Security Engineering: часть 6. Финансовые системы

Published: 09.06.2026 22:18 | Updated: 15.06.2026 22:24

Банковское дело и бухгалтерский учет: почему безопасность — это не только криптография

В предыдущих частях основной акцент делался на **конфиденциальности**, то здесь в центре внимания оказываются две другие фундаментальные характеристики безопасности: **целостность** (integrity) и **подотчетность** (accountability).
Банковская система должна гарантировать, что деньги невозможно создать из воздуха, удалить без следа или переместить незаметно. Каждая операция должна быть проверяемой, а любое изменение состояния системы — иметь документированное основание.
Главная идея этой статьи заключается в том, что безопасность финансовых систем определяется не только криптографическими механизмами. Не менее важную роль играют бухгалтерские принципы, организационные процессы, экономические стимулы и распределение ответственности между участниками системы.

Бухгалтерия как основа информационной безопасности

История банковской безопасности началась задолго до появления компьютеров и криптографии. Одним из важнейших изобретений в этой области стала система **двойной бухгалтерской записи** (double-entry bookkeeping), появившаяся еще в эпоху Возрождения.
Ее основной принцип предельно прост: каждому дебету должен соответствовать

равнозначный кредит. Любая финансовая операция затрагивает как минимум два счета, а сумма изменений всегда остается сбалансированной.
Например, при переводе 100 долларов со счета A на счет B происходит:

- списание 100 долларов со счета A;
- зачисление 100 долларов на счет B.

Общая сумма денег в системе остается неизменной.
Этот механизм оказался настолько эффективным для поддержания целостности данных, что спустя несколько столетий лег в основу формальных моделей компьютерной безопасности.

Модель Кларка—Уилсона: формализация финансовой целостности

В 1987 году Дэвид Кларк и Дэвид Уилсон предложили модель безопасности, ориентированную не на сохранение секретности данных, а на обеспечение их корректности.
В отличие от модели Белла—ЛаПадулы, которая предназначена для защиты конфиденциальной информации и использует уровни допуска, модель Кларка—Уилсона концентрируется на поддержании **корректного состояния системы** посредством контролируемых транзакций.
Основу модели составляют четыре ключевых элемента.

Компонент	Назначение	Пример в банковской системе
UDI (Unconstrained Data Items)	Непроверенные данные, поступающие извне	Сумма перевода и номер счета, введенные клиентом
CDI (Constrained Data Items)	Данные, целостность которых должна строго поддерживаться	Балансы счетов, журналы транзакций
TP (Transformation Procedures)	Единственный допустимый способ изменения CDI	Процедура банковского перевода
IVP (Integrity Verification Procedures)	Проверка корректности состояния системы	Сверка дебетов и кредитов

Центральный принцип модели заключается в том, что пользователи не могут напрямую изменять критически важные данные.
Клиент не имеет возможности самостоятельно увеличить баланс своего счета. Вместо этого он инициирует выполнение **процедуры преобразования** (TP), которая:

1. Проверяет полномочия пользователя.
2. Валидирует входные данные.
3. Контролирует соблюдение бизнес-правил.
4. Выполняет допустимые изменения.
5. Фиксирует результат в журнале аудита.

Таким образом, защищаются не отдельные данные, а **инварианты системы** — фундаментальные правила, которые никогда не должны нарушаться.
Для банков главным инвариантом остается принцип двойной записи: сумма всех дебетов должна быть равна сумме всех кредитов.

Внутренний контроль: защита от инсайдеров

Одним из наиболее важных выводов статьи является то, что крупнейшие финансовые потери банки зачастую несут не из-за внешних атак, а вследствие действий собственных сотрудников.
Даже идеально реализованная криптография не способна предотвратить злоупотребления, если внутри организации отсутствуют эффективные механизмы контроля.

Выделим два фундаментальных принципа.

Двойной контроль (Dual Control)

Для выполнения критически важных операций требуется участие нескольких сотрудников.
Например:

- выпуск мастер-ключей;
- авторизация крупных денежных переводов;
- доступ к хранилищам ключевой информации;
- выполнение административных операций в HSM.

Ни один сотрудник не должен обладать возможностью единолично осуществить высокорисковое действие.

Функциональное разделение обязанностей (Functional Separation)

Различные этапы одной операции должны выполняться разными сотрудниками. Например:

- один сотрудник инициирует платеж;
- второй подтверждает его;
- третий выполняет сверку и аудит.

Такой подход существенно снижает вероятность мошенничества и уменьшает риск ошибок.

Prevent – Detect – Recover: реалистичная модель защиты

Абсолютно безопасных систем не существует. Поэтому финансовые организации строят защиту вокруг трех взаимодополняющих механизмов:

Prevent (Предотвращение)

Меры, направленные на недопущение инцидентов:

- разграничение прав доступа;
- многофакторная аутентификация;
- разделение обязанностей;
- криптографическая защита.

Detect (Обнаружение)

Механизмы выявления нарушений:

- журналы аудита;
- мониторинг транзакций;
- сверка бухгалтерских записей;
- системы обнаружения мошенничества.

Recover (Восстановление)

Способы минимизации последствий:

- возврат ошибочных транзакций;

- страхование финансовых рисков;
- резервное копирование;
- процедуры реагирования на инциденты.

Практика показывает, что предотвратить все атаки невозможно. Поэтому способность быстро обнаруживать нарушения и восстанавливать нормальное состояние системы часто оказывается важнее абсолютной защиты.

Внутренние мошенничества и «подвешенные счета»

Показательный пример злоупотреблений, связанных со счетами невыясненных операций (suspense accounts).
Такие счета используются для временного размещения транзакций, требующих дополнительной проверки.
Схема мошенничества выглядела следующим образом:

1. Сотрудник инициировал фиктивный перевод.
2. Средства временно размещались на счете невыясненных операций.
3. Сообщник успевал снять деньги.
4. До начала обязательной проверки транзакция отменялась.

Поскольку аудит проводился через несколько дней после возникновения подозрительной операции, мошенники использовали это временное окно для сокрытия своих действий.
Подобные инциденты демонстрируют важный принцип: безопасность определяется не только техническими средствами, но и качеством организационных процедур.
Даже безупречная криптографическая защита оказывается бесполезной, если злоумышленник способен воспользоваться недостатками бизнес-процессов.

Банкоматы: первое массовое применение криптографии

Появление банкоматов стало одним из первых примеров широкого внедрения криптографических технологий в повседневную жизнь. До этого средства защиты информации в основном использовались государственными структурами и военными организациями.
Банкоматы поставили перед банками новую задачу: необходимо было

предоставить клиентам удаленный доступ к счетам, не раскрывая секретную информацию и минимизируя риск мошенничества.
Главным элементом аутентификации стал **PIN-код** (Personal Identification Number).
Однако распространенное представление о том, что PIN хранится непосредственно на карте или в открытом виде в банковской базе данных, неверно.
Банковские системы были спроектированы таким образом, чтобы даже сотрудники банка не могли получить доступ к PIN-кодам клиентов.

Как генерируется PIN: система IBM 3624

Одним из наиболее влиятельных решений стала система управления PIN-кодами, разработанная компанией IBM для банкоматов серии **IBM 3624**.
Ее ключевая особенность заключалась в том, что PIN не хранился в базе данных в явном виде.
Процесс выглядел следующим образом:

1. Брался номер карты (**PAN — Primary Account Number**).
2. PAN шифровался с использованием специального ключа проверки PIN (**PIN Verification Key**, PVK).
3. Из результата шифрования извлекались определенные цифры.
4. Полученная последовательность становилась так называемым **естественным PIN-кодом** (Natural PIN).
   Например:

```
PAN → Шифрование с использованием PVK → 4827316942...
                                    ↓
                            Natural PIN = 4827
```

Таким образом, банк мог повторно вычислить PIN при проверке, не сохраняя его в явном виде.

PIN Offset: возможность выбора PIN клиентом

Большинство людей предпочитают использовать легко запоминающиеся комбинации: даты рождения, простые последовательности или другие значимые числа.

Чтобы позволить клиенту самостоятельно выбирать PIN-код, была введена концепция **PIN Offset**.
Предположим:

- Естественный PIN: 4827
- PIN, выбранный клиентом: 1357

Система вычисляет разницу между ними по модулю 10:

```
4827
1357
————
7530
```

Полученное значение (7530) сохраняется в базе данных как **offset**.
Во время проверки происходит обратный процесс:

1. Вычисляется естественный PIN.
2. К нему применяется offset.
3. Полученный результат сравнивается с PIN, введенным клиентом.

Такой подход обеспечивает сразу несколько преимуществ:

- реальные PIN-коды не хранятся в базе данных;
- клиенты могут выбирать удобные комбинации;
- компрометация базы данных offset не раскрывает PIN напрямую.

Аппаратные модули безопасности (HSM)

Для защиты криптографических ключей банки используют **Hardware Security Modules (HSM)** — специализированные аппаратные устройства, предназначенные для выполнения криптографических операций.
Основные функции HSM:

- генерация ключей;
- хранение мастер-ключей;
- проверка PIN-кодов;
- вычисление криптографических кодов;
- выполнение операций шифрования и дешифрования.

Ключевой принцип работы HSM заключается в том, что **секретные ключи никогда не покидают устройство в открытом виде**.
Даже администраторы системы не должны иметь возможности извлечь их напрямую.
Однако отметим важную проблему: сложность интерфейсов таких устройств.
Многие HSM предоставляют десятки или даже сотни криптографических команд.
Ошибки в проектировании API могут привести к ситуациям, когда злоумышленник, не имея прямого доступа к ключам, способен отправить специально подобранную последовательность команд и получить критически важную информацию.
Это еще раз подчеркивает важный инженерный принцип:

> Безопасность системы определяется не только надежностью криптографических алгоритмов, но и корректностью интерфейсов их использования.

Магнитные полосы: эпоха статических данных

Первые банковские карты использовали магнитную полосу для хранения информации.
На ней размещались:

- номер карты;
- срок действия;
- сервисная информация;
- дополнительные данные для авторизации.

Главной проблемой такого подхода была **статичность информации**.
Данные, записанные на магнитной полосе, не изменялись от транзакции к транзакции.
Это открыло возможности для массового мошенничества.

Скимминг

Наиболее распространенной атакой стало копирование содержимого магнитной полосы с помощью специальных устройств — **скиммеров**.
Обычно преступники:

1. Устанавливали накладной считыватель на банкомат.
2. Получали копию данных магнитной полосы.

3. Захватывали PIN-код при помощи скрытых камер или поддельных клавиатур.
4. Создавали дубликат карты.

Поскольку информация на полосе оставалась неизменной, клон практически не отличался от оригинала.

CVV: первый криптографический барьер

В ответ на рост мошенничества платежные системы внедрили механизм **Card Verification Value (CVV)**.
CVV представляет собой криптографически вычисляемое значение, основанное на:

- номере карты;
- сроке действия;
- секретных ключах эмитента.

Главная идея состояла в том, чтобы создать данные, которые невозможно корректно воспроизвести без знания банковских ключей.
Появление CVV значительно усложнило создание полностью функциональных поддельных карт.
Однако это решение не устраняло фундаментальную проблему магнитной полосы: данные оставались статическими.
Следующим логичным шагом стало использование смарт-карт.

Переход к EMV: появление «умных» карт

Стандарт **EMV** (Europay, Mastercard, Visa) был разработан как ответ на эпидемию клонирования карт.
В отличие от магнитной полосы, чиповые карты содержат встроенный микропроцессор, способный выполнять криптографические операции.
Это позволило перейти от статической аутентификации к динамической.
EMV поддерживает несколько уровней проверки подлинности карты.

Метод	Принцип работы	Ограничения
SDA (Static Data Authentication)	Проверка цифровой подписи статических данных карты	Не защищает от сложных форм клонирования

Метод	Принцип работы	Ограничения
DDA (Dynamic Data Authentication)	Генерация уникальной подписи для каждой транзакции	Не подтверждает содержание транзакции
CDA (Combined Data Authentication)	Подписываются как случайное число, так и параметры транзакции	Требует более сложной инфраструктуры

SDA: статическая аутентификация

При использовании SDA карта содержит цифровую подпись, подтверждающую подлинность ее статических данных.
Терминал проверяет подпись с использованием открытых ключей платежной системы.
Преимущество метода заключается в его простоте.
Недостаток — отсутствие динамического элемента.
Если злоумышленнику удается воспроизвести необходимые данные, защита существенно ослабевает.

DDA: динамическая аутентификация

DDA использует механизм **challenge-response**.
Процесс выглядит следующим образом:

1. Терминал генерирует случайное число (nonce).
2. Карта подписывает его своим закрытым ключом.
3. Терминал проверяет полученную подпись.

Это доказывает, что карта физически присутствует и обладает необходимыми криптографическими секретами.
Однако DDA подтверждает только наличие карты, но не защищает сами параметры платежа.

CDA: комбинированная аутентификация

CDA считается наиболее надежным вариантом EMV-аутентификации.
В этом случае карта подписывает:

- случайное число терминала;
- сумму операции;
- идентификатор торговой точки;

- дополнительные параметры транзакции.

Подделать такую операцию значительно сложнее, поскольку криптографически подтверждается не только присутствие карты, но и конкретное содержимое платежа.
Тем не менее даже CDA не обеспечивает абсолютной защиты.
Безопасность системы по-прежнему зависит от качества реализации и корректности окружающей инфраструктуры.

Когда криптография бессильна: атаки на реализацию EMV

Несмотря на значительный прогресс, достигнутый благодаря внедрению EMV, переход к чиповым картам не решил проблему мошенничества окончательно. История развития платежных систем показывает, что злоумышленники редко атакуют криптографические алгоритмы напрямую. Гораздо чаще они используют ошибки реализации, недостатки бизнес-процессов и особенности взаимодействия между компонентами системы.

Атаки типа Yes-Card

Одной из первых серьезных угроз для систем Chip-and-PIN стали так называемые **Yes-карты** (Yes-cards).
Их идея заключалась в том, чтобы модифицировать чип карты таким образом, чтобы он всегда возвращал положительный результат проверки PIN-кода.
С точки зрения терминала процесс выглядел абсолютно легитимным:

1. Пользователь вводит PIN.
2. Терминал передает его карте для проверки.
3. Карта отвечает, что PIN корректен.
4. Операция продолжается.

Если терминал полагался исключительно на ответ карты и не выполнял дополнительных проверок на стороне банка, мошенническая транзакция успешно проходила.
Эти атаки продемонстрировали важную проблему:

> Безопасность протокола определяется не только его криптографической стойкостью, но и тем, как именно реализованы процедуры проверки.

Атаки ретрансляции (Relay Attacks)

Еще более показательным примером стали **атаки ретрансляции**.
Они используют фундаментальное ограничение большинства систем аутентификации: невозможность достоверно определить физическое расположение устройства.
Сценарий атаки может выглядеть следующим образом:

- злоумышленник А располагается рядом с жертвой и взаимодействует с ее настоящей картой;
- злоумышленник Б находится в магазине с устройством, имитирующим карту;
- запросы от терминала пересылаются между злоумышленниками через интернет или радиоканал;
- настоящая карта жертвы выполняет все необходимые криптографические операции;
- терминал получает корректные ответы и завершает транзакцию.

С точки зрения банка:

- использовался настоящий чип;
- криптографические проверки были успешны;
- PIN-код был введен корректно.

Тем не менее сама транзакция была инициирована мошенниками.
Подобные атаки демонстрируют важную особенность современных систем безопасности:

> Криптография подтверждает подлинность участников взаимодействия, но не всегда гарантирует корректность контекста, в котором это взаимодействие происходит.

От телеграфа к SWIFT: история электронных платежей

Проблемы безопасности банковских переводов возникли задолго до появления компьютеров.
Уже в XIX веке банки активно использовали телеграф для передачи платежных инструкций между городами и странами.
Однако телеграфные операторы получали возможность:

- изменять содержимое сообщений;
- подделывать инструкции;
- задерживать переводы;
- выполнять мошеннические операции от имени банков.

Фактически это были первые атаки на системы электронных платежей.

Тестовые ключи (Test Keys)

Для борьбы с подделкой сообщений банки начали использовать специальные **тестовые ключи**.
Они представляли собой алгоритмы, позволяющие вычислять контрольные значения на основе:

- суммы перевода;
- идентификаторов банков;
- секретной информации, известной только участникам обмена.

Получатель мог проверить корректность полученного кода и убедиться, что сообщение не было изменено.
Хотя современные криптографические методы значительно превосходят тестовые ключи по уровню защиты, сама идея аутентификации сообщений остается неизменной.

SWIFT и процедурные уязвимости

Современная международная система межбанковских сообщений **SWIFT** существенно повысила уровень автоматизации финансовых операций.
Однако опыт показывает, что наиболее серьезные угрозы возникают не из-за слабости криптографических алгоритмов, а вследствие недостатков организационных процессов.

Дело Стэнли Рифкина

Одним из самых известных примеров стало дело **Стэнли Рифкина** в 1978 году. Рифкин похитил более 10 миллионов долларов, не взламывая компьютерные системы банка.
Его схема была удивительно простой:

1. Он узнал внутренний код авторизации банковских переводов.
2. Связался с сотрудниками банка, представившись уполномоченным работником.
3. Инициировал крупный международный перевод.
4. Использовал праздничные выходные для выигрыша времени.

Главный вывод из этого случая заключается в следующем:

> Самые совершенные технические средства защиты оказываются бесполезными, если злоумышленник способен обойти процедурные механизмы контроля.

Экономика безопасности и перекладывание ответственности

Одной из центральных идей статьи является влияние экономических стимулов на уровень безопасности.
Поведение организаций определяется не только техническими возможностями, но и распределением финансовых рисков.

Liability Dumping: перекладывание ответственности

Во многих странах банки длительное время придерживались следующей логики:

> Если карта была использована корректно и PIN-код введен правильно, ответственность несет клиент.

Подобный подход создавал серьезную проблему.
Если финансовые потери несет пользователь, банк получает слабую мотивацию инвестировать в:

- совершенствование систем обнаружения мошенничества;
- повышение качества расследований;
- развитие механизмов компенсации ущерба;
- улучшение пользовательских интерфейсов безопасности.

Моральный риск (Moral Hazard)

Такая ситуация приводит к возникновению **морального риска**.
Когда организация не несет последствий недостаточной защищенности собственных систем, стимулы к улучшению безопасности существенно снижаются.
И наоборот, если банк обязан компенсировать ущерб клиентам, он становится заинтересован в:

- выявлении подозрительных операций;
- внедрении систем мониторинга в реальном времени;
- развитии антифрод-платформ;
- совершенствовании механизмов аутентификации.

Подчеркнем, что именно правильное распределение ответственности зачастую оказывает большее влияние на уровень безопасности, чем внедрение новых технологий.

Домашний банкинг: новая эпоха угроз

Развитие интернет-банкинга радикально изменило ландшафт финансовых угроз. Если раньше злоумышленникам требовалось физическое присутствие рядом с картой или банкоматом, то теперь атаки могли осуществляться удаленно и в массовом масштабе.
Наиболее распространенными стали:

Фишинг

Мошенники создают поддельные сайты банков или отправляют электронные письма, побуждая пользователей раскрыть:

- логины;
- пароли;
- одноразовые коды подтверждения;
- данные платежных карт.

Кейлоггеры

Вредоносное программное обеспечение может фиксировать:

- нажатия клавиш;
- содержимое буфера обмена;

- снимки экрана;
- данные, вводимые в банковские приложения.

Социальная инженерия

Во многих случаях злоумышленникам даже не требуется взлом технических средств защиты.
Достаточно убедить пользователя самостоятельно выполнить необходимые действия.
Именно поэтому современные атаки все чаще направлены не против технологий, а против людей.

Money Mules: индустрия финансовых посредников

Еще одной важной проблемой стали так называемые **денежные мулы** (money mules).
После успешного получения доступа к банковским счетам преступникам необходимо вывести украденные средства таким образом, чтобы не связывать их напрямую со своей личностью.
Для этого используются посредники.
Типичная схема выглядит следующим образом:

1. Через фиктивные вакансии привлекаются новые участники.
2. Им предлагают работу, связанную с обработкой платежей.
3. На их счета поступают похищенные средства.
4. Часть суммы удерживается в качестве вознаграждения.
5. Остальные деньги переводятся дальше, зачастую в другие юрисдикции.

Во многих случаях такие посредники не осознают, что становятся участниками преступной схемы.
Однако именно они часто сталкиваются с юридическими последствиями:

- блокировкой банковских счетов;
- уголовным преследованием;
- обязанностью возмещать ущерб.

Что действительно работает в банковской безопасности

Один из наиболее важных выводов статьи состоит в том, что усложнение аутентификации само по себе редко решает проблему мошенничества.
Даже самые современные механизмы защиты могут быть обойдены через социальную инженерию, ошибки реализации или организационные недостатки.
Наиболее эффективными оказываются следующие меры:

- непрерывный мониторинг транзакций;
- системы обнаружения аномалий;
- быстрое реагирование на подозрительную активность;
- временная блокировка рискованных операций;
- эффективные процедуры возврата средств;
- качественный аудит;
- правильное распределение ответственности между участниками системы.

Основные выводы

Банковские системы демонстрируют, что безопасность является междисциплинарной задачей.
Она включает в себя:

- криптографию;
- бухгалтерский учет;
- организационные процедуры;
- управление рисками;
- экономические стимулы;
- психологию поведения пользователей.

Главный урок заключается в следующем:

> Безопасность определяется не прочностью самого сильного механизма защиты, а устойчивостью всей системы в целом.

Именно поэтому эффективная защита финансовых систем требует сочетания технических, организационных и экономических мер.
Криптография играет важную роль, но сама по себе она никогда не сможет заменить грамотное проектирование процессов, качественный аудит и

правильное распределение ответственности.
В конечном итоге банковская безопасность — это не столько задача защиты информации, сколько задача построения системы, в которой мошенничество становится сложным, дорогостоящим и экономически невыгодным.

Аудит и сверка: незаметные герои банковской безопасности

Когда говорят о безопасности банковских систем, обычно вспоминают криптографию, двухфакторную аутентификацию или защиту платежных карт. Однако в реальности значительная часть мошенничеств обнаруживается благодаря гораздо менее заметным механизмам — аудиту и бухгалтерской сверке.
Именно эти процессы позволяют выявлять аномалии, которые невозможно предотвратить техническими средствами.

Сверка (Reconciliation): фундамент обнаружения мошенничества

Сверка представляет собой процесс сопоставления данных из различных источников для подтверждения их согласованности.
Основная идея проста:

> Если все операции были выполнены корректно, учетные записи различных систем должны совпадать.

В банковской сфере регулярно сверяются:

- внутренние бухгалтерские счета;
- данные процессинговых центров;
- журналы операций банкоматов;
- корреспондентские счета банков;
- отчеты платежных систем;
- остатки наличности в отделениях.

Любое несоответствие требует расследования.
Например, если банкомат сообщает о выдаче 100 000 евро, а кассетный учет показывает уменьшение наличности лишь на 90 000 евро, возникает очевидный сигнал о возможном мошенничестве или технической ошибке.

Именно благодаря процедурам сверки обнаруживаются многие финансовые преступления.
Подчеркнем важную мысль:

> Во многих случаях мошенничество выявляется не криптографическими механизмами, а нарушением бухгалтерского баланса.

Это отражает фундаментальный принцип банковской безопасности: невозможно долго скрывать действия, которые нарушают финансовую целостность системы.

Аудит как самостоятельный механизм защиты

Во многих областях информационной безопасности аудит рассматривается как вспомогательный инструмент. В банковской сфере его значение значительно выше.
Фактически аудит выступает одним из основных механизмов обеспечения подотчетности.
Эффективная система аудита должна обладать несколькими ключевыми свойствами.

Независимость

Лица, выполняющие операции, не должны проверять собственные действия.
Например:

- сотрудники фронт-офиса не проводят внутренние расследования своих операций;
- администраторы систем не являются единственными хранителями журналов событий;
- аудиторы организационно отделены от операционных подразделений.

Отсутствие независимости делает аудит формальностью и создает благоприятную среду для злоупотреблений.

Неизменяемость журналов

Аудиторские записи должны быть защищены от модификации.
Если злоумышленник способен изменить историю собственных действий, ценность журналов полностью теряется.
Поэтому банковские системы используют:

- криптографическую защиту журналов;

- системы контроля целостности;
- хранение логов на независимых платформах;
- механизмы ограничения административного доступа.

Современные подходы к **immutable logging** и **forensic readiness** во многом продолжают идеи, сформировавшиеся именно в банковской отрасли.

Регулярность проверок

Проверка должна проводиться постоянно, а не только после инцидентов.
Это включает:

- ежедневные сверки;
- выборочные проверки операций;
- анализ подозрительных транзакций;
- периодические внешние аудиты.

Чем быстрее обнаруживается нарушение, тем меньше потенциальный ущерб.

Подотчетность

Для каждой операции должно быть понятно:

- кто выполнил действие;
- когда оно было выполнено;
- какие данные были изменены;
- на каком основании было принято решение.

Подотчетность является одной из фундаментальных характеристик безопасной финансовой системы.

Принцип четырех глаз (Four-Eyes Principle)

Одним из наиболее известных банковских механизмов контроля является принцип **четырех глаз**.
Его суть заключается в том, что ни одна критически важная операция не должна выполняться и утверждаться одним человеком.
Например, отдельного подтверждения могут требовать:

- международные переводы крупных сумм;
- изменение лимитов операций;
- выпуск криптографических ключей;

- предоставление привилегированного доступа;
- одобрение кредитных решений.

Этот принцип значительно снижает риск:

- внутренних злоупотреблений;
- случайных ошибок;
- компрометации учетных записей отдельных сотрудников.

Интересно, что банковские практики постепенно распространились далеко за пределы финансовой отрасли.
Сегодня аналогичные механизмы применяются в:

- процессах согласования изменений инфраструктуры;
- системах управления доступом;
- DevSecOps-практиках через обязательный code review;
- процедурах утверждения критических изменений.

Почему банки делают ставку на обнаружение, а не на предотвращение

Интуитивно кажется, что главная цель безопасности — полностью предотвратить атаки.
Однако банковская практика показывает иной подход.
Отметим:

> Предотвратить все мошенничества невозможно.

Сложность финансовых систем, человеческий фактор и постоянная эволюция методов атак делают абсолютную защиту недостижимой целью.
Поэтому банки исторически сместили фокус на четыре направления:

1. Быстрое обнаружение мошенничества.
2. Минимизацию финансового ущерба.
3. Возврат активов.
4. Расследование инцидентов.

Такой подход лежит в основе модели:

```
Prevent → Detect → Respond → Recover
```

Фактически банковская индустрия пришла к современным концепциям безопасности задолго до их формального появления.
Многие идеи, активно используемые сегодня, имеют аналогии именно в банковской практике:

Современная концепция	**Банковский эквивалент**
Assume Breach	Предположение, что часть мошенничества неизбежна
Detection Engineering	Антифрод-системы и мониторинг транзакций
Zero Trust	Многоступенчатое подтверждение операций
Incident Response	Процедуры расследования и возврата средств
Continuous Monitoring	Постоянный аудит и сверка

Безопасность как проблема стимулов

Одним из самых важных выводов статьи является понимание того, что безопасность определяется не только технологиями, но и экономическими стимулами.
Люди и организации действуют рационально в рамках тех условий, которые создает система.
Если система вознаграждает скорость обработки операций больше, чем качество проверок, сотрудники будут искать способы обходить процедуры контроля.
Если организация не несет финансовых последствий недостаточной защищенности, инвестиции в безопасность становятся менее приоритетными.
Если пользователи остаются без правовой защиты, уровень мошенничества неизбежно возрастает.
Поэтому при проектировании безопасных систем необходимо учитывать не только технические аспекты, но и вопросы распределения ответственности.
Правильно выстроенные стимулы способны повысить безопасность эффективнее, чем внедрение новых защитных технологий.

От тестовых ключей к современным механизмам аутентификации

История банковской безопасности показывает, что многие современные идеи появились задолго до возникновения компьютерной криптографии.
Еще в эпоху телеграфных переводов банки использовали специальные **тестовые ключи (Test Keys)** для проверки подлинности сообщений.
Обычно они основывались на:

- секретных таблицах;
- арифметических алгоритмах;
- кодовых книгах.

Получатель перевода мог проверить контрольное значение и убедиться, что сообщение не было подделано.
По своей сути эти механизмы выполняли ту же функцию, что и современные **Message Authentication Codes (MAC)**:

- подтверждение подлинности отправителя;
- контроль целостности сообщения;
- обнаружение несанкционированных изменений.

Это демонстрирует важную особенность развития безопасности:

> Большинство фундаментальных принципов появились задолго до современных технологий. Изменились лишь способы их реализации.

Инсайдеры против внешних злоумышленников

Общественное восприятие часто связывает банковские угрозы исключительно с внешними хакерами.
Однако опыт показывает, что значительная часть крупных финансовых потерь связана именно с действиями инсайдеров.
Источниками риска могут быть:

- сотрудники банков;
- операторы платежных систем;
- администраторы инфраструктуры;
- подрядчики;
- сотрудники процессинговых центров.

Причина заключается в том, что инсайдеры уже обладают:

- знаниями внутренних процессов;
- легитимным доступом;
- пониманием контрольных процедур;
- возможностью скрывать следы своих действий.

Именно поэтому банковская безопасность уделяет столь большое внимание:

- разделению обязанностей;
- аудиту;
- подотчетности;
- независимому контролю.

Итоговые выводы

Данная статья о банковском деле и бухгалтерском учете демонстрирует, что обеспечение безопасности финансовых систем выходит далеко за рамки криптографии.
Эффективная защита строится на сочетании нескольких взаимосвязанных элементов:

- поддержания целостности данных;
- строгих бухгалтерских принципов;
- разделения обязанностей;
- независимого аудита;
- непрерывного мониторинга;
- правильного распределения ответственности;
- экономических стимулов, поощряющих безопасное поведение.

Главный урок заключается в следующем:

> Безопасность финансовых систем определяется не способностью предотвратить каждую атаку, а способностью своевременно обнаруживать нарушения, ограничивать последствия и обеспечивать восстановление нормального состояния системы.

Банковская отрасль одной из первых осознала, что абсолютной защиты не существует.
Вместо попыток создать неприступную систему она выстроила механизмы, делающие мошенничество заметным, дорогостоящим и экономически

невыгодным.
Именно этот подход остается одним из наиболее ценных уроков для современной информационной безопасности.