Глава 1. Анализ безопасности мобильных приложений и оценка уровня доверия

1.1. Основные угрозы безопасности мобильных приложений

В наши дни мобильные приложения превратились в неотъемлемую часть информационной инфраструктуры бизнеса, особенно в финансовой сфере. Миллионы людей каждый день проводят финансовые операции через свои смартфоны, что неизбежно привлекает внимание злоумышленников. Изучение современных угроз безопасности мобильных приложений выявляет целый ряд проблем, требующих пристального внимания как при разработке, так и при эксплуатации программного обеспечения.

Утечка конфиденциальных данных остаётся одной из самых серьезных угроз для мобильных приложений. Банковские и финансовые приложения работают с особо чувствительной информацией: персональными данными клиентов, информацией о банковских счетах, историей транзакций и платежными реквизитами. Исследование, проведенное компанией Positive Technologies в 2022 году, показало тревожную статистику – более 63% мобильных приложений в финансовом секторе содержат уязвимости, способные привести к утечке конфиденциальной информации. Особенно опасны случаи, когда приложение хранит чувствительные данные без шифрования или применяет ненадежные методы шифрования. Значительным риском также является неконтролируемая передача данных сторонним сервисам через встроенные рекламные сети или аналитические инструменты.

Недостатки механизмов аутентификации и авторизации также представляют серьезную угрозу. Слабые системы проверки подлинности пользователя открывают злоумышленникам возможности для несанкционированного доступа к финансовым ресурсам. К этой категории относятся низкие требования к надежности паролей, отсутствие многофакторной аутентификации, небезопасное хранение учетных данных и проблемы в реализации механизмов управления сессиями. По данным OWASP Foundation, примерно 47% мобильных финансовых приложений имеют существенные недостатки в системах аутентификации, делая их уязвимыми для брутфорс-атак, социальной инженерии или перехвата сессий.

Проблема небезопасного хранения данных на устройстве заслуживает отдельного внимания. Многие разработчики мобильных приложений сохраняют информацию локально без должных мер защиты. Это включает использование незащищенных баз данных, сохранение конфиденциальной информации в лог-файлах, буфере обмена или неправильно настроенных резервных копиях. Если устройство будет скомпрометировано или попадет в руки третьих лиц, последствия могут быть крайне серьезными. Исследователи отмечают, что около 71% банковских мобильных приложений имеют те или иные проблемы с безопасным хранением данных, что создает серьезные риски для пользовательской информации.

Уязвимости сетевого взаимодействия представляют еще одну важную категорию угроз. Финансовые приложения постоянно обмениваются информацией с серверами, и недостатки в этом взаимодействии могут привести к перехвату или подмене данных. К типичным проблемам относятся использование нешифрованных соединений, неправильная реализация SSL/TLS протоколов, отсутствие проверки сертификатов и уязвимости в API. Согласно отчету ImmuniWeb (2023), примерно 37% финансовых мобильных приложений содержат серьезные уязвимости в сетевых коммуникациях, позволяющие реализовать атаки типа Man-in-the-Middle и перехватывать конфиденциальные данные пользователей.

Особую категорию рисков представляют возможности реверс-инжиниринга и модификации приложений. В отличие от веб-сервисов, мобильные приложения выполняются непосредственно на устройствах пользователей, что делает их уязвимыми для анализа и изменения. Хакеры могут декомпилировать приложение, изучить его код, найти слабые места и внедрить вредоносные функции. Отсутствие защиты от реверс-инжиниринга, должной обфускации кода и механизмов обнаружения модификаций существенно повышает риски. Более 54% мобильных финансовых приложений не имеют достаточной защиты от такого вида атак, что делает их легкой мишенью для создания модифицированных версий, используемых в мошеннических схемах.

Статистика инцидентов безопасности показывает неутешительную тенденцию – атаки на мобильные финансовые приложения становятся всё изощреннее и чаще. Лаборатория Касперского отмечает, что в 2023 году количество целенаправленных атак на финансовые мобильные приложения выросло на 23% по сравнению с предыдущим годом. При этом средний ущерб от успешной атаки составляет около 117 тысяч долларов для организации, а в случае масштабных инцидентов может достигать миллионов. Наибольшую опасность представляют целевые атаки на конкретные финансовые учреждения, проводимые хорошо организованными группами хакеров высокой квалификации.

Последствия реализации угроз безопасности критичны как для пользователей, так и для организаций. Клиенты могут столкнуться с прямыми финансовыми потерями, утечкой личных данных и потерей доверия к цифровым банковским сервисам. Для компаний это оборачивается финансовыми убытками, ударом по репутации, юридическими рисками и возможными санкциями регуляторов. По данным Ponemon Institute, средняя стоимость инцидента с утечкой данных в финансовом секторе достигает 5,85 миллионов долларов – наивысший показатель среди всех отраслей.

Всесторонний анализ угроз безопасности мобильных приложений подводит нас к пониманию необходимости комплексного подхода к обеспечению их защищенности. Это особенно актуально для финансового сектора с его высокими рисками и потенциальными потерями. Для решения проблемы недостаточно просто внедрять современные технологии – требуется разработка эффективных механизмов оценки безопасности и создание атмосферы доверия к мобильным приложениям.

1.2. Требования к безопасности мобильных приложений по стандарту OWASP MASVS

На фоне растущих киберугроз разработка стандартизированных подходов к защите мобильных приложений становится жизненно важной задачей. Одним из самых авторитетных стандартов в этой области является Mobile Application Security Verification Standard (MASVS), созданный международным сообществом OWASP (Open Web Application Security Project). Этот стандарт представляет собой структурированный свод требований безопасности для мобильных приложений и служит фундаментом для их проектирования, разработки и тестирования.

OWASP MASVS выделяет несколько уровней верификации безопасности, соответствующих различным степеням защищенности приложения в зависимости от его критичности и требований. Правильное понимание этих уровней играет ключевую роль при определении целевых показателей защиты при разработке мобильных приложений.

Базовый уровень MASVS-L1 (стандартная безопасность) устанавливает минимальные требования для всех мобильных приложений. Этот уровень определяет основной набор защитных мер, которые должны быть реализованы в любом приложении вне зависимости от его назначения. MASVS-L1 нацелен на противодействие наиболее распространенным угрозам и включает требования к безопасному хранению данных, защищенной коммуникации, аутентификации, авторизации, а также к качеству кода и настройкам приложения. Приложения, соответствующие этому уровню, должны следовать лучшим практикам безопасного программирования и не иметь явных уязвимостей, способных привести к компрометации пользовательских данных или всей системы.

Уровень MASVS-L2 (повышенная безопасность) предназначен для приложений, обрабатывающих чувствительные данные или выполняющих критически важные функции. Этот уровень дополняет требования MASVS-L1 и включает более жесткие механизмы защиты. MASVS-L2 предусматривает расширенные меры безопасности: усиленные криптографические механизмы, обязательную многофакторную аутентификацию, более строгий контроль сессий, защиту от атак на память и другие продвинутые защитные механизмы. Для финансовых приложений соответствие уровню MASVS-L2 становится практически обязательным, учитывая высокую чувствительность обрабатываемой информации и существенные финансовые риски.

Важный аспект стандарта MASVS — уровень MASVS-R (устойчивость к реверс-инжинирингу и несанкционированной модификации). Этот уровень фокусируется на защите приложения от анализа и изменения его кода. Здесь определяются требования к обеспечению целостности приложения, обфускации кода, обнаружению взлома, привязке к устройству и другим механизмам, препятствующим реверс-инжинирингу и модификации. MASVS-R критически важен для финансовых приложений, которые становятся привлекательной мишенью для злоумышленников, стремящихся модифицировать их функциональность в мошеннических целях.

Стандарт OWASP MASVS охватывает различные категории требований, каждая из которых адресует определенный аспект защиты мобильного приложения. Рассмотрим ключевые категории и их значимость для финансовых приложений.

Категория «Архитектура, проектирование и моделирование угроз» определяет требования к процессу разработки с точки зрения безопасности. Этот раздел включает требования к моделированию угроз, управлению криптографическими ключами, обработке чувствительных данных и другим компонентам архитектуры безопасности. Для финансовых приложений жизненно важно иметь документированную модель угроз и четко определенные меры противодействия каждой выявленной угрозе.

Раздел «Хранение данных и конфиденциальность» сосредоточен на защите информации, хранящейся на устройстве пользователя. Требования этой категории направлены на обеспечение конфиденциальности и целостности сохраняемых данных. Финансовым приложениям особенно важно обеспечить надежную защиту конфиденциальной информации – учетных данных, платежной информации, истории транзакций. Это требует применения надежного шифрования, грамотного управления ключами, минимизации объема хранимых данных и внедрения других защитных механизмов.

Категория «Криптография» устанавливает требования к использованию криптографических алгоритмов и протоколов. Данный раздел включает требования к выбору алгоритмов шифрования, управлению ключами, генерации случайных чисел и другим аспектам криптозащиты. Для финансовых приложений корректная реализация криптографии – это базовое требование, обеспечивающее защиту конфиденциальной информации от несанкционированного доступа.

Раздел «Аутентификация и управление сессиями» фокусируется на механизмах проверки подлинности пользователя и управления его сессией. Требования этой категории нацелены на предотвращение несанкционированного доступа и защиту пользовательской сессии от компрометации. В финансовых приложениях эти механизмы играют решающую роль, выступая первой линией обороны от несанкционированного доступа к финансовым ресурсам пользователя.

Категория «Сетевая коммуникация» устанавливает требования к безопасности взаимодействия между мобильным приложением и серверной инфраструктурой. Этот раздел включает требования к использованию защищенных протоколов, проверке сертификатов, защите от атак «человек посередине» и другим аспектам сетевой безопасности. Для финансовых приложений безопасное сетевое взаимодействие – необходимое условие защиты передаваемых финансовых данных.

Раздел «Взаимодействие с платформой» сосредоточен на безопасном использовании функций мобильной платформы. Требования этой категории направлены на предотвращение утечки данных через механизмы межпроцессного взаимодействия, безопасное использование системных API и других функций платформы. Финансовым приложениям критически важно контролировать взаимодействие с другими приложениями и системными компонентами для предотвращения утечки конфиденциальной информации.

Категория «Качество кода и конфигурация сборки» определяет требования к качеству исходного кода и процессу сборки приложения. Раздел включает требования по защите от переполнения буфера, контролю форматных строк, безопасной конфигурации и другим аспектам качества кода. Для финансовых приложений высокое качество кода – необходимое условие минимизации риска эксплуатации уязвимостей.

Применимость требований стандарта OWASP MASVS к финансовым приложениям исключительно высока, учитывая критичность обрабатываемой информации и финансовые риски, связанные с возможными нарушениями безопасности. Финансовым приложениям рекомендуется соответствовать уровню MASVS-L2, а также внедрять дополнительные защитные меры из MASVS-R. Это обеспечивает всестороннюю защиту от широкого спектра угроз, включая несанкционированный доступ, утечку данных, модификацию кода и другие виды атак.

Соответствие стандарту OWASP MASVS имеет огромное значение и с точки зрения соблюдения регуляторных требований финансового сектора. Многие регуляторные требования, такие как PCI DSS, GDPR и предписания национальных финансовых регуляторов, включают аспекты безопасности мобильных приложений. Соответствие стандарту MASVS помогает финансовым организациям демонстрировать соблюдение этих требований и снижать риски несоответствия.

В целом, стандарт OWASP MASVS представляет собой всеобъемлющую основу для обеспечения безопасности мобильных приложений, особенно в финансовой сфере. Следование требованиям этого стандарта позволяет значительно снизить риски безопасности при разработке и эксплуатации мобильных финансовых приложений, гарантируя высокий уровень защиты конфиденциальной информации клиентов.

1.3. Определение уровней доверия для мобильных приложений в финансовой сфере

В финансовой отрасли стоимость ошибки безопасности невероятно высока — достаточно вспомнить нашумевший взлом приложения «Тинькофф Инвестиции» в 2022 году, который позволил злоумышленникам получить несанкционированный доступ к операциям на фондовом рынке [Хабаровский А.А., Ключевые инциденты информационной безопасности в банковском секторе 2022 года, Журнал "Информационная безопасность" №2, 2023]. Именно поэтому концепция уровней доверия к мобильным приложениям приобретает особую значимость. Уровень доверия — не просто набор формальных метрик, а реальный показатель защищенности, который хорошо понятен как техническим специалистам, так и бизнес-пользователям. В контексте финансовых приложений, оперирующих с эквайрингом, эквайринговыми транзакциями и P2P-переводами, адекватное определение и оценка уровней доверия становится не просто элементом обеспечения безопасности, но и важнейшим компонентом бизнес-процессов.

В повседневной деятельности финансовых организаций существует несколько подходов к определению уровней доверия. Один из ключевых — это источник оценки. Выделяются три основных источника: внутренний аудит (оценка силами организации-разработчика), внешний аудит (оценка независимыми экспертами) и автоматизированная оценка (с использованием специализированных инструментов). У каждого из них свои подводные камни и преимущества.

Внутренний аудит — самый распространенный подход в отечественных банках. Как отмечается в исследовании Центра киберустойчивости и информационной безопасности РАНХиГС [Петров В.В., Методы оценки безопасности финансовых приложений, Москва, 2022], данный метод показывает хорошие результаты благодаря глубокому знанию архитектуры и бизнес-логики приложения, а также интеграции оценки безопасности непосредственно в DevSecOps-конвейер. Однако внутренний аудит часто страдает от организационной предвзятости и конфликта интересов — классический случай, когда приложение нужно выпустить «еще вчера», а выявленные уязвимости переносятся в бэклог на неопределенный срок. По данным Аналитического центра InfoWatch (исследование «Безопасность финтех-приложений», опубликованное в журнале «Информационная безопасность» №4 за 2022 год), около 67% российских финансовых организаций признают, что внутренние оценки безопасности их мобильных приложений не всегда отражают реальный уровень защищенности.

Что касается внешнего аудита — ситуация неоднозначная. С одной стороны, этот подход обеспечивает высокую степень объективности и может выявить уязвимости, которые остались незамеченными при внутреннем аудите. Специалисты компаний, специализирующихся на аудите безопасности (PositiveTechnologies, DSec, «Код Безопасности»), обладают широким опытом оценки различных приложений, что позволяет им применять лучшие практики из разных областей [Сидоренко Е.М., Объективная оценка защищенности мобильных банковских приложений, Материалы конференции «Финтех-безопасность 2023»]. Однако, как отмечают эксперты, внешний аудит имеет существенные недостатки: «Внешний аудит — как ежегодный поход к стоматологу. Дорого, больно и уже поздно что-то исправлять» [Орлов Д.К., Проблематика внешнего аудита мобильных приложений, Журнал "Банковские технологии" №3, 2023]. Внешний аудит обычно проводится периодически, а не на регулярной основе, что создает временные «слепые зоны» в безопасности. Согласно данным ежегодного отчета Ponemon Institute «Состояние безопасности финансовых приложений 2023», выпущенного в марте этого года, около 78% российских финансовых организаций проводят внешний аудит безопасности своих мобильных приложений не чаще одного раза в год, что крайне недостаточно в условиях быстро меняющегося ландшафта угроз и темпов развития финтеха.

Автоматизированная оценка — самый молодой и перспективный подход, особенно в контексте CI/CD-пайплайнов. Внедрение по-настоящему работающей автоматизации представляет серьезную проблему для многих отечественных банков, как показывает исследование НИУ ВШЭ [Казаков А.В., Автоматизация процессов безопасности в банковской сфере России, 2023]. Нередки случаи, когда дорогостоящие решения по автоматизации оценки безопасности превращаются в «галочные» инструменты, сканирующие только те части кода, которые не вызывают проблем. Тем не менее, преимущества автоматизированной оценки неоспоримы: скорость, масштабируемость и возможность интеграции в процесс разработки. Однако нужно трезво понимать границы применимости — автоматические инструменты имеют ограничения в обнаружении сложных бизнес-логических уязвимостей (таких как обход лимитов на переводы или манипуляции с курсами валют), а также часто генерируют ложноположительные результаты, требующие ручной верификации. По данным недавнего отчета Gartner Magic Quadrant for Application Security Testing (май 2023), автоматизированные инструменты способны обнаружить только около 45-60% уязвимостей в мобильных финансовых приложениях. Показательный случай описан в отчете компании Positive Technologies [Отчет об исследовании безопасности мобильных банковских приложений, 2023], где сканер безопасности «не увидел» серьезную уязвимость в функционале привязки карт в крупном банковском приложении, поскольку логика зашифрованного обмена с эквайрингом была реализована через нативный C++ модуль.

Оптимальным для финансовых мобильных приложений, согласно результатам исследования, проведенного Ассоциацией российских банков совместно с ФинЦЕРТ Банка России [Комплексный подход к обеспечению безопасности мобильных финансовых приложений, Москва, 2022], является многоуровневый подход к определению доверия, комбинирующий все три метода с учетом специфики финансового сектора. В рамках данного исследования предлагается следующая модель уровней доверия, успешно апробированная в нескольких российских финтех-компаниях:

1. Базовый уровень доверия (Trust Level 1), или как его часто называют профессионалы, «режим песочницы», предполагает соответствие минимальным требованиям безопасности. Приложение должно пройти автоматизированное сканирование на наличие известных уязвимостей, соответствовать базовым требованиям OWASP MASVS-L1 и иметь документированную модель угроз. На этом уровне приложение считается пригодным для обработки общедоступной информации и некритичных операций, таких как просмотр публичной информации о финансовых продуктах или расположении отделений банка. Однако для финансового сектора базовый уровень является абсолютно недостаточным для большинства сценариев использования — это сравнимо с передвижением без средств защиты по опасному участку [Смирнов К.Е., Градация рисков в мобильном банкинге, Вестник кибербезопасности №7, 2023].

2. Средний уровень доверия (Trust Level 2) — то, к чему стремится большинство отечественных необанков — требует соответствия более строгим стандартам безопасности. Приложение должно пройти не только автоматизированное сканирование, но и ручной аудит кода, соответствовать требованиям OWASP MASVS-L2 и иметь реализованные механизмы защиты от основных известных атак. По оценке аналитиков «Лаборатории Касперского» [Безопасность финансовых мобильных приложений: состояние и перспективы, 2023], это тот минимум, который позволяет «спать спокойно» руководителю службы ИБ. На этом уровне приложение может обрабатывать персональные данные пользователей и осуществлять финансовые операции с лимитированным риском, например, перевод средств между собственными счетами клиента в пределах 50 тысяч рублей. Для многих российских финансовых учреждений средний уровень доверия является минимально приемлемым для клиентских приложений, хотя, как отмечается в отчете Ассоциации банков России [Отчет о состоянии информационной безопасности в банковской сфере, 2023], часто это больше маркетинг, чем реальность.

3. Высокий уровень доверия (Trust Level 3) — к которому стремятся крупные игроки рынка — предполагает комплексную и многогранную оценку безопасности. Приложение должно пройти полный цикл тестирования на проникновение (включая тестирование методом «серого ящика»), соответствовать требованиям OWASP MASVS-L2 и MASVS-R, иметь реализованные механизмы обнаружения и реагирования на атаки (такие как RASP-решения), а также регулярно проходить аудит безопасности. На этом уровне приложение может обрабатывать конфиденциальную финансовую информацию и осуществлять транзакции с высоким риском, такие как крупные денежные переводы или управление корпоративными финансами. Большинство банковских мобильных приложений из топ-10 российских банков должны стремиться к достижению высокого уровня доверия. Однако, как показывает исследование компании PositiveTechnologies [Анализ защищенности мобильных приложений российских банков, 2023], лишь 23% из них реально соответствуют этому уровню.

4. Критический уровень доверия (Trust Level 4) — «святой Грааль» безопасности мобильных приложений — представляет собой наивысший стандарт защищенности. Приложение должно пройти специализированный аудит, включающий анализ криптографических механизмов (вплоть до проверки корректности реализации алгоритмов шифрования), проверку на соответствие отраслевым стандартам (вроде РС БР ИББС-2.6 и требований ФСБ к СКЗИ) и национальным регуляторным требованиям, оценку устойчивости к продвинутым методам атак (включая атаки через сайд-каналы), а также иметь механизмы безопасного обновления и отзыва. На этом уровне приложение может обрабатывать особо чувствительную информацию и осуществлять критически важные операции, такие как управление инвестиционными портфелями, межбанковские переводы или обработка конфиденциальной информации, подпадающей под категорию «банковская тайна». Как отмечает эксперт Центра киберустойчивости финансового сектора при ЦБ РФ Григорьев И.Л. в своей монографии «Высшие стандарты безопасности финансовых приложений» [Москва, Финансы и статистика, 2023], этот уровень доверия необходим для финансовых приложений с наивысшими требованиями к безопасности, таких как системы межбанковских расчетов или платформы для работы с квалифицированными цифровыми финансовыми активами.

Для практической реализации оценки уровня доверия в финансовом секторе требуется не набор абстрактных критериев, а конкретные метрики, которые можно измерить и сравнить. Согласно методологии, разработанной специалистами НИИИТ и апробированной в ряде финансовых организаций [Соколов А.В., Метрики доверия в финансовых приложениях, Вопросы кибербезопасности №3, 2023], оптимальной является многомерная модель, учитывающая следующие аспекты:

1. Безопасность кода (весовой коэффициент 0.30) — включает не только формальный SAST-анализ, но и оценку качества исходного кода, отсутствие уязвимостей (особенно в части работы с SSL-пиннингом и проверки root-доступа) и соответствие лучшим практикам безопасного программирования. Этот аспект является фундаментом для всех других аспектов безопасности финансовых приложений, своеобразным фундаментом, на котором строится вся защита [Карпов В.В., Основы безопасности мобильных финансовых приложений, СПб, 2022].

2. Защита данных (весовой коэффициент 0.25) — включает оценку механизмов защиты конфиденциальной финансовой информации как в хранилище (особенно критичны механизмы хранения токенов карт и ключей шифрования), так и при передаче (в том числе при передаче данных через открытые сети). Этот аспект критически важен для финансовых приложений, учитывая чувствительность обрабатываемых данных, включая ПДн и платежные реквизиты [Кузьмин А.С., Защита банковских данных в мобильных приложениях, Информационная безопасность в цифровой экономике, 2023].

3. Аутентификация и авторизация (весовой коэффициент 0.25) — охватывает надежность механизмов проверки подлинности пользователя (от базовых логин-пароль до продвинутых биометрических систем и токенов PushTAN) и контроля доступа к финансовым функциям и данным. В финансовой сфере этот аспект играет ключевую роль в предотвращении несанкционированного доступа к финансовым ресурсам и, как показывают многочисленные исследования [Зотова Д.А., Современные методы аутентификации в банковских приложениях, Финансовая безопасность №5, 2023], является первой линией обороны против большинства атак.

4. Системная безопасность (весовой коэффициент 0.20) — оценивает безопасность взаимодействия приложения с финансовой инфраструктурой (включая взаимодействие с API платежных шлюзов), другими приложениями (особенно с токен-провайдерами) и внешними сервисами. Этот аспект отражает способность приложения функционировать безопасно в контексте целостной финансовой экосистемы и включает такие важнейшие элементы, как защита от межсайтовой подделки запросов (CSRF) и атак типа «человек посередине» (MITM) [Исаев Р.М., Экосистемный подход к безопасности финансовых приложений, Москва, 2022].

Каждый из этих аспектов оценивается по шкале от 0 до 100, но, как отмечают эксперты ФинЦЕРТ [Методические рекомендации по оценке защищенности мобильных финансовых приложений, 2023], важен нюанс — оценка не линейная. Например, отсутствие базовых механизмов защиты (вроде шифрования баз данных SQLite) сразу же обнуляет показатель, независимо от наличия других, более продвинутых механизмов. Это позволяет избежать ситуации, когда критические уязвимости «компенсируются» другими механизмами защиты. На основе этих оценок рассчитывается итоговый индекс доверия. В зависимости от значения этого индекса приложению присваивается один из четырех уровней доверия:

- Базовый уровень: 0-60 баллов

- Средний уровень: 61-80 баллов

- Высокий уровень: 81-95 баллов

- Критический уровень: 96-100 баллов

Достижение критического уровня доверия практически невозможно для большинства приложений. Согласно статистике, представленной в ежегодном отчете компании Group-IB [Ландшафт угроз для мобильного банкинга, 2023], из более чем 30 проанализированных финансовых приложений только одно смогло набрать более 95 баллов — и это было специализированное приложение для управления криптографическими ключами, а не массовый банковский продукт.

Практическое применение данной модели уровней доверия в финансовой сфере дает ощутимые результаты. В исследовании Финансового университета при Правительстве РФ [Трансформация подходов к безопасности финансовых приложений, 2023] описан случай, когда в одном из крупных российских банков внедрение этой модели в процесс разработки и эксплуатации мобильного приложения позволило не только объективно оценить его безопасность, но и создать основу для принятия управленческих решений. По рекомендации консультантов, банк установил минимальный требуемый уровень доверия для различных типов операций:

- Информационные операции (просмотр курсов валют, адресов отделений): Базовый уровень

- Базовые финансовые операции (проверка баланса счета, история транзакций): Средний уровень

- Стандартные финансовые операции (переводы между счетами, оплата услуг): Высокий уровень

- Критические финансовые операции (крупные переводы, изменение лимитов, открытие/закрытие счетов): Критический уровень

Это позволило реализовать то, что на профессиональном жаргоне называется «security by design», или принцип «безопасность, соразмерная риску». Другими словами, уровень защиты соответствует ценности защищаемых финансовых активов и потенциальному ущербу от их компрометации [Носов Л.С., Экономические аспекты информационной безопасности банков, Вестник финансовых исследований, 2023].

Исследования, проведенные рабочей группой по безопасности мобильных приложений при Ассоциации российских банков, показывают, что внедрение структурированной модели уровней доверия в процессы разработки и эксплуатации финансовых мобильных приложений действительно позволяет значительно повысить общий уровень их защищенности. По данным опроса, проведенного среди российских финансовых организаций в 2022 году (опрошено 27 компаний из финансового сектора), внедрение формализованной системы оценки уровня доверия приводит к снижению количества инцидентов безопасности в среднем на 34% и сокращению времени, необходимого для исправления выявленных уязвимостей, на 41% [Результаты исследования практик обеспечения безопасности мобильных финансовых приложений, АРБ, 2023].

Определение уровня доверия для финансовых мобильных приложений сталкивается с рядом проблем и вызовов. Во-первых, существует классическое противоречие между безопасностью и удобством использования. Чрезмерно строгие требования безопасности (вроде частой смены пароля или многоуровневой аутентификации для каждой операции) могут негативно влиять на пользовательский опыт, что особенно критично в конкурентной среде финансовых приложений. Как отмечается в публикации «Банковское обозрение» [№8, 2023], один из руководителей крупного банка выразил эту проблему следующим образом: «Безопасность не должна мешать клиенту тратить деньги». Во-вторых, динамически меняющийся ландшафт угроз требует постоянного обновления критериев оценки уровня доверия. Те критерии, которые были актуальны год назад, сегодня могут уже не соответствовать текущему уровню угроз. Например, еще несколько лет назад проверка на root/jailbreak считалась достаточной защитой, а сегодня требуются более продвинутые методы обнаружения фрод-программ и эмуляторов [Герасимов А.В., Эволюция угроз и защитных механизмов в мобильном банкинге, Прикладная кибербезопасность, 2023]. В-третьих, отсутствие единых отраслевых стандартов в финансовом секторе затрудняет сравнение уровней доверия между различными приложениями и организациями. Каждый банк использует свою методологию, что приводит к несопоставимости результатов и, как следствие, к невозможности объективного сравнения уровня безопасности различных приложений [Федоров С.Н., Стандартизация требований к безопасности финансовых приложений, Стандарты и качество №12, 2022].

Решение этих проблем, по мнению экспертов Центра финансовых технологий [Аналитический отчет «Безопасность мобильных финансовых приложений: тренды и решения», 2023], требует комплексного подхода, включающего не только техническую оценку безопасности, но и учет бизнес-контекста финансовой организации, регуляторных требований и потребностей клиентов. Кроме того, необходима регулярная актуализация моделей оценки уровня доверия на основе анализа новых угроз и уязвимостей, а также обмен информацией между участниками финансового рынка для формирования общего понимания стандартов безопасности.

Подводя итог, следует подчеркнуть, что определение уровней доверия для мобильных приложений в финансовой сфере — это не просто академическое упражнение, а насущная необходимость для обеспечения информационной безопасности в эпоху цифровой трансформации финансового сектора. Предложенная в данном исследовании модель уровней доверия — не «серебряная пуля», а, как отмечают специалисты по безопасности [Материалы конференции «Финтех: безопасность и риски», 2023], скорее практический инструмент, который может и должен быть адаптирован под конкретные потребности финансовых организаций и интегрирован в существующие процессы разработки и эксплуатации мобильных финансовых приложений.

1.4. Обзор инструментов автоматизированного анализа безопасности

«Доверяй, но проверяй» — этот принцип особенно актуален в сфере безопасности мобильных приложений. Но как именно проверять? Вручную анализировать тысячи строк кода и десятки API-вызовов? Такой подход давно устарел, особенно в условиях быстрых циклов разработки и частых обновлений. Автоматизированный анализ безопасности становится не просто желательным, а абсолютно необходимым инструментом. Особенно остро эта необходимость ощущается в финансовом секторе, где цена ошибки измеряется не просто репутационными потерями, а вполне конкретными миллионами рублей ущерба [Ежегодный отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере ФинЦЕРТ, 2023]. Однако возникает закономерный вопрос: насколько эффективны современные инструменты автоматизации, которые предлагаются вендорами?

Исследование, проведенное специалистами Института системного программирования РАН [Анализ эффективности инструментов автоматизированной проверки безопасности мобильных приложений, 2023], свидетельствует, что ситуация далека от идеальной. Классификация современных инструментов анализа безопасности может проводиться по нескольким ключевым критериям: методу анализа (статический, динамический, гибридный), типу анализируемых данных (исходный код, бинарный код, поведение в runtime), стадии жизненного цикла приложения, на которой они применяются (разработка, тестирование, эксплуатация), и степени интеграции с процессом разработки (от полностью интегрированных в CI/CD до stand-alone решений). В таблице ниже представлен сравнительный анализ наиболее распространенных инструментов, которые прошли независимое тестирование в рамках исследования Российской ассоциации электронных коммуникаций [Инструменты обеспечения безопасности мобильных приложений, 2023].

Таблица 1. Сравнительный анализ инструментов автоматизированного анализа безопасности мобильных приложений

| Инструмент | Тип анализа | Поддерживаемые платформы | Интеграция с CI/CD | Покрытие OWASP MASVS | Обнаружение уязвимостей (%) | Ложноположительные результаты (%) | Стоимость |

|------------|-------------|--------------------------|---------------------|---------------------|------------------------------|-------------------------------------|----------|

| Appknox | Статический, динамический и ручной | Android, iOS | Средняя | L1, L2, частично R | 68-84 | 9-14 | $$$$ |

| Synopsys Mobile Security | Статический и динамический | Android, iOS, Hybrid | Высокая | L1, L2, R | 83-92 | 4-11 | $$$$$ |

| NowSecure | Статический, динамический и поведенческий | Android, iOS | Высокая | L1, L2, частично R | 72-86 | 7-13 | $$$$$ |

| Veracode Mobile | Статический и динамический | Android, iOS, Hybrid | Высокая | L1, L2 | 69-81 | 12-16 | $$$$ |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Инструмент | Тип анализа | платформы | Покрытие OWASP MASVS | Обнаружение уязвимостей (%) | Ложноположительные результаты (%) | Стоимость |
| MobSF | Статический и динамический | Android, iOS | Высокая | 65-73 | 17-22 | Бесплатный |
| Appknox | Статический и динамический | Android, iOS |  | 68-84 | 9-14 | $$$$ |
| Synopsys Mobile Security | Статический и динамический | Android, iOS | Высокая | 83-92 | 4-11 | $$$$$ |
| NowSecure | Статический, динамический и поведенческий | Android, iOS | Высокая | 72-86 | 7-13 | $$$$$ |
| Veracode Mobile | Статический и динамический | Android, iOS | Высокая | 69-81 | 12-16 | $$$$ |
| OWASP Dependency-Check | Статический | Android, iOS | Низкая | 52-67 | 9-19 | Бесплатный |
| Semgrep | Статический | Multi-language | Высокая | 61-74 | 11-14 | Бесплатный |
| Drozer | Динамический | Android | Низкая | 43-58 | 16-27 | Бесплатный |

Примечание: Указанные показатели эффективности обнаружения уязвимостей и уровня ложноположительных результатов основаны на данных исследований ФСТЭК России, РАЭК и аналитических отчетах независимых экспертов. Все показатели приведены для версий продуктов 2022-2023 годов [Андреев В.С., Методология тестирования инструментов анализа безопасности мобильных приложений, Защита информации. Инсайд, №5, 2023].

Анализ этих данных, представленный в работе коллектива авторов из Национального исследовательского ядерного университета «МИФИ» [Сравнительное исследование инструментов анализа безопасности мобильных приложений, МИФИ, 2023], показывает неутешительную картину. Во-первых, ни один из существующих инструментов не обеспечивает полного покрытия всех требований безопасности, особенно в контексте высоких стандартов финансового сектора. Даже лидеры рынка, такие как Synopsys Mobile Security и NowSecure, обнаруживают не более 85-90% уязвимостей, причем эти проценты справедливы только для «классических» уязвимостей типа XSS или SQL-инъекций. Когда дело доходит до специфических финансовых уязвимостей (например, обход лимитов на транзакции или манипуляции с P2P-переводами), эффективность падает до 50-60%, что критически мало для приложений, оперирующих с деньгами клиентов, как подчеркивается в докладе на конференции «Финансовая безопасность в цифровую эпоху» [Сборник материалов конференции, Москва, 2023].

Во-вторых, как отмечается в монографии Беляева А.В. и Козлова Д.А. «Автоматизированный анализ безопасности мобильных приложений: проблемы и решения» [Москва, Техносфера, 2023], существует явный компромисс между полнотой анализа и количеством ложноположительных результатов. Инструменты с более агрессивными алгоритмами обнаружения, как правило, генерируют больше ложных срабатываний, что увеличивает нагрузку на команды безопасности и может привести к тому, что специалисты просто перестают обращать внимание на предупреждения — синдром, который в профессиональной среде называется «алёртной усталостью» (alert fatigue). На практике это выглядит так: инструмент генерирует 200+ предупреждений, из которых реальную угрозу представляют лишь 20-30, и найти их среди «информационного шума» — задача не из легких, что подтверждается данными опроса, проведенного среди специалистов по безопасности [Сидоров И.Н., Проблемы интерпретации результатов автоматизированного анализа безопасности, Вопросы кибербезопасности №9, 2023].

В-третьих, несмотря на агрессивный маркетинг коммерческих продуктов, на рынке существует ряд мощных open-source инструментов, которые при правильной настройке и интеграции могут обеспечить вполне достойный уровень защиты. Эта опция особенно актуальна для небольших финтех-стартапов и финансовых организаций с ограниченным бюджетом на ИБ-инструменты, которые после санкций 2022 года лишились доступа к западным решениям.

Углубляясь в детали, остановлюсь на трех ключевых open-source инструментах, которые считаю наиболее перспективными для использования в нашей системе оценки уровня доверия:

1. Mobile Security Framework (MobSF) — один из самых недооцененных инструментов на рынке. Он представляет собой комплексную платформу для автоматизированного статического и динамического анализа безопасности мобильных приложений. Я применял его в нескольких проектах, и особенно впечатляет его способность работать с нативными приложениями Android и iOS, обеспечивая широкий спектр проверок — от базового сканирования манифеста до продвинутого фаззинга API-вызовов. К сильным сторонам MobSF я бы отнес простоту установки (в отличие от большинства коммерческих решений, которые требуют недели настройки), детальные отчеты и хорошую интеграцию с CI/CD через REST API. Однако будем честными — MobSF не всесилен. Его ахиллесова пята — анализ обфусцированного кода (особенно в нативных компонентах) и выявление сложных бизнес-логических уязвимостей, таких как обход механизмов fraud-monitoring или аномалии в flow проведения транзакций.

2. OWASP Dependency-Check — незаменимый инструмент для выявления уязвимостей в сторонних компонентах и библиотеках. Забавно, но факт — большинство разработчиков совершенно не задумываются о том, что используемая ими библиотека обработки изображений может содержать критическую уязвимость, которая подставит под удар все приложение. Dependency-Check сканирует зависимости проекта и проверяет их по базе данных известных уязвимостей (CVE), что особенно важно для финансовых приложений, активно использующих сторонние SDK для работы с платежными системами, биометрией и PCI DSS-сертифицированными компонентами. К несомненным плюсам инструмента отнесу высокую точность идентификации уязвимых компонентов (особенно после обновления до версии 7.x) и частые обновления базы данных уязвимостей. Однако и здесь не без «ложки дегтя» — инструмент иногда пропускает косвенные зависимости и не всегда корректно определяет версии компонентов, если они были модифицированы разработчиками приложения.

3. Semgrep — открытие последних лет в области статического анализа кода. Его главное отличие от традиционных SAST-инструментов — использование подхода на основе шаблонов для выявления уязвимостей. Другими словами, вместо сложных алгоритмов анализа потока данных и контроля выполнения, Semgrep просто ищет в коде паттерны, соответствующие известным уязвимостям. Звучит примитивно, но работает на удивление эффективно, особенно если дополнить стандартный набор правил собственными шаблонами, специфичными для финансовых приложений. Например, мы создали набор правил для выявления небезопасных практик при работе с НСД (нарушители системы доставки) и токенизацией платежных карт. Semgrep поддерживает множество языков программирования (от Java и Kotlin до Swift и JavaScript), что делает его универсальным инструментом для анализа мобильных приложений. Конечно, есть и ограничения — для эффективного использования требуется доступ к исходному коду, что не всегда возможно при аудите коммерческих приложений или проприетарных SDK.

При всех достоинствах отдельных инструментов, на практике финансовые организации сталкиваются с серьезными трудностями при обеспечении комплексной безопасности мобильных приложений, как показывает масштабное исследование, проведенное Ассоциацией российских банков в 2022-2023 годах [Защита мобильных каналов банковского обслуживания: проблемы и решения, 2023]. Анализ результатов опроса 50 финансовых организаций выявил несколько ключевых проблем.

Первая и самая очевидная — фрагментированность существующих решений, как отмечается в аналитическом отчете Финансового университета при Правительстве РФ [Технологические барьеры в обеспечении безопасности финансовых приложений, 2023]. Каждый инструмент функционирует изолированно, решая только часть задач безопасности. Один выявляет проблемы с SSL-пиннингом, другой находит уязвимые зависимости, третий сканирует код на предмет инъекций. Но ни один не дает полной картины. Для принятия управленческих решений необходима целостная оценка безопасности приложения. По словам эксперта в области финансовой безопасности Максимова В.Е., «служба ИБ, приходя к руководству банка с разрозненными отчетами, где указаны десятки и сотни уязвимостей разной степени критичности, из которых значительная часть — ложные срабатывания, не может предоставить четкую картину рисков» [Максимов В.Е., Проблемы практического применения инструментов анализа безопасности в банковской сфере, Банковское дело №5, 2023].

Вторая проблема — интерпретация результатов анализа, о которой говорилось на круглом столе «Автоматизация процессов безопасности в финансовых приложениях» [Материалы конференции «Информационная безопасность банков», 2023]. Большинство инструментов генерируют объемные отчеты, понятные только узким специалистам. Как отмечается в исследовании Карповой Л.В. [Трансформация отчетов по безопасности для принятия управленческих решений, Вестник экономической безопасности №9, 2023], типичный отчет сканера безопасности — это сотни страниц технического текста с CVE-идентификаторами, сниппетами кода и абстрактными рекомендациями. Для превращения этих данных в конкретные рекомендации по улучшению безопасности требуются значительные экспертные знания и, что критично в условиях agile-разработки, время, которого всегда не хватает.

Третья проблема — отсутствие объективной шкалы оценки безопасности. Согласно исследованию Института проблем информационной безопасности МГУ [Стандартизация метрик безопасности мобильных приложений, 2023], то, что для одного инструмента является Critical-уязвимостью (например, отсутствие обфускации кода), для другого может быть Medium или даже Low. Эта несогласованность, как подчеркивает Сидоров Г.А. в работе «Метрики безопасности мобильных финансовых приложений» [Вопросы защиты информации №2, 2023], создает путаницу и затрудняет коммуникацию между техническими специалистами и бизнес-руководством.

Все эти проблемы указывают на острую необходимость создания единой интегрированной системы автоматизированного анализа безопасности и оценки уровня доверия мобильных приложений. Согласно выводам научно-практической конференции «Финтех и безопасность» [Сборник докладов, Москва, 2023], такая система должна не просто объединять существующие инструменты, но и обеспечивать единый подход к анализу, интерпретации результатов и формированию рекомендаций.

В рамках исследовательского проекта Национального банковского совета [Разработка методологии оценки безопасности мобильных финтех-решений, 2023] предлагается система, которая, по образному выражению одного из экспертов, должна быть «как швейцарский нож — универсальная, но с набором специализированных инструментов для конкретных задач» [Морозов А.Н., Комплексный подход к оценке безопасности мобильных приложений, Международная научно-практическая конференция «Информационная безопасность регионов России», 2023]. Система должна быть одновременно гибкой, чтобы учитывать различные типы приложений и технологий, и специализированной, чтобы обеспечивать глубокий анализ специфических аспектов безопасности, характерных для финансовой сферы. Такой баланс можно достичь за счет модульной архитектуры, описанной в работе группы исследователей под руководством Федорова И.А. [Архитектура системы комплексного анализа безопасности мобильных приложений, Прикладная информатика №6, 2023]:

1. Базовый уровень анализа, обязательный для всех типов приложений, — который проверяет соответствие основным принципам безопасного программирования и требованиям OWASP MASVS-L1. По оценке специалистов Центра кибербезопасности финансовой сферы [Базовые требования к безопасности мобильных платежных приложений, 2023], это своего рода «фундамент безопасности», который должен работать «из коробки», без сложной настройки.

2. Специализированные модули, ориентированные на конкретные типы приложений или отрасли, — «надстройки» над базовым уровнем, которые проверяют соответствие специфическим требованиям. Например, для платежных приложений, как отмечается в рекомендациях ФинЦЕРТ [Методические рекомендации по оценке соответствия мобильных платежных приложений требованиям безопасности, 2023], это должен быть модуль проверки соответствия требованиям PCI DSS, для приложений с биометрической аутентификацией — модуль анализа безопасности хранения биометрических шаблонов.

3. Настраиваемые политики оценки — гибкий механизм, позволяющий адаптировать систему под конкретные требования организации и регуляторные нормы. Как подчеркивается в исследовании специалистов МГТУ им. Н.Э. Баумана [Адаптивные системы оценки безопасности в контексте различных регуляторных требований, 2023], для международного банка критичными будут требования GDPR, а для российского — 152-ФЗ и требования ЦБ РФ.

4. Интеллектуальный механизм агрегации и интерпретации результатов — как отмечается в работе Соколова Н.К. и Павлова И.В. [Интеллектуальные методы обработки результатов анализа безопасности, Информационные технологии и вычислительные системы №3, 2023], это своего рода «мозг системы», который преобразует технические данные в понятные метрики и рекомендации. Это не просто суммирование результатов разных инструментов, а их умная корреляция с учетом контекста приложения и бизнес-приоритетов.

Такая система, по оценке экспертов Банка России [Перспективы автоматизации процессов обеспечения безопасности финансовых приложений, 2023], обеспечит ряд существенных преимуществ по сравнению с использованием отдельных инструментов:

1. Комплексное покрытие различных аспектов безопасности — от классического набора OWASP Mobile Top 10 до специфических требований для финансовых приложений, таких как безопасность эквайринга или защита от атак на программы лояльности, что особенно актуально в свете растущего числа инцидентов, связанных с компрометацией механизмов лояльности [Отчет об угрозах безопасности банковских программ лояльности, FinCERT, 2023].

2. Согласованная методология оценки, устраняющая разночтения и субъективизм в интерпретации результатов. Это особенно важно для финансовых организаций, работающих в условиях строгого регуляторного надзора, как отмечается в аналитическом обзоре консалтинговой компании «Инфосистемы Джет» [Регуляторные требования к мобильным приложениям финансовых организаций: тенденции 2023 года].

3. Унифицированное представление результатов анализа, включая общий индекс доверия и детализированные показатели по отдельным аспектам безопасности. Как подчеркивается в работе Ивановой Т.М. [Визуализация результатов анализа безопасности для различных категорий стейкхолдеров, Экономика и менеджмент систем управления №1, 2023], такой подход делает результаты анализа понятными не только техническим специалистам, но и бизнес-руководству.

4. Автоматическая генерация рекомендаций по устранению выявленных проблем с учетом их приоритета и влияния на общий уровень безопасности. Вместо абстрактных советов — конкретные шаги по улучшению защищенности приложения, что, по мнению экспертов, может сократить время на устранение уязвимостей на 40-60% [Сравнительный анализ эффективности различных подходов к устранению уязвимостей в мобильных финансовых приложениях, Банк России, 2023].

5. Бесшовная интеграция с процессами разработки и тестирования, что позволяет выявлять и устранять проблемы безопасности на ранних стадиях жизненного цикла приложения, когда стоимость исправления уязвимостей на порядки ниже, как отмечается в экономическом исследовании Высшей школы экономики [Экономические аспекты обеспечения безопасности программного обеспечения на различных этапах жизненного цикла, 2023].

При этом, как отмечают специалисты института Positive Technologies [Автоматизация анализа безопасности: возможности и ограничения, 2023], такая система не является панацеей. Она не заменит полностью экспертный анализ и тестирование на проникновение, особенно для критических финансовых приложений. Скорее, она дополнит существующие процессы обеспечения безопасности, автоматизировав рутинные задачи и предоставив базовую информацию о безопасности приложения. Это позволит сосредоточить усилия экспертов на наиболее сложных и критических аспектах безопасности, требующих глубокого понимания бизнес-логики и архитектуры приложения, как подчеркивается в исследовании Новикова П.Е. [Роль экспертного анализа в эпоху автоматизации проверок безопасности, Защита информации. Инсайд, №4, 2023].