. Принцип отложенной регистрации реализован через таблицу «Книга регистрации», связанную с таблицей актов отношением «один-к-одному».

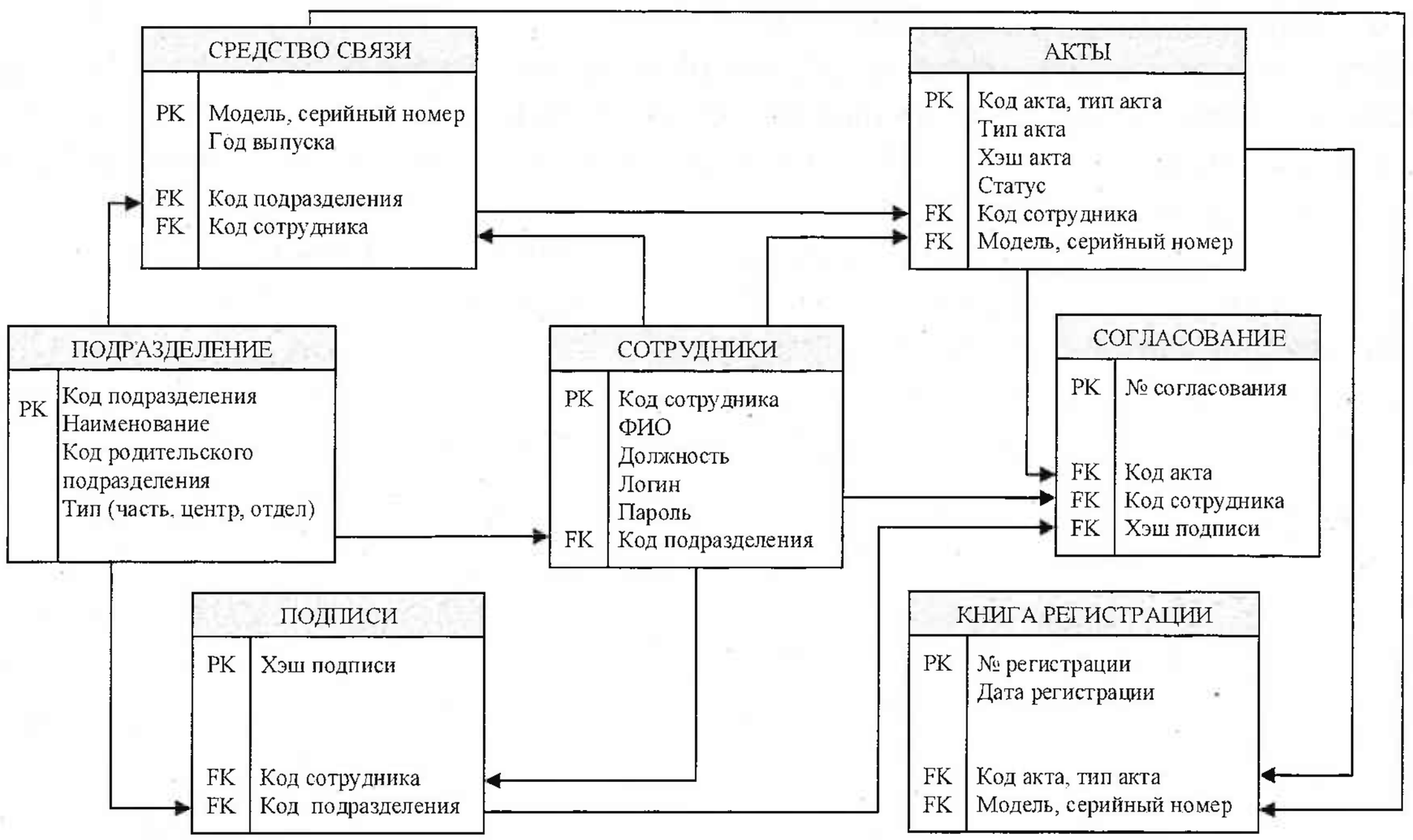


Рисунок 2. – Схема базы данных

Подлинность каждого документа обеспечивается криптографическим хешем, генерируемым при наложении электронной подписи уполномоченным лицом. Хеш-функция создает уникальный «цифровой отпечаток» файла фиксированной длины, обладающий двумя критически важными свойствами: детерминированностью (одинаковые входные данные всегда дают одинаковый хеш) и лавинным эффектом (минимальное изменение контента полностью меняет результат) [3]. При этом восстановление исходных данных из хеш-значения вычислительно невозможно.

В системе эталонный хеш файла сохраняется в момент создания акта и используется как базовое значение для всех последующих проверок. Последовательность хешей,

зафиксированных при участии каждого уполномоченного лица, формирует верифицируемую цепочку, которая не только подтверждает подлинность каждой подписи, но и гарантирует неизменность документа на всем пути его утверждения [3].

В отличие от стандартных электронных подписей, верификация которых осуществляется лишь на завершающем этапе, в разработанной системе хеш SHA-256 пересчитывается и сохраняется после каждой подписи. При обнаружении изменения документа между этапами согласования операция подписания блокируется, а процесс сбрасывается к начальному состоянию.

Таким образом, база данных выступает не пассивным хранилищем, а активным компонентом системы безопасности, обеспечивающим целостность документов через криптографические хеши электронных подписей, автоматизацию учета через книгу регистрации и строгое разграничение доступа на основе организационной структуры.

Механизм иерархического согласования. Система автоматически строит маршрут подписания для каждого документа в зависимости от того, к какому подразделению относится оборудование. Порядок участников жестко задан:

Шаг 1. Комиссия – три пользователя, у которых в профиле установлен признак «член комиссии». Они подписывают первыми, подтверждая, что лично осмотрели образец технических средств связи.

Шаг 2. Начальник отдела – пользователь с ролью «начальник отдела», привязанный к тому же отделу, что и оборудование. Он подтверждает факт закрепления техники.

Шаг 3. Начальник центра – пользователь с ролью «начальник центра», отвечающий за вышестоящее подразделение.

Шаг 4. Командир воинской части (соединения) – пользователь с ролью «командир», который утверждает документ окончательно.

После того как акт переходит на очередной уровень, система автоматически отправляет уведомление соответствующему пользователю. В интерфейсе этот документ появляется на вкладке «На подпись» (рисунок 3). Пользователь может открыть акт, ознакомиться с его содержанием и принять одно из двух решений:

подписать – документ переходит к следующему участнику цепочки;

отклонить – система требует указать причину отклонения, после чего документ возвращается инициатору со статусом «Отклонен».

Уведомления о поступлении новых документов на подпись отображаются визуально, что позволяет своевременно реагировать и не задерживать процесс согласования.

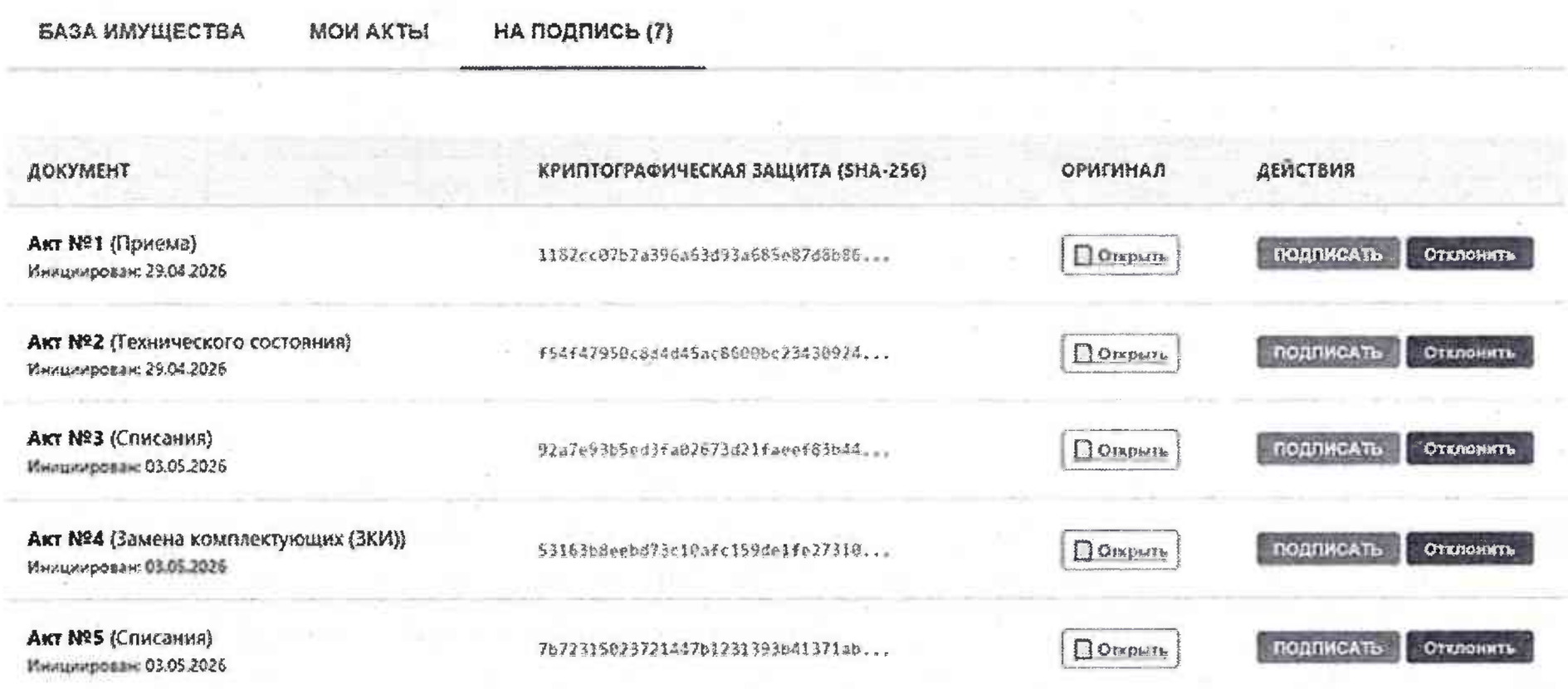


Рисунок 3. – Вкладка «На подпись»

Если в системе нет хотя бы одного из перечисленных участников, создание документа становится невозможным. Система выдает сообщение, каких именно участников не хватает.

На каждом следующем уровне документ может быть подписан (согласован), пока это не сделали на предыдущих уровнях. Такой подход гарантирует, что документ пройдет полный цикл согласования.

Сервер обеспечивает связь между пользовательским интерфейсом и базой данных, он принимает запросы от пользователя, обрабатывает их согласно заданным алгоритмам и формирует ответы, гарантируя, что ни одна операция не будет выполнена в обход установленных правил.

Процедура регистрации пользователей предполагает обязательное указание организационной принадлежности. В зависимости от занимаемой должности пользователь закрепляется за конкретным отделом или центром, что находит прямое отражение в структуре базы данных. При последующей авторизации сервер считывает эти параметры, определяя роль и права доступа [4]. Таким образом, права на просмотр и редактирование информации автоматически ограничиваются рамками закрепленного подразделения, обеспечивая разграничение полномочий уже на этапе входа в систему.

Процесс создания нового документа начинается с проверки наличия образцов технических средств связи в реестре. В случае, если устройство не найдено, сервер инициирует процедуру создания новой учетной карточки, требуя заполнения обязательных полей идентификации. Только после регистрации устройства в базе данных открывается возможность привязки к нему документа.

Далее пользователь загружает готовый файл документа (например, акт технического состояния) и формирует маршрут согласования, включающий членов комиссии и председателя. Сервер сохраняет файл и создает запись в таблице документов со статусом «Создан». Одновременно генерируется начальный криптографический хеш содержимого файла, который фиксируется в базе как эталон для последующей верификации. Хеш представляет собой результат работы хеш-функции – алгоритма, преобразующего входные данные произвольного размера в строку фиксированной длины. Именно это свойство делает его полезным для быстрого поиска, проверки целостности данных и защиты информации [5]. На каждом этапе (рисунок 4) сервер проверяет актуальный хеш файла. В случае, если содержимое было изменено после предыдущей подписи, операция блокируется и процесс согласования сбрасывается.

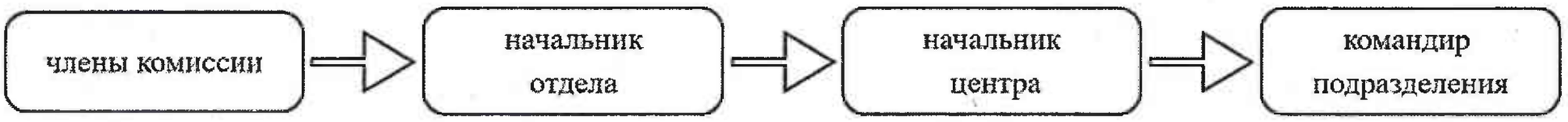


Рисунок 4. – Последовательность подписи документов (вариант)

Получая запрос на подписание, сервер идентифицирует роль пользователя и проверяет его место в цепочке утверждения. Алгоритм маршрутизации актов автоматически формирует цепочку из четырех обязательных ступеней подписания: три члена комиссии, начальник отдела, начальник центра, командир воинской части (соединения). При отсутствии в системе не менее трех пользователей с правом члена комиссии создание документа блокируется. Переход документа в статус «Утвержден» и его регистрация в книге учета (рисунок 5) происходит только после подписи всех участников цепочки.

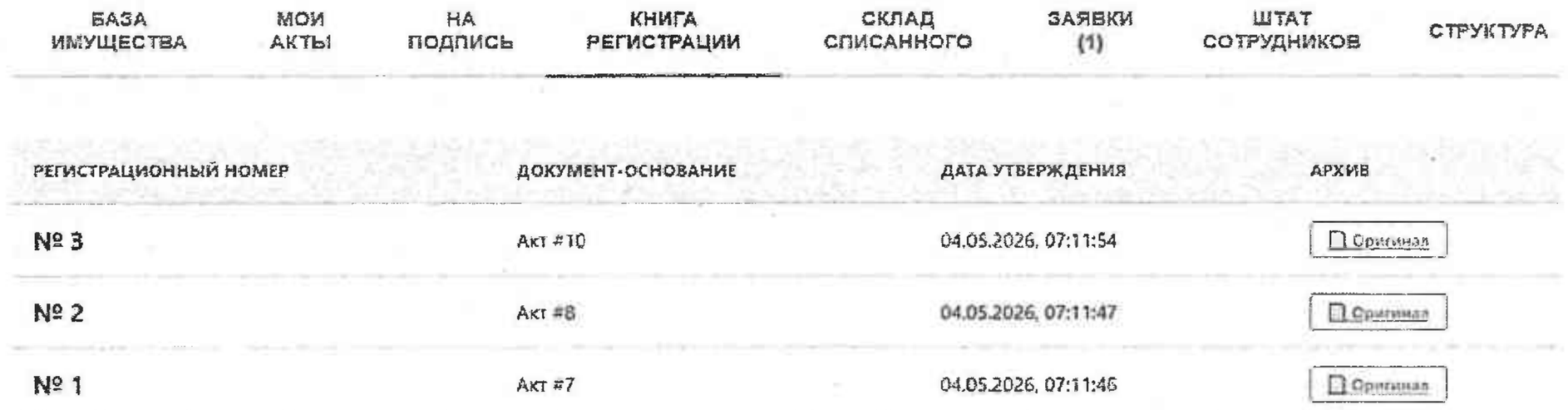


Рисунок 5. – Окно электронной книги регистрации документов (вариант)

Предложенная модель документооборота, в отличие от традиционных систем, где запись в книгу учета производится вручную в начале процесса или вообще не связана с утверждением, реализует принцип отложенной регистрации: документ попадает в реестр автоматически и только после завершения всех четырех уровней согласования. Это исключает появление незавершенных или отклоненных документов в официальной книге учета. В этот момент сервер генерирует уникальный регистрационный номер и фиксирует в реестре полный набор атрибутов: регистрационный номер, дата записи, наименование документа, дата регистрации, на какие технические средства выдан (получен) документ. После этого документ становится доступен для просмотра в общем реестре в пределах полномочий каждого пользователя.

Такая архитектура серверной части обеспечивает полный контроль над документооборотом: каждый документ имеет четкий статус и неизменяемую запись в реестре, а автоматизация ключевых этапов – от проверки устройства до его регистрации – минимизирует влияние человеческого фактора и повышает достоверность учетных данных.

Пользовательский интерфейс завершает архитектурный контур системы, трансформируя сложные механизмы серверной обработки и криптографической верификации в интуитивно понятные инструменты работы. Проектирование осуществлялось по принципу минимальной достаточности. Интерфейс, в зависимости от роли пользователя, предоставляет ровно тот набор функций и данных, который необходим для выполнения должностных обязанностей в рамках установленной иерархии. Панель навигации формирует персонализированное меню, фильтруемое по принадлежности к подразделению, сотрудник отдела видит только технику и документы своего подразделения, начальник центра получает доступ к сведениям всех подчиненных отделов, а командир части работает с полным списком средств связи. Таким образом, построение исключает возможность случайного обращения к чужим данным и позволяет пользователю сосредоточиться на решении задач, не отвлекаясь на излишнюю информацию.

Структура навигации сгруппирована вокруг трех составляющих системы:

1. Книга регистрации документов – предоставляет доступ к официальному реестру утвержденных актов с возможностью фильтрации по типам документов, периодам и подразделениям.

2. Технические средства связи – иерархический каталог оборудования, сгруппированный по типам (персональные компьютеры, моноблоки, принтеры, плоттеры, мониторы и т. д.), что ускоряет поиск конкретной единицы техники.

3. Штат сотрудников – реестр личного состава с визуализацией закрепленной техники, позволяющий контролировать распределение ресурсов.

Такое построение навигации минимизирует количество переходов между разделами и позволяет пользователю сосредоточиться на решении задач, не затрачивая время на поиск необходимых модулей.

Центральным элементом интерфейса является таблица средств связи (рисунок 6), где каждая строка представляет собой отдельную единицу техники. Колонки отображают модель, тип, серийный номер, год выпуска, наработку в часах, категорию, текущий статус (например, «В эксплуатации») и доступные действия.

При нажатии на строку открывается детальная карточка средства связи, которая объединяет идентификационные данные устройства и всю связанную с ним документацию. В отличие от систем, где пользователь вручную вводит идентификатор оборудования при создании документа, в данной работе учетная карточка, идентифицируемая комплексом «модель + серийный номер + год выпуска», выступает первичным объектом. Это полностью исключает ошибки ручного ввода и гарантирует, что каждый акт относится к реально существующей единице техники.

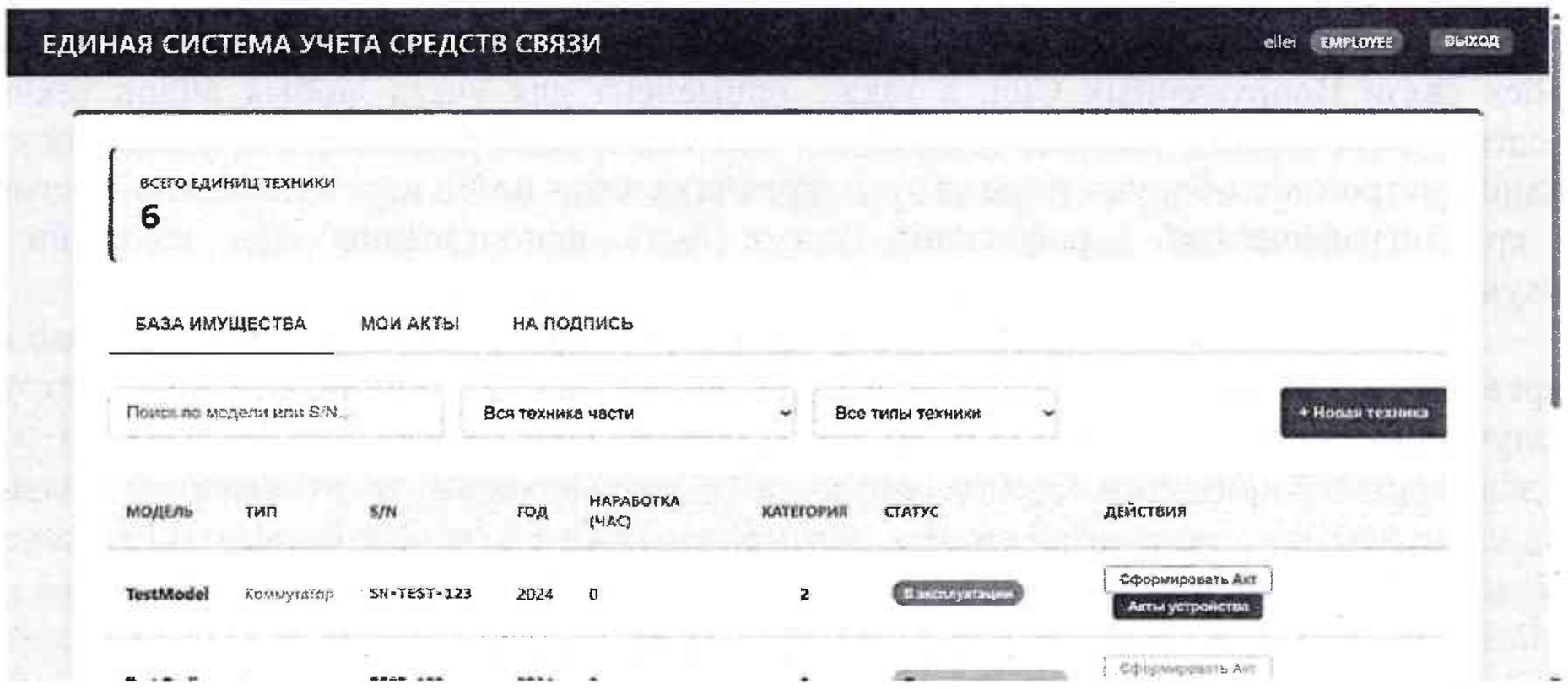


Рисунок 6. – Пользовательский интерфейс системы (вариант)

Кнопка «Сформировать документ», размещенная в непосредственной близости от идентификационных данных, обеспечивает мгновенный запуск процесса документооборота. При ее активации пользователь загружает готовый файл документа и выбирает из предустановленного списка лиц, уполномоченных на подписание. Сервер автоматически проверяет корректность маршрута согласования в соответствии с иерархической структурой подразделения.

Таблица документов отражает полную историю эксплуатации технического средства связи. Каждая строка таблицы содержит тип документа, дату его создания и регистрационный номер из книги учета. Наличие или отсутствие регистрационного номера служит ключевым визуальным индикатором статуса документа: если номер присвоен, значит, акт утвержден командиром воинской части (соединения), если поле пусто – документ находится в процессе согласования.

Для минимизации задержек в процессе согласования интерфейс интегрирован с системой уведомлений. Когда документ поступает на уровень пользователя для подписания, система генерирует уведомление, содержащее ссылку на конкретный документ, его тип и информацию о средстве связи. Начальники отделов (центров) получают сводные уведомления о накоплении документов, ожидающих их подписи. Командир воинской части (соединения) видит список документов, готовых к финальному утверждению. Визуальная простота интерфейса скрывает многоуровневую архитектуру системы: реляционные связи базы данных, криптографические алгоритмы и серверную логику согласования.

Выводы

Предлагаемая нами архитектура системы учета технических средств связи может быть реализована без нарушения привычных процедур прохождения документов и с сохранением их утвержденных форм.

В целом научная новизна полученных нами результатов заключается в следующем:

1. Для учета технических средств связи в организациях с иерархической структурой реализована модель документооборота, объединяющая принципы отложенной регистрации, иерархического разграничения доступа и сквозной криптографической верификации.

2. Разработана последовательная цепочка хешей SHA-256, фиксирующая состояние документа после каждой подписи и обеспечивающая автоматическую блокировку утверждения при любых посторонних изменениях в противоположность стандартным электронным цифровым подписям, верификация которых осуществляется лишь на завершающем этапе.

3. Учетная карточка технического средства связи, идентифицируемая комплексом «модель, серийный номер, год выпуска», использована в качестве первичного объекта привязки документа, что исключает ошибки ручного ввода при создании актов.

Разработанная система после апробации может быть внедрена в соединениях и частях войск связи Вооруженных Сил, а также применена для учета любых видов технических средств, подлежащих учету по уникальным номерам (автомобильная техника, вооружение, радиоэлектронное оборудование и др.). Предложенные принципы отложенной регистрации и криптографической верификации могут быть использованы при создании систем документооборота в любых организациях со сложной иерархической структурой.

Практическая ценность работы заключается в создании универсального шаблона для перевода бумажных процессов в электронный вид в организационных структурах. Полученные результаты могут быть адаптированы для учета других категорий ресурсов, а заложенные принципы криптографической верификации и отложенной регистрации использованы при разработке систем документооборота в любых организациях со сложной структурой подчинения.

Список использованных источников

1. Кручинин, В. В. Методы и технологии разработки клиент-серверных приложений : учеб. пособие / В. В. Кручинин, Ю. В. Морозова. – Томск : Томский гос. ун-т систем управления и радиоэлектроники, 2018. – 106 с.

2. Реляционные базы данных: определение, примеры, особенности [Электронный ресурс] // OTUS. – Режим доступа: https://otus.ru/journal/relyacionnye-bazy-opredelenie-primery-osobennosti/. – Дата обращения: 02.02.2026.

3. Хеш цифровой подписи: что это такое и как работает [Электронный ресурс] // TechAttribute. – Режим доступа: https://techattribute.ru/hjesh-cifrovoj-podpisi-chto-jeto/. – Дата обращения: 10.02.2026.

4. Ролевая модель доступа RBAC [Электронный ресурс] // Glabit. – URL: https://glabit.ru/blog/rolevaya-model-dostupa-rbac. – Дата обращения: 10.02.2026.

5. Проверка хеш-суммы файла: зачем нужна и как выполнить [Электронный ресурс] // ComputerInfo. – Режим доступа: https://computerinfo.ru/hash-check/. – Дата обращения: 10.02.2026.

---

* Сведения об авторах:
Аскерко Анатолий Владимирович,
УО «Военная академия Республики Беларусь»;
Лейбук Екатерина Владимировна,
Савицкий Алексей Юрьевич,
УО «Белорусский государственный университет информатики и радиоэлектроники».
Статья поступила в редакцию 13.04.2026 г.