



Банк России

АВГУСТ 2025



**ОБЗОР СОБЫТИЙ  
В СФЕРЕ ПРОТИВОДЕЙСТВИЯ  
ОТМЫВАНИЮ ДОХОДОВ,  
ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ,  
И ФИНАНСИРОВАНИЮ  
ТЕРРОРИЗМА**

## СОДЕРЖАНИЕ

<b>СПИСОК СОКРАЩЕНИЙ</b>	4
<b>РОССИЙСКИЕ НОВОСТИ</b>	5
Постановления Правительства Российской Федерации .....	5
• № 1157 и № 1180 .....	5
• № 1183.....	6
<b>МЕЖДУНАРОДНЫЕ НОВОСТИ</b> .....	7
Новости ФАТФ .....	7
• О руководстве ФАТФ по проведению национальной оценки рисков ОД .....	7
Новости международных организаций и объединений.....	7
• О докладе БМР об альтернативном подходе к обеспечению соответствия требованиям в сфере ПОД в экосистемах публичных блокчейнов без разрешений .....	7
• О заявлении Вольфсбергской группы об эффективном мониторинге подозрительной активности.....	8
Новости стран мира .....	9
• О росте мошенничества и ОД с использованием криптообменников в США .....	9
• О принципах применения штрафных санкций за нарушения Закона о ПОД/ФТ в Канаде.....	10
• О мерах надзорного органа США в отношении финансовой организации Paxos Trust Company, LLC .....	10
• О докладе Европейской службы банковского надзора о результатах оценки эффективности использования надзорными органами технологий SupTech в целях ПОД/ФТ .....	11
• О внесении изменений в Указание Резервного банка Индии «О применении мер НПК» .....	11
• О мерах Центрального банка Нидерландов в отношении банка Bunq B.V .....	12

Настоящий материал подготовлен  
Службой финансового мониторинга и валютного контроля

Фото на обложке: Shutterstock.com

Адрес: 107016, Москва, ул. Неглинная, д. 12, к. В

Телефон: +7 499 300 30 00

Официальный сайт Банка России: [www.cbr.ru](http://www.cbr.ru)

© Центральный банк Российской Федерации, 2025

## СПИСОК СОКРАЩЕНИЙ

<b>ОД/ФТ</b>	Легализация (отмывание) доходов, полученных преступным путём, и финансирование терроризма
<b>ПОД/ФТ</b>	Противодействие легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма
<b>ПОД/ФТ/ФРОМУ</b>	Противодействие легализации (отмыванию) доходов, полученных преступным путём, финансированию терроризма и финансированию распространения оружия массового уничтожения
<b>ОД</b>	Легализация (отмывание) доходов, полученных преступным путём
<b>ПОД</b>	Противодействие легализации (отмыванию) доходов, полученных преступным путём
<b>ФАТФ</b>	Группа разработки финансовых мер борьбы с отмыванием денег
<b>ПУВА</b>	Поставщики услуг в сфере виртуальных активов
<b>НПК</b>	Надлежащая проверка клиентов
<b>ПВК</b>	Правила внутреннего контроля

## РОССИЙСКИЕ НОВОСТИ

### Постановления Правительства Российской Федерации

**2 августа и 7 августа 2025 года Правительством Российской Федерации приняты постановления № 1157 «Об утверждении требований к правилам внутреннего контроля, разрабатываемым организациями, осуществляющими операции с денежными средствами или иным имуществом, и индивидуальными предпринимателями» и № 1180 «Об утверждении требований к правилам внутреннего контроля, разрабатываемым адвокатами, доверительными собственниками (управляющими) иностранной структуры без образования юридического лица, исполнительными органами личного фонда (кроме наследственного фонда), в том числе международного личного фонда (кроме международного наследственного фонда), лицами, осуществляющими предпринимательскую деятельность в сфере оказания юридических или бухгалтерских услуг, лицами, осуществляющими майнинг цифровой валюты (в том числе участниками майнинг-пула), лицами, организующими деятельность майнинг-пула, нотариусами, аудиторскими организациями и индивидуальными аудиторами».**

Обновленные редакции требований, предъявляемых при разработке организациями, осуществляющими операции с денежными средствами или иным имуществом (за исключением кредитных организаций и некредитных финансовых организаций), и субъектами статьи 7.1 Федерального закона № 115-ФЗ<sup>1</sup> правил внутреннего контроля в целях ПОД/ФТ/ФРОМУ, изданы в том числе в целях приведения их в соответствие с положениями Федерального закона № 115-ФЗ в редакции федеральных законов № 222-ФЗ и № 522-ФЗ<sup>2</sup>.

Так, в число субъектов исполнения требований к ПВК включены лица, осуществляющие майнинг цифровой валюты (в том числе участники майнинг-пула), и лица, организующие деятельность майнинг-пула, а в периметр требований к ПВК включены вопросы противодействия экстремистской деятельности.

Кроме того, определено, что:

- при оценке риска совершения клиентом подозрительных операций организации, осуществляющие операции с денежными средствами или иным имуществом, и субъекты статьи 7.1 Федерального закона № 115-ФЗ должны учитывать результаты секторальной оценки рисков совершения операций в целях ОД/ФТ;
- программа, регламентирующая порядок действий в случае отказа в приеме клиента на обслуживание является неотъемлемым компонентом ПВК субъектов статьи 7.1 Федерального закона № 115-ФЗ;

<sup>1</sup> Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

<sup>2</sup> Федеральный закон от 8 августа 2024 года № 222-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» и Федеральный закон от 28 декабря 2024 года № 522-ФЗ «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и отдельные законодательные акты Российской Федерации» - см. обзоры событий в сфере ПОД/ФТ за август и декабрь 2024 года.

- входящая в состав ПВК субъектов статьи 7.1 Федерального закона № 115-ФЗ программа идентификации должна в обязательном порядке включать обновление сведений, полученных в результате идентификации клиентов, представителей клиентов, выгодоприобретателей и бенефициарных владельцев (в случае если клиент принят на обслуживание, предполагающее длящийся характер отношений);
- ПВК, разрабатываемые нотариусами, должны содержать программу, регламентирующую порядок действий при принятии решения об отказе в совершении нотариального действия.

Постановление № 1157 вступило в силу с 10 августа 2025 года, постановление № 1180 – с 16 августа 2025 года.

*Источник информации: «Официальный интернет-портал правовой информации» (<http://www.pravo.gov.ru>).*

**7 августа 2025 года Правительством Российской Федерации принято постановление № 1183 «О внесении изменений в некоторые акты Правительства Российской Федерации».**

Постановлением № 1183 внесены изменения в Правила размещения физическими лицами своих биометрических персональных данных в единой биометрической системе с использованием мобильного приложения единой биометрической системы, утвержденные Постановлением № 1066<sup>3</sup>, в соответствии с которыми банки, соответствующие критериям, предусмотренным Федеральным законом № 115-ФЗ, вправе подтвердить биометрические персональные данные физического лица, размещённые физическим лицом самостоятельно в единой биометрической системе (ЕБС), до истечения срока их использования при условии наличия у банка технической возможности.

Одновременно расширен перечень случаев использования биометрических персональных данных, размещённых физическим лицом в ЕБС с использованием мобильного приложения ЕБС, предусмотренный Постановлением № 1067<sup>4</sup>.

В указанный перечень включено (1) осуществление микрофинансовой организацией при дистанционном приеме на обслуживание клиента - физического лица идентификации клиента, представителя клиента, а также идентификации или аутентификации заемщика в целях заключения договора потребительского займа в электронной форме, (2) осуществление доступа к официальному сайту в сети «Интернет» и мобильному приложению микрофинансовой организации.

Кроме того, предусмотрен дополнительный перечень случаев использования биометрических персональных данных, размещенных физическим лицом в ЕБС с использованием мобильного приложения ЕБС, достоверность которых подтверждена банком. В указанный перечень включены:

<sup>3</sup> Постановление Правительства Российской Федерации от 15 июня 2022 года № 1066 «О размещении физическими лицами своих биометрических персональных данных в единой биометрической системе с использованием мобильного приложения единой биометрической системы».

<sup>4</sup> Постановление Правительства Российской Федерации от 15 июня 2022 года № 1067 «О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой биометрической системе с использованием мобильного приложения единой биометрической системы».

- осуществление идентификации и (или) аутентификации для приема на обслуживание или обслуживания клиентов - физических лиц организациями, осуществляющими операции с денежными средствами или иным имуществом, регулирование, контроль и надзор за которыми осуществляют Банк России (в случаях, не противоречащих требованиям законодательства Российской Федерации);
- предоставление пользователям платформы цифрового рубля доступа к платформе цифрового рубля в целях совершения операций с цифровыми рублями.

*Источник информации: «Официальный интернет-портал правовой информации» (<http://www.pravo.gov.ru>).*

## МЕЖДУНАРОДНЫЕ НОВОСТИ

### Новости ФАТФ

**28 августа 2025 года** ФАТФ опубликовано практическое руководство для стран – членов Глобальной сети Группы по проведению национальной оценки рисков отмывания денег (НОР)<sup>5</sup>.

Руководство призвано помочь странам - членам Глобальной сети ФАТФ укрепить применяемый ими риск-ориентированный подход в сфере ПОД/ФТ.

В руководстве содержатся практические материалы для разработки и совершенствования методологии проведения НОР в соответствии со Стандартами ФАТФ. В частности, в документе (i) освещается передовая практика стран и приоритетные области для оценки рисков странами (в первую очередь, рисков, связанных с коррупцией, виртуальными активами и ПУВА, юридическими лицами и образованиями, а также теневой экономикой); (ii) приведены оценочные данные об объемах доходов от преступной деятельности, перечень наиболее распространенных предикатных преступлений, а также типологии ОД/ФТ на национальном и международном уровнях.

Также в руководстве содержатся: практические примеры стран; рекомендации по устранению пробелов данных об имеющихся в странах рисках и повышению качества их анализа; ориентиры для разработки целевых планов мер по снижению рисков ОД/ФТ.

Руководство может применяться как для проведения НОР, так и секторальных или тематических исследований.

*Источник информации: официальный сайт ФАТФ в сети Интернет.*

### Новости международных организаций и объединений

**13 августа 2025 года** опубликован доклад Банка международных расчётов (БМР) с предложением концепции альтернативного подхода к обеспечению соответствия требованиям в сфере ПОД в экосистемах публичных блокчейнов без разрешений<sup>6</sup>.

<sup>5</sup> FATF Toolkit. Money Laundering National Risk Assessment Toolkit.

<sup>6</sup> An approach to anti-money laundering compliance for cryptoassets.

В докладе отмечается существенный рост объёмов ежедневных переводов криптоактивов (включая стейблконы), осуществляемых в публичных блокчейнах без разрешений (permissionless)<sup>7</sup>, и не охваченных действующими процедурами в сфере ПОД после вывода средств в децентрализованные («бессерверные») кошельки<sup>8</sup> (unhosted wallets), а также их последующая интеграция в традиционную финансовую систему. Так, например, в 2024 году стейблконы обошли биткоин как основной инструмент, используемый в целях совершения незаконных крипtotранзакций, составив около 63% от их совокупного объёма.

Предложенная БМР концепция направлена на преодоление ограничений традиционной модели осуществления надзора, применяемой в криптовалютном секторе, в которой предусмотрено участие посредников.

В данной концепции предлагается формировать индексы комплаенса по ПОД для каждой единицы криптоактивов или кошельков на основе полной истории транзакций в блокчейне (от «допущенных» /allow-listed/ с высоким индексом «чистоты» до «запрещённых» /deny-listed/ с низким индексом, отражающим высокий риск вовлечённости в незаконные транзакции). Такие индексы могут использоваться банками, компетентными органами, криптовалютными биржами при принятии решения о проведении или отказе в проведении операции по переводу криптоактивов (включая стейблконы) в фиатную валюту в целях недопущения попадания средств, полученных в результате незаконной деятельности, в банковскую систему.

Также предлагаются варианты контроля: от строгого с обязательной полной идентификацией для всех кошельков до более гибких проверок. С применением такого вариативного подхода обязанность по проведению проверки возлагается на участников финансового рынка, стимулируя тем самым проведение операций через кошельки с высоким индексом.

*Источник информации: официальный сайт БМР в сети Интернет.*

**27 августа 2025 года опубликовано заявление Вольфсбергской группы<sup>9</sup> об эффективном мониторинге подозрительной активности<sup>10</sup>.**

Финансовым организациям рекомендуется расширить рамки традиционного мониторинга транзакций за счёт перехода к мониторингу подозрительной активности, предусматривающему анализ не только самих транзакций, но и данных о поведении клиентов с учётом ключевых угроз ОД/ФТ. В этих целях предлагается

<sup>7</sup> Публичный блокчейн без разрешений (permissionless public blockchain) – это децентрализованная распределённая сеть, в которой отсутствует централизованный посредник, что усложняет проведение проверок в целях ПОД и делает невозможным блокировку или разрешение транзакций на уровне сети без изменения её протоколов (классические примеры – биткоин, эфириум).

<sup>8</sup> Unhosted wallets.

<sup>9</sup> Вольфсбергская группа является ассоциацией тринадцати глобальных банков (Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank и UBS), целью которой является разработка рекомендаций по управлению рисками, связанными с совершением финансовых преступлений. Особое внимание Вольфсбергской группой уделяется совершенствованию практики «знай своего клиента» и мер ПОД/ФТ.

<sup>10</sup> The Wolfsberg Group – Statement on Effective Monitoring for Suspicious Activity. Part II: Transitioning to innovation.

использовать инструменты машинного обучения, искусственного интеллекта и автоматизации.

Финансовым организациям предлагается внедрить инновационный подход в процедуры мониторинга подозрительной активности, учитывающий три ключевых компонента:

- переход и валидация: трансформация от устаревших систем к современным, автоматизированным платформам, в рамках которых оценивается не эквивалентность старой системе, а общая эффективность;
- баланс между риском моделей и риском совершения финансовых преступлений: предпочтение моделям, которые могут быть несовершенными, но вместе с тем обеспечивать более оперативное выявление финансовыми организациями подозрительной активности;
- объяснимость: используемые финансовыми организациями модели должны быть прозрачными; типологии должны быть учтены в параметрах моделей.

При этом автоматизированные инструменты мониторинга должны дополнять, а не заменять более широкую систему контроля, предусматривающую возможность направления запросов на осуществление аналитического анализа данных, а также привлечения высококвалифицированных экспертов в области анализа подозрительной активности.

*Источник информации: официальный сайт Вольфсбергской группы в сети Интернет.*

## Новости стран мира

**4 августа 2025 года опубликована информация Сети по борьбе с финансовыми преступлениями (Financial Crimes Enforcement Network, FinCEN) о резком росте случаев мошенничества и ОД с использованием криптообменников<sup>11</sup>.**

По информации FinCEN, в 2024 году в Федеральное бюро расследований США поступило около 11 тыс. обращений об использовании криптообменников в целях совершения мошенничества и ОД (что на 99% превысило количество аналогичных обращений за предыдущий год). Совокупная сумма нанесённого ущерба за указанный период составила около 247 млн долларов США<sup>12</sup>.

Отмечается, что наиболее активными пользователями криптообменников являются транснациональные преступные группировки (среди них Картель Халиско – Новое поколение), которые используют криптообменники для ОД в результате незаконной торговли наркотиков как наиболее удобный инструмент в связи с оперативностью и анонимностью проведения операций в блокчейн. Этому также способствует тот факт, что большинство операторов криптообменников продолжают работать без регистрации в качестве операторов по переводу денежных средств (money services businesses) и с нарушениями требований противолегализационного законодательства.

<sup>11</sup> Convertible virtual currency kiosks.

<sup>12</sup> Из них более 2/3 суммы приходится на мошеннические схемы в отношении пожилых клиентов.

FinCEN призывает финансовые организации усилить надзор за подозрительной активностью, связанной с использованием криптообменников, с применением перечня индикаторов подозрительности, предусматривающего в том числе следующие индикаторы: (1) дробление операций на суммы, не превышающие пороговые значения для направления отчётности; (2) перемещение криптовалюты между кошельками, связанными с известными схемами мошенничества; (3) использование криптообменников пожилыми лицами, ранее не осуществлявшими операции с криптовалютой и др.

*Источник информации: официальный сайт FinCEN в сети Интернет.*

**6 августа 2025 года** подразделением финансовой разведки Канады (Financial Transactions and Reports Analysis Centre, FINTRAC) опубликованы актуализированные принципы применения административных мер воздействия (штрафных санкций) за нарушения Закона о ПОД/ФТ<sup>13</sup>.

За нарушения противолегализационного законодательства предусмотрены следующие диапазоны штрафных санкций (из расчёта за одно нарушение):

- за незначительные нарушения от 1 до 1 000 канадских долларов<sup>14</sup>;
- за серьёзные нарушения от 1 до 100 000 канадских долларов<sup>15</sup>;
- за особо тяжкие нарушения от 1 до 100 000 канадских долларов (для физических лиц) и от 1 до 500 000 (для юридических лиц)<sup>16</sup>.

Субъекты исполнения противолегализационного законодательства, в отношении которых FINTRAC вынесено постановление о назначении штрафных санкций, вправе в течение 30 дней обжаловать такое решение непосредственно в FINTRAC или подать соответствующую апелляцию в Федеральный суд.

*Источник информации: официальный сайт FINTRAC в сети Интернет.*

**7 августа 2025 года** опубликовано мировое соглашение между Департаментом штата Нью-Йорк по надзору за рынком финансовых услуг (New York State Department of Financial Services, NYSDFS) и нью-йоркской финансовой организацией Paxos Trust Company, LLC (Paxos)<sup>17</sup> в связи с выявленными нарушениями законодательства в сфере ПОД/ФТ.

По результатам проверки NYSDFS установлено, что несмотря на действующее с 2020 г. соглашение о сотрудничестве с криптобиржей Binance Holdings Limited (в рамках выпуска и распространения стейблкоинов Binance USD (BUSD)), которым предусмотрена обязанность Paxos на регулярной основе проводить проверку в отношении Binance Holdings Limited<sup>18</sup> на предмет исполнения требований в сфере

<sup>13</sup> Administrative monetary penalties policy.

<sup>14</sup> Более 57,5 тыс. рублей в эквиваленте.

<sup>15</sup> Более 5,7 млн рублей в эквиваленте.

<sup>16</sup> Более 28,7 млн рублей в эквиваленте.

<sup>17</sup> Paxos Trust Company LLC – трастовая компания, специализирующаяся на блокчейн-технологиях и финансовых услугах; оказывает брокерские услуги по криптовалютам, услуги токенизации активов и расчётные услуги.

<sup>18</sup> По итогам анализа операций Binance Holdings Limited за период 2017–2022 гг. установлено, что через платформу криптовалютной биржи были проведены операции на сумму более 1,6 млрд

ПОД/ФТ, Paxos не были внедрены соответствующие механизмы внутреннего контроля в целях ПОД/ФТ. Кроме того, в программе по обеспечению соблюдения противолегализационных требований Paxos были выявлены системные недостатки, связанные в том числе с ненадлежащим применением мер НПК и неэффективным мониторингом операций клиентов.

Сумма штрафа за нарушения противолегализационного законодательства для компании составила 26,5 млн долларов США (более 2,1 млрд рублей в эквиваленте). Кроме того, компания обязуется дополнительно выделить сумму в размере 22 млн долларов США для совершенствования программы ПОД/ФТ.

*Источник информации: официальный сайт FinCEN в сети Интернет.*

**12 августа 2025 года** опубликован доклад Европейской службы банковского надзора (European Banking Authority, EBA) о результатах оценки эффективности использования надзорными органами стран - членов Европейского союза (ЕС) и некоторыми третьими странами<sup>19</sup> технологий SupTech в целях ПОД/ФТ<sup>20</sup>.

Несмотря на заметный прогресс в части разработки и применения инструментов SupTech (к настоящему времени надзорными органами реализуются 60 проектов по разработке или применению инструментов SupTech), в целом применение надзорными органами указанных технологий отличается неравномерностью и находится преимущественно на этапе становления.

Низкое качество данных, нехватка ресурсов, правовая неопределенность, операционные и репутационные риски, а также сопротивление внутри организаций могут затормозить процесс внедрения инструментов SupTech. Большинство надзорных органов сообщает об «умеренной» готовности к интеграции в полном объёме инновационных инструментов, а разработка SupTech, как правило, осуществляется изолированно, что приводит к рискам дублирования и проблемам в части функциональной совместимости инструментов.

Имеющиеся у надзорных органов инструменты SupTech в настоящее время преимущественно используются для оценки рисков и управления данными.

*Источник информации: официальный сайт EBA в сети Интернет.*

**18 августа 2025 года** опубликована информация о внесении изменений в Указание Резервного банка Индии «О применении мер надлежащей проверки клиентов»<sup>21</sup> (далее – Указание об НПК), регламентирующих порядок идентификации клиентов и контроля за операциями.

Резервным банком Индии отмечается, что внесённые в законодательство изменения направлены на достижение баланса между соблюдением требований

---

долларов США с участием субъектов, вовлечённых в противоправную деятельность, включая операции с лицами, в отношении которых действуют санкции Управления валютного контролёра США (OFAC).

<sup>19</sup> В опросе ЕВА приняли участие 31 надзорный орган из 25 стран - членов ЕС и 3 надзорных органа стран, не являющихся членами ЕС.

<sup>20</sup> Report on the Use of AML/CFT SupTech Tools. SupTech – технологии, используемые регуляторами для повышения эффективности контроля и надзора за деятельностью участников финансового рынка.

<sup>21</sup> Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016.

в сфере ПОД/ФТ и доступностью финансовых услуг для всех категорий граждан, включая социально и финансово уязвимые группы.

Основные изменения предусматривают:

(i) обеспечение защиты уязвимых групп населения:

- банки обязаны обеспечивать равный доступ к финансовым услугам;
- банкам запрещено отклонять заявки на открытие счетов или обновление информации о клиенте в рамках НПК без детального рассмотрения и письменной фиксации причин отказа;
- в правилах закреплены положения о защите прав лиц с ограниченными возможностями.

(ii) расширение требований к идентификации клиентов:

Обязательная идентификация клиента предусмотрена не только при установлении деловых отношений, но и при:

- проведении разовых операций на сумму равную или более 50 000 индийских рупий<sup>22</sup> (включая связанные операции);
- при любых трансграничных денежных переводах.

(iii) применение новых методов аутентификации:

- допускается использование Aadhaar Face Authentication<sup>23</sup> наряду с другими методами;
- при удалённом принятии на обслуживании клиента предусмотрено обязательное применение «проверки на присутствие» (liveness check), которая не должна приводить к исключению лиц с особыми потребностями.

*Источник информации: официальный сайт Резервного банка Индии в сети Интернет.*

**25 августа 2025 года Центральным банком Нидерландов (De Nederlandsche Bank, DNB) опубликован пресс-релиз о текущем статусе применения штрафных санкций<sup>24</sup> к банку Bnpq B.V.<sup>25</sup> в связи с серьёзными нарушениями требований законодательства в сфере ПОД/ФТ.**

По результатам проверки DNB были выявлены систематические нарушения противолегализационного законодательства, которые были допущены банком в

---

<sup>22</sup> Около 46 тыс. рублей в эквиваленте.

<sup>23</sup> Aadhaar Face Identification – это биометрический механизм аутентификации, используемый в индийской системе Aadhaar, в котором сравнивается лицо пользователя с его зарегистрированным изображением в базе данных Aadhaar для подтверждения личности и обеспечения безопасного доступа к услугам и сервисам. Aadhaar является крупнейшим в мире национальным проектом по цифровой биометрической идентификации населения.

<sup>24</sup> Штрафные санкции к банку были применены DNB в мае 2025 года, информация о них опубликована только сейчас. Указанные меры были оспорены банком, в связи с чем было подано соответствующее обращение. Процедура рассмотрения указанного обращения ещё не завершена.

<sup>25</sup> Bnpq B.V. – один из крупнейших цифровых банков Европы, нидерландская финтех компания.

период с января 2021 по май 2022 гг. и связаны с ненадлежащим функционированием механизмов внутреннего контроля.

Банком (i) не осуществлялся должным образом мониторинг подозрительных операций клиентов (в связи с неэффективностью системы мониторинга операций); (ii) не применялись меры по выявлению и снижению рисков совершения финансовых преступлений в установленные законодательством сроки; (iii) не проводились или проводились в недостаточном объёме проверки в отношении оповещений системы внутреннего контроля по ПОД/ФТ о рисках ОД/ФТ.

Сумма штрафа для банка составила 2,6 млн евро (около 243 млн рублей в эквиваленте).

*Источник информации: официальный сайт DNB в сети Интернет.*