УДК 004

ПРИНЦИПЫ СИСТЕМНОЙ ИНЖЕНЕРИИ ПРИ АНАЛИЗЕ И СОВЕРШЕНСТВОВАНИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ООО БАНК «ЭЛИТА»

Кашицын М.А.,
студент,
Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия

Соколов Н.В.,
старший преподаватель кафедры информатики и информационных технологий
Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия

Аннотация

В статье рассматривается применение принципов системной инженерии при анализе и совершенствовании автоматизированной системы межбанковского обмена электронными сообщениями в ООО Банк «Элита». Особое внимание уделено вопросам соответствия требованиям Положения Банка России № 802-П, управлению жизненным циклом системы, идентификации требований заинтересованных сторон и управлению рисками. В исследовании демонстрируется, как системная инженерия способствует построению надёжной и управляемой архитектуры безопасности в банковской ИТ-среде. На основе проведенного анализа сформулированы практические рекомендации по повышению устойчивости и соответствия системы регуляторным нормам, что может быть применено в других кредитных организациях.

Ключевые слова: системная инженерия, информационная безопасность, межбанковский обмен, жизненный цикл, управление рисками, СЗИ, безопасность сообщений.

PRINCIPLES OF SYSTEM ENGINEERING IN ANALYSIS AND IMPROVEMENT OF THE AUTOMATED SYSTEM IN ELITA BANK LLC

Kashitsyn M.A.,
student,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia
Sokolov N.V.,
Senior Lecturer at the Department of Computer Science and Information Technology
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Abstract

The article discusses the application of system engineering principles in the analysis and improvement of the automated system for interbank electronic message exchange in Elita Bank LLC. Particular attention is paid to compliance with the requirements of Bank of Russia Regulation No. 802-P, system life cycle management, identification of stakeholder requirements and risk management. The study demonstrates how system engineering contributes to the construction of a reliable and manageable security architecture in the banking IT environment. Based on the analysis, practical recommendations are formulated to improve the sustainability and compliance of the system with regulatory standards, which can be applied in other credit institutions.

Keywords: system engineering, information security, interbank exchange, life cycle, risk management, information security system, message security.

Информационная безопасность является критически важным элементом функционирования современной банковской системы. В условиях цифровизации процессов, роста числа киберугроз и усиления регуляторных требований, защита каналов межбанковского обмена электронными сообщениями становится одной из ключевых задач для инженерно-технических

служб [9], [10]. Системная инженерия, как дисциплина, направленная на комплексное проектирование, разработку и сопровождение сложных технических систем [7], [8], предоставляет эффективные методы для построения безопасных, надёжных и управляемых информационных решений. В данной статье рассматривается, как принципы системной инженерии могут быть применены для анализа и совершенствования системы межбанковского обмена в ООО Банк «Элита», включая реализацию требований Положения Банка России № 802-П [4] и других нормативных актов в области ИБ.

Банковский сектор характеризуется высокой сложностью информационных систем, которые должны функционировать бесперебойно и безопасно. Традиционный подход, при котором меры безопасности внедряются точечно, уже не справляется с современными вызовами. Необходим взгляд на систему как на целостный объект, имеющий начало и конец жизненного цикла [6], вовлекающий множество заинтересованных сторон и подверженный постоянно меняющимся рискам. Именно такой взгляд и предлагает системная инженерия, интегрируя технические, организационные и управленческие аспекты. Целью данной статьи является демонстрация практического применения принципов системной инженерии для решения конкретных проблем в области межбанковских коммуникаций и формирования дорожной карты по переходу к более зрелой и управляемой модели информационной безопасности.

В Банке «Элита» функционирует автоматизированная система обмена электронными сообщениями с платёжной системой Банка России. Через данную систему ежедневно передаются платёжные поручения, отчёты, выписки, запросы и другие документы. Передача осуществляется по защищённым каналам связи с использованием криптографических средств, в том числе электронной подписи (ЭП). Данная система относится к критически важным бизнес-процессам, так как её сбой или компрометация напрямую ведут к финансовым потерям и репутационным рискам.

Ключевыми компонентами этой системы являются: шлюз обмена сообщениями с ЦБ РФ, который выступает точкой входа и выхода для всего трафика; сервисы генерации и проверки ЭП, обеспечивающие юридическую значимость и целостность передаваемых данных; сервер хранения и архивирования сообщений, предназначенный для долгосрочного хранения информации в соответствии с регуляторными требованиями; журналы аудита, фиксирующие все операции с сообщениями; а также интерфейсы с внутренними банковскими системами, такими как 1С и ABS (Automated Banking System), обеспечивающие интеграцию с учётными и операционными процессами банка. Несмотря на кажущуюся надёжность архитектуры, детальный анализ выявил ряд системных проблем.

Несмотря на наличие средств защиты информации (СЗИ), в текущей реализации системы выявлены следующие проблемы и риски [9],[10]. Одной из наиболее острых проблем является сложность управления сертификатами ЭП, включая своевременную замену и отзыв. Этот процесс зачастую осуществляется вручную, что приводит к риску использования просроченных или скомпрометированных ключей, а следовательно, к отклонению сообщений со стороны контрагентов или регулятора. Другой значительный недостаток – отсутствие централизованного мониторинга событий безопасности, в том числе на уровне шлюза. События безопасности регистрируются в разрозненных логах, что затрудняет оперативное обнаружение и расследование инцидентов, таких как попытки несанкционированного доступа или аномальная активность.

Также наблюдается слабая формализация требований к резервному копированию и восстановлению в случае сбоя. Хотя резервные копии создаются, процедуры их восстановления не были полноценно протестированы, а целевые показатели времени восстановления (RTO) и точки восстановления (RPO) [3] не были формально установлены, что ставит под вопрос возможность быстрого возобновления работы после серьёзного инцидента. Ручной ввод некоторых

параметров в процессе подготовки сообщений повышает вероятность ошибок, ведущих к искажению данных или их отправке по неверному маршруту.

Важной организационной проблемой является несогласованность между подразделениями (ИБ, ИТ, бухгалтерия) при реагировании на инциденты. Отсутствие четких регламентов взаимодействия приводит к задержкам в принятии решений и нейтрализации угроз. Наконец, было выявлено формальное выполнение требований 802-П без полной интеграции мер защиты в жизненный цикл системы [4]. Меры безопасности часто воспринимаются как разовое мероприятие для прохождения проверки, а не как неотъемлемая часть процессов разработки и эксплуатации. Эти и другие факторы указывают на необходимость применения системного подхода к проектированию защищённой архитектуры обмена, в том числе с учётом всего жизненного цикла ИС и участия всех заинтересованных сторон.

Системная инженерия обеспечивает единый подход к проектированию, внедрению и сопровождению сложных систем, включая те, что функционируют в условиях жёстких регуляторных требований. Её суть заключается в рассмотрении системы как целостного объекта с момента зарождения идеи до утилизации, при активном участии всех сторон, на которых влияет её функционирование [7], [8]. Ниже рассмотрим, как её принципы применяются в рамках автоматизированной системы межбанковского обмена в Банке «Элита».

Фундаментом любого системно-инженерного проекта является чёткая и неизбыточная идентификация требований. На этапе инициализации проекта системный инженер совместно со специалистами по информационной безопасности должен сформулировать и зафиксировать требования [5], среди которых: безусловное соответствие Положению Банка России № 802-П, что является обязательным условием легитимности всей системы; реализация механизмов криптографической защиты информации (включая ЭП) с использованием сертифицированных ФСБ России средств; всеобъемлющее журналирование всех событий безопасности с гарантированным хранением

записей не менее 1 года для последующего аудита и расследования инцидентов; организация резервного копирования в соответствии с принципами RPO ≤ 15 мин и RTO ≤1 ч, что гарантирует минимальные потери данных и времени простоя; строгое разграничение прав доступа по ролям в системах обработки сообщений для минимизации риска внутренних угроз; а также обеспечение доступности сервиса на уровне ≥ 99,5 % в год, что соответствует высоким стандартам бесперебойности банковских операций.

Идентификация требований производится с учётом мнений всех заинтересованных сторон. Этот процесс итеративен и предполагает использование различных техник, таких как интервью, анкетирование и анализ документов. Требования должны быть конкретными, измеримыми, достижимыми, релевантными и ограниченными по времени, чтобы их можно было объективно проверить на этапе тестирования. Например, требование к доступности 99,5% легко верифицируемо с помощью данных мониторинга, в то время как требование «обеспечить высокую безопасность» – нет.

Успех проекта напрямую зависит от того, насколько полно учтены интересы и ожидания всех сторон, вовлеченных в жизненный цикл системы или как-то с ним связанных. В проекте модернизации системы межбанковского обмена в Банке «Элита» следующие внутренние группы участников: служба информационной безопасности, которая заинтересована в защите каналов связи, управлении рисками и проведении регулярного аудита; ИТ-служба, которая фокусируется на таких аспектах, как надёжность системы, её резервирование и бесперебойное обновление сертификатов; бухгалтерия, как ключевой пользователь, ожидает своевременной и безошибочной передачи и получения платёжных документов, так как сбои напрямую влияют на финансовые операции банка; руководство банка, которое заинтересовано в стратегических целях, а именно соответствию регуляторным требованиям для избежания штрафов и минимизация инцидентов для сохранения деловой репутации.

К внешним сторонам можно отности Банк России, который, как регулятор и оператор платёжной системы, предъявляет жёсткие требования к защищённому приёму и передаче сообщений по протоколу МЭДО. Также важной стороной являются вендоры ПО, от которых зависит поддержка актуальности сертифицированных СЗИ и своевременное устранение уязвимостей. Оценка ожиданий этих сторон позволяет сбалансировать функциональные и нефункциональные требования к системе. Например, требование бухгалтерии к скорости обработки может конфликтовать с требованием ИБ-службы к дополнительным проверкам. Системный инженер выступает медиатором, находя компромиссное решение, удовлетворяющее всех в рамках установленных ограничений и стандартов.

Ключевым принципом системной инженерии является рассмотрение системы через призму её полного жизненного цикла [6]. Работа над системой обмена в Банке «Элита» должна учитывать все этапы, от концепции до вывода из эксплуатации, как это определено в международных стандартах, таких как ISO/IEC/IEEE 15288 [2]. Первым этапом является *инициация*, на котором происходит постановка задачи, проводится первичный анализ угроз и выбирается архитектурное решение. На *этапе проектирования* строится детальная модель архитектуры, разрабатываются и формализуются требования к защите, выбираются конкретные технологии и продукты.

Этап разработки и интеграции включает в себя настройку шлюза, внедрение средств ЭП, развертывание систем журналирования и резервного копирования, а также интеграцию с внутренними системами банка. Затем следует критически важный этап тестирования, на котором проводится верификация выполнения всех требований, в том числе требований 802-П, и проверка отказоустойчивости системы в различных сценариях. После ввода в эксплуатацию начинается этап сопровождения, который включает регулярный аудит, процедуры замены криптографических ключей, анализ журналов и применение обновлений безопасности. Наконец, этап вывода из эксплуатации

предусматривает безопасное архивирование исторических данных и их последующее уничтожение в соответствии с политикой хранения информации, чтобы избежать утечки чувствительных данных после прекращения использования системы. Такой полный охват позволяет управлять системой проактивно, а не реагировать на проблемы по мере их возникновения.

Для построения оптимальной и безопасной архитектуры системная инженерия предлагает использовать стандартизированные *методы моделирования*. При проектировании системы межбанковского обмена в Банке «Элита» применяются следующие методики: DFD-диаграммы (Data Flow Diagrams) используются для визуализации потоков данных и сообщений между различными подсистемами (входящие, исходящие, подтверждения), что позволяет выявить точки обработки информации и потенциальные уязвимости на стыках компонентов; UML-диаграммы (Unified Modeling Language), в частности диаграммы последовательностей и прецедентов, отображают взаимодействие пользователя (например, бухгалтера или ИБ-специалиста) с системой, помогая проектировать удобный и безопасный пользовательский интерфейс; ER-модели (Entity-Relationship) описывают структуру хранения метаданных сообщений, электронных подписей и архивов в базах данных, что является основой для проектирования отказоустойчивых и эффективных хранилищ.

Для *формализации спецификаций и требований* активно используются стандарты, которые описывают структуру документа с требованиями к программному обеспечению. Это обеспечивает однозначность трактовки требований всеми участниками проекта – разработчиками, тестировщиками и заказчиками. Например, при получении сообщения из ЦБ, процесс, описанный на DFD и UML, может выглядеть так: шлюз выполняет валидацию ЭП, затем расшифровку содержимого, после чего регистрирует сообщение в журнале, уведомляет ответственного сотрудника через интерфейсное приложение и,

наконец, отправляет копию на сервер архивирования. Каждый из этих шагов должен быть описан, спроектирован и протестирован.

Управление рисками является не дополнительной функцией, а ключевым, сквозным элементом системной инженерии в банковской сфере. В рамках проекта модернизации системы обмена выполняется непрерывный процесс управления рисками, основанный на стандартах типа ISO/IEC 27005 [1]. Он начинается с идентификации и анализа угроз, к которым относятся несанкционированный доступ к каналам связи, подмена передаваемых сообщений, полный или частичный сбой передачи данных, а также инсайдерские угрозы. Затем производится классификация активов (сами сообщения, ключи шифрования, сервера) и выявление их уязвимостей (например, устаревшее ПО на шлюзе).

На следующем этапе выполняется расчёт уровней риска по упрощённой шкале, где риск = вероятность возникновения × потенциальный ущерб. Это позволяет ранжировать риски и сфокусировать ресурсы на обработке наиболее критичных из них. Далее проектируются и внедряются контрмеры, которые могут быть техническими (внедрение межсетевого экрана, настройка SIEM) или организационными (разработка регламентов, обучение персонала). Завершающим и непрерывным элементом является постоянный аудит журналов событий, желательно с использованием SIEM-системы (Security Information and Event Management), которая агрегирует данные с различных источников и позволяет коррелировать события для выявления сложных атак. Особое внимание уделяется инцидентам, связанным с нарушением целостности сообщений, истечением срока действия сертификатов, ошибками маршрутизации и задержками в доставке, так как они напрямую влияют на финансовую деятельность банка.

В результате применения принципов системной инженерии к анализу автоматизированной системы межбанковского обмена в ООО Банк «Элита» были выявлены ключевые точки повышения защищённости и эффективности.

Во-первых, были сформулированы и структурированы требования информационной безопасности с учётом требований Положения № 802-П и ГОСТ Р 57580.1. Это создало чёткую и измеримую основу для дальнейшего проектирования и тестирования системы. Во-вторых, выявлены заинтересованные стороны и их роли в жизненном цикле системы, что позволило устранить традиционные конфликты между целями ИТ (скорость, функциональность) и ИБ (безопасность, соответствие). Был налажен диалог между подразделениями.

В-третьих, разработана комплексная модель жизненного цикла системы, включающая этапы проектирования, внедрения и сопровождения, с акцентом на верификацию и аудит. Это перевело эксплуатацию системы из реактивного режима «латания дыр» в проактивный режим управляемого развития. В-четвёртых, проведён всесторонний анализ рисков, определены уязвимые места и предложены конкретные меры по их снижению. Например, была предложена автоматизация ротации ключей ЭП для исключения человеческого фактора и внедрение системы мониторинга журналов для оперативного обнаружения аномалий. В-пятых, в качестве центрального элемента будущей архитектуры было предложено внедрение SIEM-системы для централизованного мониторинга событий безопасности со всех компонентов, включая шлюз межбанковского обмена.

На основе проведенного анализа сформулированы следующие рекомендации. Первой рекомендацией является необходимость формализовать архитектуру системы межбанковского обмена с использованием моделей DFD и UML. Это обеспечит общее понимание системы всеми участниками проекта и выявит слабые места на ранних стадиях. Второй ключевой рекомендацией является внедрение автоматизированных процедур управления ключами, резервного копирования и восстановления. Автоматизация минимизирует риск человеческой ошибки и гарантирует выполнение установленных требований к RPO и RTO.

Третья рекомендация заключается в необходимости регулярно пересматривать список угроз и рисков с актуализацией мер защиты. Угрозы кибербезопасности постоянно эволюционируют, и система защиты должна адаптироваться к ним. Четвертый пункт – обеспечить регулярное обучение персонала, участвующего в процессе обмена, в том числе по вопросам работы с криптографией и осознания роли в обеспечении безопасности. И наконец, пятой рекомендацией является проведение регулярного внешнего аудита системы на соответствие требованиям 802-П и ГОСТ 57580.1 [4], [5]. Независимая оценка поможет выявить скрытые недостатки и подтвердить уровень зрелости системы управления информационной безопасностью.

Заключение

Применение системной инженерии к задачам информационной безопасности в банковской сфере позволяет обеспечить структурированный и управляемый подход к разработке, эксплуатации и модернизации критически важных ИС. Это не просто набор технических практик, а целостная философия управления сложностью, учитывающая технические, организационные и человеческие аспекты.

Опыт Банка «Элита» показывает, что принципы системной инженерии позволяют выстраивать защищённую архитектуру межбанковского обмена и обеспечивать соответствие требованиям регуляторов. Внедрение этих принципов позволило перейти от разрозненных и зачастую противоречащих друг другу мер к комплексной и согласованной системе безопасности.

Интеграция методов системной инженерии в практику ИБ является необходимым шагом для устойчивого и безопасного функционирования банковской инфраструктуры в условиях цифровизации и растущих киберугроз. Это инвестиция не только в технологические активы, но и в зрелость процессов и компетенций персонала, что в конечном итоге формирует устойчивое конкурентное преимущество и укрепляет доверие клиентов и регуляторов.

Библиографический список:

1. ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: ISO, 2022. [Электронный ресурс]. — Режим доступа — URL: https://www.iso.org/standard/80585.html (дата обращения: 26.08.2025)

2. ISO/IEC/IEEE 15288:2023. Systems and software engineering — System life cycle processes. — Geneva: ISO, 2023. [Электронный ресурс]. — Режим доступа — URL: https://www.iso.org/standard/81702.html (дата обращения: 26.08.2025)

3. Sber. RTO и RPO: что это и в чём отличия - habr.com, 2024. [Электронный ресурс]. — Режим доступа — URL: https://habr.com/ru/companies/sberbank/articles/838226/ (дата обращения: 26.08.2025).

4. Банк России. Положение № 802-П от 25.07.2022 «О требованиях к защите информации в платёжной системе Банка России». [Электронный ресурс]. — Режим доступа — URL: https://docs.cntd.ru/document/351621361 (дата обращения: 26.08.2025)

5. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. - Центральный банк Российской Федерации, 2018. [Электронный ресурс]. — Режим доступа — URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 26.08.2025)

6. Зараменских, Е. П. Информационные системы: управление жизненным циклом: учебник и практикум для вузов / Е. П. Зараменских. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 486 с. — (Высшее образование). — ISBN 978-5-534-21415-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/571328 (дата обращения: 25.08.2025).

7. Левенчук, А. Системная инженерия. — 2022: учебник / А. Левенчук. - Ridero, 2022. - 378 с. - ISBN: 978-5-0059-0127-9

8. Николенко В. Ю. Системы систем. Базовые сведения: учебник / В.Ю. Николенко. - Ridero, 2025. - 394 с. - ISBN: 978-5-0065-7293-5

9. Рыжов, М. Р. Информационная безопасность банка России / М. Р. Рыжов, Н. М. Гореева // Материалы Всероссийской (национальной) научно-практической конференции с международным участием, посвящённой 110-летию со дня рождения Ивана Сергеевича Кауричева : Материалы конференции, г. Калуга, 14 декабря 2023 года. – Калуга: ИП Якунина В.А., 2024. – С. 478-483. [Электронный ресурс]. — Режим доступа — URL: https://www.elibrary.ru/item.asp?id=65615535 (дата обращения: 27.08.2025)

10. Саяпина, Н. Н. Информационная безопасность банка как необходимое условие его функционирования / Н. Н. Саяпина, Л. А. Кусакин // Экономика сферы сервиса: проблемы и перспективы : Материалы V Всероссийской научно-практической конференции, Омск, 20–22 ноября 2018 года / Минобрнауки России, ОмГТУ; под общ. ред. А.С. Полынского. – Омск: Омский государственный технический университет, 2019. – С. 84-87. [Электронный ресурс]. — Режим доступа — URL: https://www.elibrary.ru/item.asp?id=36897594 (дата обращения: 27.08.2025)

Оригинальность 78%