

Юлия Николаевна Самопальникова

кандидат экономических наук, доцент, доцент кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, i.n.samopalnikova@utmn.ru

Елена Юрьевна Петренко

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, petrenkoel04@mail.ru

Лада Васильевна Карфидова

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, karfidova.lada@mail.ru

ДЕЯТЕЛЬНОСТЬ КОММЕРЧЕСКИХ БАНКОВ В ПРОТИВОДЕЙСТВИИ НЕЗАКОННЫМ ОПЕРАЦИЯМ

Аннотация. Статья посвящена анализу деятельности коммерческих банков в противодействии незаконным операциям. Рассматриваются ключевые нормативно-правовые акты, регулирующие внутренний контроль в банках, такие как федеральный закон 115-ФЗ и положения Банка России. Описание механизмов, реализуемых банками для обеспечения финансовой безопасности, включает идентификацию клиентов, оценку рисков, мониторинг операций и сотрудничество с Росфинмониторингом. В статье подробно рассматривается роль автоматизированных систем AML (Anti-Money Laundering) в выявлении подозрительных транзакций, а также меры, внедряемые Сбербанком, для защиты клиентов и предотвращения мошенничества.

Ключевые слова: коммерческие банки, противодействие незаконным операциям, финансовый мониторинг, AML.

Julia Nikolaevna Samopalnikova

Candidate of Sciences (Economics), Associate Professor of the Department of Economic Security, System Analysis and Control, University of Tyumen, Tyumen, i.n.samopalnikova@utmn.ru

Elena Yurievna Petrenko

Student of the specialty "Economic Security" at Tyumen State University, Tyumen, petrenkoel04@mail.ru

Lada Vasilievna Karfidova

Student of the specialty "Economic Security" at Tyumen State University, Tyumen, karfidova.lada@mail.ru

ACTIVITIES OF COMMERCIAL BANKS IN COUNTERING ILLEGAL TRANSACTIONS

Abstract. The article analyzes the activities of commercial banks in countering illegal transactions. Key regulatory legal acts regulating internal control in banks, such as Federal Law 115-FZ and regulations of the Bank of Russia, are considered. The description of the mechanisms implemented by banks to ensure financial security includes customer identification, risk assessment, monitoring of operations and cooperation with Rosfinmonitoring. The article examines in detail the role of automated AML (Anti-Money Laundering) systems in detecting suspicious transactions, as well as measures implemented by Sberbank to protect customers and prevent fraud.

Keywords: commercial banks, countering illegal transactions, financial monitoring, AML.

Коммерческие банки являются важнейшими участниками финансовой системы и одновременно уязвимыми звеньями в контексте совершения незаконных операций. Сложность финансовых потоков и глобализация рынков способствуют

увеличению числа попыток легализации преступных доходов через банковские структуры. Это обуславливает необходимость эффективной системы внутреннего контроля и взаимодействия банков с государственными органами [1].

Для реализации этих задач банки руководствуются четко установленными нормативно-правовыми актами, регламентирующими порядок идентификации клиентов, анализа операций и сотрудничества с надзорными органами.

В частности, коммерческие банки действуют в соответствии с:

1. Федеральным законом от 07.08.2001 № 115-ФЗ (ред. от 28.12.2024) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [2].

2. Положением Банка России от 02.03.2012 № 375-П (ред. от 07.11.2022) «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [3].

3. Международным стандартом по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения рекомендации ФАТФ (с изменениями от февраля 2025 года) [4].

Соблюдение этих норм контролируется как внутренними службами комплаенс-контроля, так и государственными регуляторами (Росфинмониторингом и Банком России).

Коммерческие банки обязаны идентифицировать клиентов, оценивать риски операций и передавать информацию о подозрительных транзакциях в Росфинмониторинг [5].

Основные направления противодействия незаконным операциям в коммерческих банках отражены в табл. 1.

Таблица 1

**Основные направления противодействия незаконным операциям
в коммерческих банках**

<i>Направление</i>	<i>Механизм реализации</i>	<i>Ответственное подразделение</i>
Идентификация клиентов (KYC)	Сбор паспортных и корпоративных данных, биометрия	Отдел обслуживания / KYC-центр
Оценка рисков (Risk-Based Approach)	Присвоение клиентам уровней риска	Отдел финансового мониторинга
Мониторинг операций	Автоматический анализ транзакций	IT-департамент / служба безопасности
Подозрительная активность (SAR)	Формирование отчетов о подозрительных операциях	AML-специалисты
Внутренние регламенты и обучение	Проведение обучения, регулярные аудиты	Отдел комплаенс-контроля
Взаимодействие с Росфинмониторингом	Направление отчетов, участие в проверках	Юридический департамент

Источник: составлено авторами на основе данных [6, 7].

В последние годы наблюдается рост количества сообщений, направляемых банками в уполномоченные органы. Это связано как с усилением контроля, так и с совершенствованием технических средств.

Динамика операций без согласия клиентов в банках РФ и их объема в 2020–2024 гг. отражены на рис. 1 и 2.

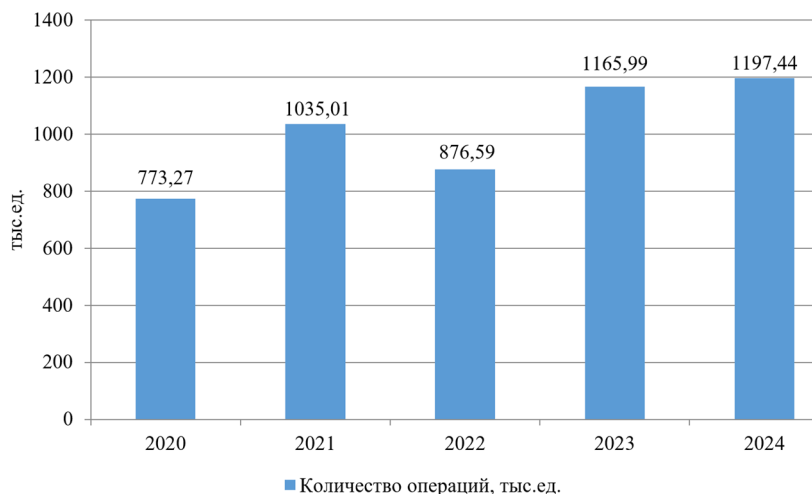


Рис. 1. Динамика операций без согласия клиентов в банках РФ в 2020–2024 гг.

Источник: составлено авторами на основе данных [8].

Анализ представленных данных показывает стабильный рост как количества, так и суммарного объема операций, совершенных без согласия клиентов в банках РФ. Количество таких операций увеличилось с 773,27 тыс. в 2020 году до 1197,44 тыс. в 2024 году, что составляет прирост примерно 54,9%.

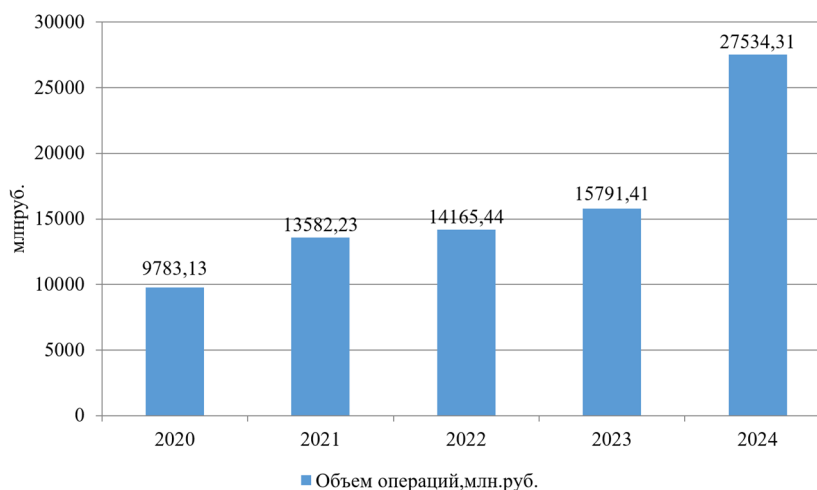


Рис. 2. Объем операций без согласия клиентов в банках РФ в 2020–2024 гг.

Источник: составлено авторами на основе данных [8].

Еще более заметна динамика по сумме незаконных транзакций: с 9783,13 млн руб. в 2020 году до 27534,31 млн руб. в 2024 году — рост составил 181,4%. Рост количества и объемов незаконных транзакций свидетельствует не только об активности злоумышленников, но и о наличии уязвимостей в системе банковского контроля. Это подчеркивает актуальность внедрения и развития более совершенных инструментов анализа и мониторинга операций. В условиях растущих угроз особую значимость приобретают современные системы противодействия легализации доходов, полученных преступным путем (AML — Anti-Money Laundering), которые играют ключевую роль в обеспечении финансовой безопасности [9].

Эти системы позволяют автоматически выявлять подозрительные транзакции, оценивать поведенческие риски клиентов, контролировать цепочки переводов и взаимодействовать с внешними источниками информации. AML-платформы базируются на принципах анализа больших данных (Big Data), машинного обучения и риск-ориентированного подхода, что позволяет существенно повысить эффективность комплаенс-процедур. Функциональные модули AML-систем и их задачи отражены в табл. 2.

Таблица 2

Функциональные модули AML-систем и их задачи

<i>Модуль</i>	<i>Основная функция</i>	<i>Пример реализации</i>
KYC (Know Your Customer)	Идентификация и верификация клиента	Проверка паспорта, ИНН, ФИО
Transaction Monitoring	Анализ операций в реальном времени	Выявление нетипичных транзакций
Watchlist Filtering	Сопоставление с санкционными списками	Сверка с базами OFAC, UNSC
Case Management	Обработка инцидентов и подозрительных операций	Ведение истории расследований
Reporting Module	Формирование отчетности для Росфинмониторинга	Форматирование SAR/STR

Источник: составлено авторами на основе данных [9, 10].

Сбербанк, как крупнейший банк Российской Федерации, обладающий наибольшей клиентской базой и масштабной инфраструктурой, играет ключевую роль в национальной системе противодействия легализации преступных доходов.

Сбербанк реализует многоуровневую архитектуру противодействия незаконным операциям, сочетающую технологические платформы, регламентные процедуры и клиентоориентированные механизмы безопасности (табл. 3).

**Дополнительные клиентские меры Сбербанка
в рамках AML и кибербезопасности**

<i>Сервис</i>	<i>Назначение</i>	<i>Связь с AML и защитой транзакций</i>
«Близкие рядом»	Назначение доверенного помощника для подтверждения операций	Защита уязвимых клиентов
«Закрыть доступ к счетам и картам»	Быстрое отключение доступа при подозрении на мошенничество	Срочная блокировка активности
«Определитель номера»	Выявление и блокировка подозрительных звонков и сообщений	Защита от социальной инженерии
«Антивирус в приложении»	Сканирование устройства на вредоносное ПО	Блокировка вирусов, крадущих данные
«Куда привязаны ваши карты»	Проверка активных подписок и автосписаний	Контроль подозрительных регулярных платежей
«Утечки данных»	Мониторинг компрометации личной информации	Выявление рисков несанкционированного доступа

Источник: составлено авторами [11].

Все эти функции усиливают клиентскую защищенность и интегрированы в общую AML-экосистему Сбербанка, дополняя базовые модули комплаенс-контроля. Их назначение — минимизировать риски уже на пользовательском уровне, особенно в отношении фишинга, социальной инженерии и компрометации устройств.

Тем не менее, даже при внедрении современных технологий банки продолжают сталкиваться с рядом устойчивых проблем, препятствующих эффективному противодействию незаконным операциям:

1. Человеческий фактор: ошибки сотрудников при классификации клиентов.
2. Сложность бенефициарной структуры затрудняет выявление фактического владельца;
3. Финансовая нагрузка: содержание систем AML требует больших инвестиций.

Таким образом, противодействие незаконным операциям остается одним из ключевых направлений деятельности коммерческих банков. Несмотря на внедрение современных цифровых решений и развитие автоматизированных систем анализа, проблема сохраняет свою актуальность из-за наличия как технических, так и организационных барьеров.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Противодействие отмыванию денег и валютный контроль // Банк России: сайт. — URL: https://cbr.ru/counteraction_m_ter/ (дата обращения: 10.04.2025).
2. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федеральный закон от 07.08.2001 № 115-ФЗ: принят Государственной Думой 13 июля 2001 года: одобрен Советом Федерации 20 июля 2001 года (ред. от 28.12.2024) //КонсультантПлюс: надежная правовая поддержка: сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 10.04.2025).

3. О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Положение Банка России от 02.03.2012 № 375-П (ред. от 07.11.2022). // Гарант.ру: информационно-правовой портал: сайт. — URL: <https://base.garant.ru/70162622/> (дата обращения: 10.04.2025).
4. Международный стандарт по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения рекомендации ФАТФ (с изменениями от февраля 2025 года) // Банк России: сайт. — URL: https://cbr.ru/content/document/file/174972/fatf_rec_ru.pdf (дата обращения: 10.04.2025).
5. Об утверждении требований к идентификации клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев, в том числе с учетом степени (уровня) риска совершения подозрительных операций : приказ Росфинмониторинга от 20.05.2022 № 100 (ред. от 29.12.2022): утвержден приказом Федеральной службы по финансовому мониторингу от 20.05.2022 года № 100 // Консультант-Плюс: надежная правовая поддержка : сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_419741/ (дата обращения: 10.04.2025).
6. Тадевосян А.В. Деятельность коммерческих банков в противодействии незаконным операциям с денежными средствами: выпускная квалификационная работа специалиста 5 курса очной формы обучения по направлению подготовки 38.05.01 Экономическая безопасность / А. В. Тадевосян. — Тюмень, 2020. — 73 с. // Электронная библиотека ТюмГУ: сайт. — URL: https://vk.com/away.php?to=https%3A%2F%2Flibrary.utmn.ru%2Fdl%2FVKR_Tyumen%2FVKR_2020%2FFEI%2FTadevosyanAV_2020.pdf%2Fview&utf=1 (дата обращения: 10.04.2025).
7. Акишина К.Д. Противодействие незаконным финансовым доходам в банковской сфере / К.Д. Акишина, Л.А. Козачек, М.Н. Михайлюк // Индустриальное, инновационное и финансовое развитие России: факторы и тенденции: Сборник статей Всероссийской научно-практической конференции студентов и молодых ученых, Сочи, 09 апреля 2021 года / под ред. Н.В. Агазаряна, В.В. Сорокожердьева, Т.В. Шурухиной. — Москва: АНО «Научно-исследовательский институт истории, экономики и права», 2021. — С. 13-16. // Электронная библиотека Elibrary.ru: сайт. — URL: <https://www.elibrary.ru/> (дата обращения: 10.04.2025).
8. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций // Банк России: сайт. — URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 11.04.2025).
9. Truntsevsky Yu. V. Anti-Money Laundering by Restricting Financial Transactions / Yu. V. Truntsevsky, S. I. Dolganov // Criminal Law and Operative Search Activities: Problems of Legislation, Science and Practice, Moscow, 23 апреля 2021 года. — Moscow, 2021. — Р. 5-9 // Электронная библиотека Elibrary.ru: сайт. — URL: <https://www.elibrary.ru/> (дата обращения: 10.04.2025).
10. Gladkova S. B. Противодействие легализации доходов, полученных преступным путем, и финансированию терроризма: теоретический бэкграунд и практическая реализация / С. Б. Gladkova, Д. Е. Дробов // Вестник экономической безопасности. — 2021. — № 1. — С. 90-95. // Электронная библиотека Elibrary.ru: сайт. — URL: <https://www.elibrary.ru/> (дата обращения: 10.04.2025).
11. Сервисы безопасности в СберБанк Онлайн // Сбербанк: сайт. — URL: <https://www.sberbank.ru/ru/person> (дата обращения: 11.04.2025).