Маркина Олеся Викторовна
слушатель
Научный руководитель
Логинова Наталья Анатольевна
д-р экон. наук, доцент, профессор
ФГКОУ ВО «Санкт-Петербургский университет МВД России»
г. Санкт-Петербург

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ: СУЩНОСТЬ, УГРОЗЫ МОШЕННИЧЕСТВА И ЛЕГАЛИЗАЦИЯ ДОХОДОВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: *в работе раскрывается сущностьэкономической безопасности как многоуровневой системы в условиях цифровизации финансовых услуг. Анализируется трансформация угроз мошенничества и легализации доходов, полученных преступным путём. Рост масштаба и скорости атак, смещение фокуса на социальную инженерию, индустриализация преступной деятельности и компрометация цифровой идентичности. На основе данных Банка России за 2021–2025 гг. показана динамика операций без добровольного согласия клиентов и эффективность систем предотвращения. Обосновывается необходимость перехода от преимущественно транзакционного мониторинга к профильному риск-ориентированному анализу на уровне лица (цифровой профиль личности). Рассматриваются индикаторы риска, возможности межбанковского обмена сведениями и правовые ограничения, связанные с обработкой персональных данных.*

Ключевые слова: *экономическая безопасность, мошенничество, легализация доходов, цифровизация, риск-ориентированный подход, цифровой профиль личности, Банк России, персональные данные.*

Цель исследования состоит в том, чтобы раскрыть сущность экономической безопасности как многоуровневой системы. Проанализировать как трансформируются угроз мошенничества и легализации доходов под влиянием циф-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

ровых технологий, а также обосновать необходимость перехода от преимущественно транзакционного мониторинга к профильному риск-ориентированному на уровне лица.

Сама категория экономической безопасности в Отечественной науке сформировалась в первой половине девяностых годов. Это стало ответом на системный кризис переходной экономики. Л.И. Абалкин рассматривал ее как состояние экономической системы, позволяющее динамично и эффективно развиваться, решать социальные задачи и обеспечивать государству возможность проводить самостоятельную экономическую политику [4; 7; 9]. Угрозы понимались как факторы, которые способны вывести систему из данного состояния.

В дальнейших работах акцент сменился на многоуровневую структуру объектов. Е.А. Олейникова выделяла уровни государства, региона и личности [4; 7; 9]. Угрозы на каждом уровне имеют собственную природу, но взаимосвязаны. Современные исследователи В.И. Авдийский, В.А. Дадалко, Н.Г. Синявский, Е.И. Кузнецова, В.Ш. Уразгалиев развивают этот подход [1; 2; 4; 7]. Они выделяют в системе обеспечения экономической безопасности объекты, субъекты, механизмы и инструменты. Особое внимание обращают на финансовую безопасность, так как она является ключевой составляющей, связанной с устойчивостью денежно-кредитной и банковской систем. Экономическая безопасность личности определяется защищенностью ее доходов и сбережений от противоправных посягательств.

Содержание этой категории на нормативном уровне раскрыто в Стратегии экономической безопасности Российской Федерации на период до 2030 года. Экономическая безопасность определяется как состояние защищенности национальной экономики от внешних и внутренних угроз, обеспечивая экономический суверенитет страны, единство ее экономического пространства и условия для реализации стратегических национальных приоритетов [6].

Среди вызовов и угроз Стратегия называет высокий уровень криминализации и коррупции в экономической сфере, а также сохранение значительной доли теневой экономики. Концепция развития национальной системы ПОД ФТ

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

ориентирует участников на риск-ориентированный подход и применение современных технологий анализа данных.

Важно отметить, что цифровизация финансовых услуг изменила угрозы по меньшей мере в пяти измерениях.

Первым является масштаб атак. Что раньше требовало личного участия злоумышленников, а также затрачивало большое количество времени, на сегодняшний день автоматизируется. Например, массовый обзвон потенциальных жертв, рассылка сообщений, подбор паролей, регистрация фиктивных учетных записей выполняются программными средствами практически без участия человека. Себестоимость одной попытки фактически обнулилась, поэтому доходность всей схемы теперь определяется исключительно количеством совершённых атак. Поэтому даже при очень высокой эффективности банковских систем защиты, потери продолжают расти. Поток атак увеличивается быстрее, чем совершенствуются средства выявления и предотвращения хищений.

Вторым изменением является скорость. Сокращение времени между хищением и выводом средств. Быстрые платежи и круглосуточное дистанционное обслуживание позволяют преступникам завершать операцию за пару минут. Классические процедуры финансового мониторинга, которые построены на последующем анализе операций, уже не успевают за скоростью современных преступных схем.

Третьим элементом является смена фокусирования атаки с технической системы на человека. Так как техническая защита банковских систем все чаще совершенствуются, то злоумышленники стали чаще атаковать самого клиента, побуждая его выполнить операцию добровольно под влиянием обмана. Данная процедура формально проходит все процедуры аутенфикации. Законодатель отреагировал на эту угрозу, расширив понятие перевода без согласия клиента и включив в него случаи, когда согласие было получено под влиянием обмана или злоупотребления доверием. Сам факт необходимости такого расширения показывает, насколько глубоко изменилась природа угрозы.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Четвертое существенное изменение связано с индустриализацией преступной деятельности. Мошенничество с использованием цифровых технологий превратилось в самостоятельную отрасль с выстроенным разделением труда. Одни участники занимаются добычей и продажей баз персональных данных, другие проводят массовые обзвоны абонентов и занимаются социальной инженерией, третьи предоставляют банковские карты и счета для приёма похищенных средств, а четвёртые обеспечивают быстрый вывод денег в наличные или криптовалюту. Такая специализация заметно повышает эффективность преступных схем и одновременно сильно затрудняет их полное раскрытие, ведь каждый участник отвечает только за свой узкий участок работы.

Пятым изменением является компрометация самой личности. Массовые утечки и быстрое развитие технологий открыли злоумышленникам новые возможности. Теперь они могут не только собирать подробную информацию о жертве, но и убедительно имитировать её голос и внешность. Особенно опасными такие технологии становятся при удалённом открытии счетов и прохождении биометрической идентификации. Технологии имитации голоса и внешности всё чаще используют именно для массового создания фиктивных аккаунтов, которые впоследствии задействуют в схемах отмывания денег. Из-за этого опасность угрожает уже цифровой идентичности человека.

В совокупности, эти пять изменений превратили мошенничество и легализацию доходов в интегрированный, быстротекущий и высокоорганизованный процесс [4; 7; 10]. Угроза приобрела системный характер и напрямую затрагивает экономическую безопасность на уровне личности, финансовых организаций и государства в целом.

Статистика Банка России позволяет достаточно полно оценить динамику и масштабы угрозы [5]. Данные об операциях без добровольного согласия клиентов за период 2021–2025 годов приведены в таблице 1 и наглядно отражены на рисунке 1.

Таблица 1

Операции без добровольного согласия клиентов 2021–2025 гг.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Показатель	2021	2022	2023	2024	2025
Объем операций без добровольного согласия клиентов, млрд руб.	13,6	14,2	15,8	27,5	29,3
Темп прироста к предыдущему году, %	+38,8	+4,3	+11,5	+74,4	+6,4
Объем предотвращенных операций, трлн руб.	-	-	5,8	13,5	13,9
Количество предотвращенных операций, млн	-	-	34,8	72,2	134,2
Доля возвращенных клиентам средств, %	-	-	-	9,8	5,9

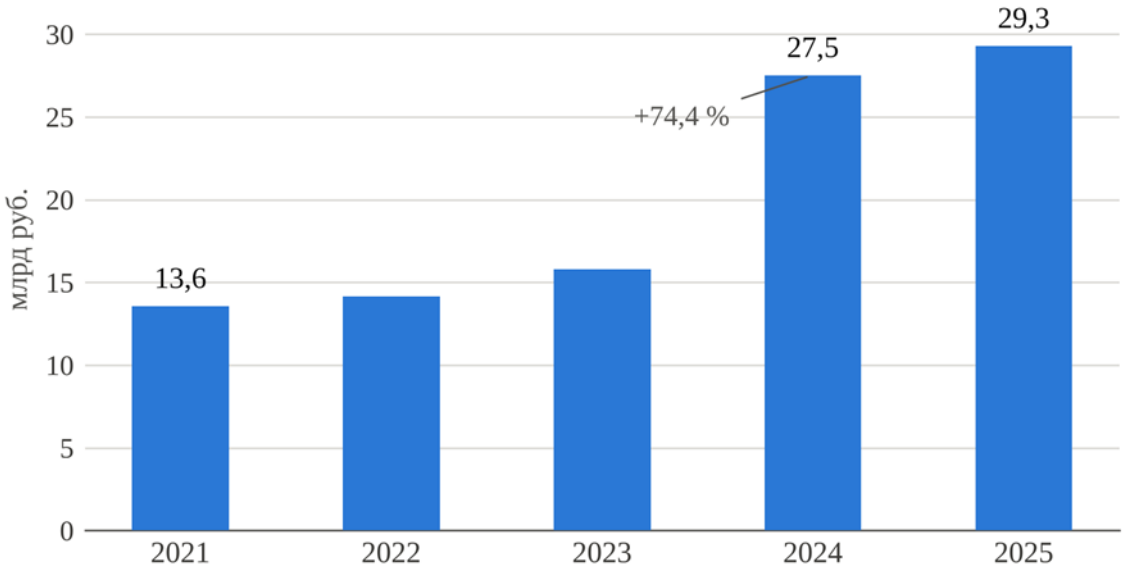


Рис. 1. Динамика объема операций без добровольного согласия клиентов в Российской Федерации 2021–2025 гг., млрд руб.

Исходя из представленных показателей видно, что объём таких операций за пять лет вырос более чем в два раза с 13,6 миллиарда рублей в 2021 году до 29,3 миллиарда рублей в 2025 году. Особенно резкий скачок произошёл в 2024 году, когда объём хищений увеличился на 74,4% и достиг 27,5 миллиарда рублей. Этот рост во многом связан со смещением акцента злоумышленников на социальную инженерию и увеличением средних сумм похищаемых средств.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

В 2025 году темп прироста существенно замедлился и составил всего 6,4%, однако количество операций при этом выросло на 31,2%. Регулятор связывает увеличение числа зафиксированных случаев с введением в приложениях крупных банков обязательной функции быстрого сообщения о мошенничестве, что позволило клиентам чаще заявлять о сравнительно небольших суммах ущерба.

Одновременно заметно выросла эффективность работы банковских систем защиты. Если в 2023 году было предотвращено 34,8 миллиона мошеннических операций на сумму 5,8 триллиона рублей, то в 2024 году эти показатели выросли до 72,2 миллиона операций и 13,5 триллиона рублей, а в 2025 году до 134,2 миллиона операций и 13,9 триллиона рублей. Таким образом на один похищенный рубль приходится уже несколько сотен рублей, сохранённых благодаря своевременному выявлению подозрительных операций. Вместе с тем доля средств, возвращённых клиентам, остаётся низкой и в 2025 году снизилась до 5,9% против 9,8% годом ранее.

Анализ структуры хищений показывает, что наибольшие суммы в 2025 году приходились на операции по счетам без использования платёжных карт и на переводы через Систему быстрых платежей (СБП). Это свидетельствует о смещении преступной активности в каналы мгновенных расчётов, где время на реакцию банковских систем минимально.

Однако, приведенная банковская статистика отражает лишь часть реального ущерба. По оценкам, охватывающим весь рынок. По более широким оценкам, которые охватывают весь рынок и учитывают в том числе передачу наличных курьерам, а также потери от инвестиционного мошенничества, объём средств, похищенных у граждан в 2025 году, оказывается существенно выше и достигает примерно от 275 до 285 миллиардов рублей. Такая разница объясняется тем, что значительная часть ущерба возникает за пределами банковского контура и поэтому не отражается в отчётности по операциям без добровольного согласия.

Таким образом, несмотря на очевидный прогресс в работе систем предотвращения мошенничества, абсолютные потери граждан продолжают оставаться

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

высокими, а сама угроза приобретает всё более массовый и системный характер.

Что касаемо легализации доходов, полученных преступным путем, то данный процесс описывается трехстадийной моделью, в которую входят:

1) размещение средств в финансовой системе;

2) многослойноеперемещениедля разрыва связи с источником;

3) интеграция в легальный оборот.

Экономический ущерб от легализации доходов, добытых преступным путем значительно шире последствий отдельных преступлений. Такая деятельность искажает ценовые сигналы на рынках, подрывает честную конкуренцию, сокращает налоговые поступления и одновременно создаёт дополнительные стимулы для совершения новых предикатных преступлений.

В Российской Федерации традиционные схемы с участием юридических лиц под воздействием платформы «Знай своего клиента» и мер банковского надзора постепенно сокращаются [3; 5]. Теперь злоумышленники все чаще используют счета обычных людей. Одновременно сохраняется проблема вовлечения физических лиц в обналичивание средств. Эти процессы не означают полного вытеснения одних схем другими. По данным Банка России, в 2025 году общий объем подозрительных операций в банковском секторе снизился [5].

В цифровой среде стадии размещения средств, их дальнейшего перемещения и включения в легальный оборот часто следуют друг за другом. Деньги, которые получены в результате мошеннических действий перемещаются между счетами различных физических лиц, дробятся на небольшие суммы, направляются на электронные кошельки, либо конвертируются в цифровые активы. В силу этого каждая отдельная операция сама по себе не может не может вызывать подозрений. При анализе всей последовательности переводов и характера связей между участниками становится очевидным, что денежные средства используются только для быстрого перемещения между счетами.

Для выявления таких схем важна не только сумма, а сочетание признаков во времени и в сети взаимосвязанных счетов. К таким сигналам относятся тран-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

зитные операции, значительные объемы переводов между физическими лицами, их концентрация в короткие интервалы, отсутствие понятных источников поступлений и обычных расходов. Совокупность подобных сигналов должна становиться основанием для дополнительной проверки сотрудником банка.

Примеры сочетаний признаков, которые могут использоваться при анализе цифрового профиля личности, представлены в таблице 2.

Таблица 2

Примеры индикаторов риска для анализа цифрового профиля личности

Участник или схема	Возможные сигналы для дополнительной проверки	Что позволяет заметить профильный анализ
Потерпевший от социальной инженерии	Резкое отклонение от привычного поведения, перевод новому получателю, несколько операций за короткое время	Сопоставление с обычной историей операций и выявление нетипичной последовательности
Захват учетной записи	Изменение устройства или контактных данных, вход в нетипичное время, изменение настроек безопасности	Связь изменений средств доступа с последующими операциями
Дропперство	Многочисленные поступления от разных лиц с быстрым выводом, транзитный характер операций	Выявление повторяющихся цепочек переводов и связей между счетами
Фиктивная или подмененная учетная запись	Аномалии при дистанционной идентификации, несколько счетов с похожими признаками, отсутствие обычной активности	Сопоставление сведений об идентификации и последующем поведении счета
Организатор или сеть посредников	Повторяющиеся связи между множеством счетов и устройств, согласованные переводы в короткие интервалы	Анализ сети взаимосвязанных счетов, а не каждой операции по отдельности

В настоящей работе цифровой профиль личности понимается как формируемая на законном основании совокупность сведений, необходимых для сопоставления текущих операций с подтвержденным обычным поведением клиента и выявления связей между подозрительными операциями. В него могут входить история переводов и снятия наличных, динамика сумм и частоты операций, связи счетов с повторяющимися контрагентами, сведения об изменениях средств доступа и подтвержденные данные об источниках дохода.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Профильный анализ дополняет транзакционный контроль. На уровне отдельной операции выявляется отклонение от обычного шаблона. Анализ временной последовательности помогает обнаружить быстрое получение и вывод средств. Анализ связей между счетами позволяет увидеть цепочку транзитных переводов, в том числе распределённых по разным банкам.

Практическим примером развития межбанковского обмена сведениями является платформа «Антидроп». Банк России сообщил о начале её разработки в 2025 году. На момент подготовки работы она находится в стадии проектирования и должна рассматриваться как перспективное направление развития системы, а не как уже действующий повсеместно механизм.

Стадии преступного цикла и возможные точки контроля на основе цифрового профиля личности схематично показаны на рисунке 2.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

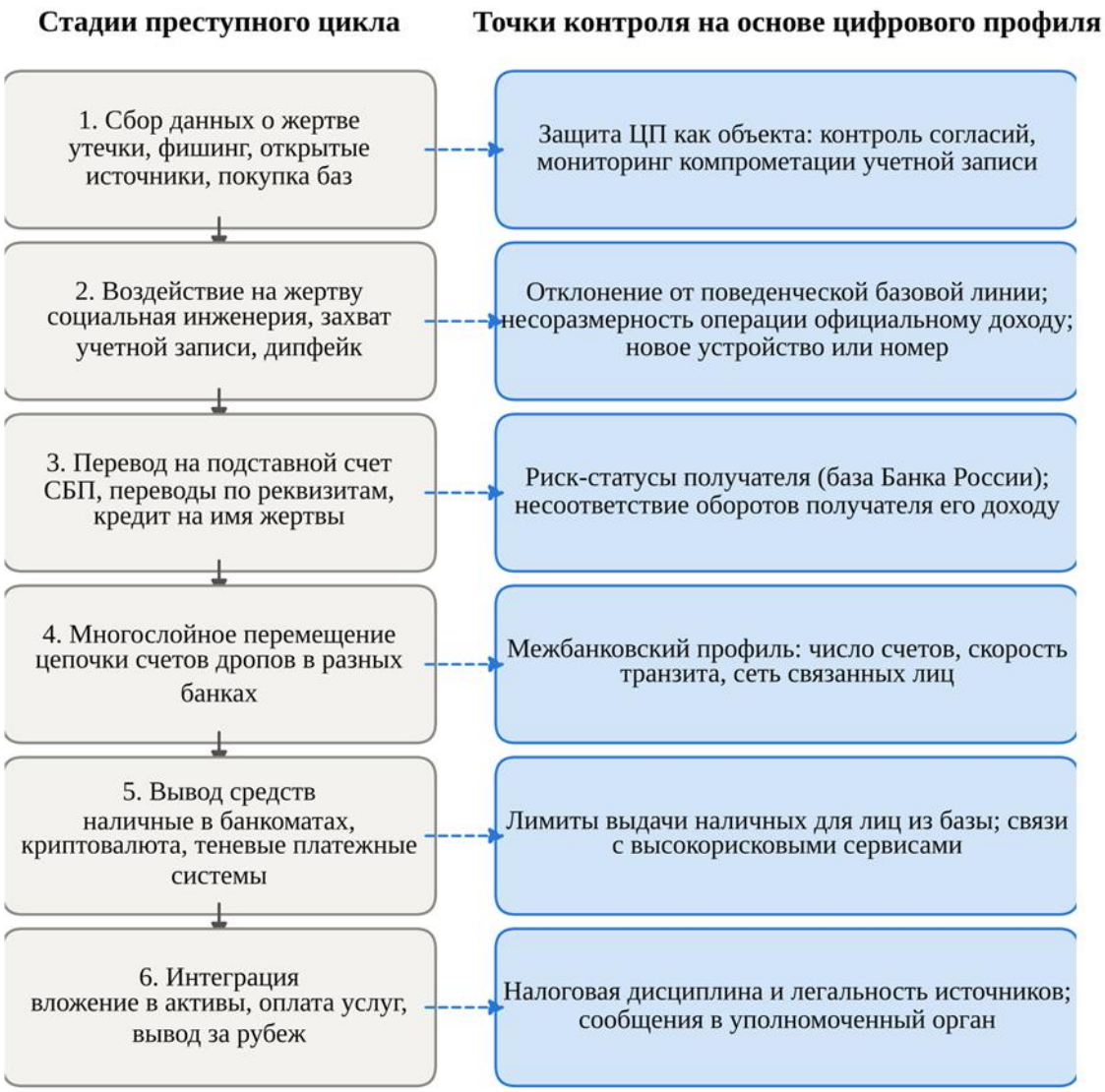


Рис. 2. Цикл «мошенничество – легализация доходов» в цифровой среде и возможные точки контроля на основании ЦПЛ

Схема показывает, как средства могут перемещаться от потерпевшего через счета посредников, к каналам обналичивания или иного вывода. Сопоставление операций с профилем клиента и связями между счетами может помочь обнаружить нетипичные последовательности на нескольких этапах этого цикла.

Внедрение профильного анализа связано и с риском ложных срабатываний. Нетипичный перевод может иметь вполне законное объяснение. Например, продажа имущества, сбор средств на лечение или помощь родственнику. Поэтому сигнал риска должен запускать проверку обстоятельств, а не автоматически закреплять за человеком статус правонарушителя.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Использование цифрового профиля должно учитывать требования Федерального закона №152-ФЗ «О персональных данных» [8]. Закон ограничивает принятие решений, затрагивающих права и законные интересы человека, исключительно на основании автоматизированной обработки. Для риск-ориентированного мониторинга это означает необходимость проверяемых критериев, обязательного участия уполномоченного сотрудника в спорных случаях, возможности исправления неточных сведений и строгого ограничения использования данных заявленной целью.

Таким образом, переход от анализа отдельной транзакции к анализу риск-профиля личности способен повысить возможность выявлять последовательности и связи, которые остаются незаметными в пределах одного банка или одной операции. Вместе с тем цифровой профиль следует рассматривать как инструмент предварительного выявления риска, а не как автоматическое доказательство противоправного поведения. Его результативность необходимо оценивать по способности предотвращать ущерб, снижать долю ложных сигналов и сохранять доступ добросовестных клиентов к финансовым услугам [4; 7; 10].

Проведенный анализ показывает, что цифровизация ускорила и сделала мошенничество более масштабным, а использование счетов физических лиц позволяет быстро перемещать и маскировать преступные доходы. Официальные данные Банка России подтверждают, что вышеперечисленные меры и контроль подозрительных операций развиваются, однако статистика по отдельным сегментам описывает разные явления и требует корректного сопоставления.

Переход от анализа отдельной транзакции к анализу цифрового профиля личности может повысить способность выявлять связи, незаметные в пределах одного банка или одной операции. Также цифровой профиль следует рассматривать как инструмент предварительного выявления риска. Его результативность необходимо оценивать по способности предотвращать ущерб, снижать долю ложных сигналов и сохранять доступ добросовестных клиентов к финансовым услугам.

Список литературы

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

1. Авдийский, В. И. Национальная и региональная экономическая безопасность России: учеб. пособие / В. И. Авдийский, В. А. Дадалко, Н. Г. Синявский. – Москва : ИНФРА-М, 2017. – 363 с. – URL: https://znanium.ru/catalog/document?id=435956 (дата обращения: 18.11.2026). – Текст : электронный.

2. Авдийский, В. И. Теневая экономика и экономическая безопасность государства: учеб. пособие. 3-е изд., перераб. и доп / В. И. Авдийский, В. А. Дадалко, Н. Г. Синявский. – Москва : ИНФРА-М, 2018. – 538 с. – URL: https://library.cbr.ru/catalog/lib/books/262457/ (дата обращения: 18.11.2026). – Текст : электронный.

3. Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма (утв. Президентом РФ 30.05.2018). – URL: https://www.consultant.ru/document/cons_doc_LAW_299375/ (дата обращения: 18.11.2026). – Текст : электронный.

4. Кузнецова, Е. И. Экономическая безопасность: учебник и практикум для вузов. 3-е изд., перераб. и доп / Е. И. Кузнецова. – Москва : Юрайт, 2025. – 338 с. – URL: https://urait.ru/bcode/561732 (дата обращения: 18.11.2026). – Текст : электронный.

5. Обзор операций, совершённых без добровольного согласия клиентов финансовых организаций: аналитические материалы Банка России за 2021–2025 гг. – URL: https://cbr.ru/analytics/ib/operations_survey/2025/ (дата обращения: 18.11.2026). – Текст : электронный.

6. Стратегия экономической безопасности Российской Федерации на период до 2030 года: утв. Указом Президента Российской Федерации : от 13.05.2017 №208. – URL: https://www.consultant.ru/document/cons_doc_LAW_216629/ (дата обращения: 18.11.2026). – Текст : электронный.

7. Уразгалиев, В. Ш. Экономическая безопасность: учебник и практикум для вузов. 2-е изд., перераб. и доп. / В. Ш. Уразгалиев. – Москва : Юрайт,

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

2022. – 725 с. – URL: https://urait.ru/bcode/489524 (дата обращения: 18.11.2026). – Текст : электронный.

8. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (в ред. на 2026 г.). – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 18.11.2026). – Текст : электронный.

9. Гончаренко, Л. П. (ред.). Экономическая безопасность : учебник для вузов. 3-е изд., перераб. и доп / Л. П. Гончаренко. – Москва : Юрайт, 2026. – 370 с. – URL: urait.ru/bcode/583017 (дата обращения: 18.11.2026). – Текст : электронный.

10. Меньшов, В. Н. Цифровое мошенничество как угроза экономической безопасности России: проблема измерения ущерба и оценка эффективности мер противодействия / В. Н. Меньшов // Прогрессивная экономика. – 2026. – URL: progressive-economy.ru (дата обращения: 18.11.2026). – Текст : электронный.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)