Научная специальность: 5.2.4. Финансы
УДК 336.71
DOI:

ОЦЕНКА И МЕТОДЫ БОРЬБЫ С КИБЕРМОШЕННИЧЕСТВОМ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ РФ

КРИВОШАПОВА Светлана Валерьевна, кандидат экономических наук, доцент кафедры «Экономики и управления» Владивостокского государственного университета
Владивостокский государственный университет (690014, Россия, Владивосток, улица Гоголя 41, e-mail: svetlana.krivoshapova@vvsu.ru)

SPRIN: 3812-9760
AuthorID: 768866;
ORCID: 0000-0002-1457--4369.
ScopusID: 57200409029

ПАТКИНА Арина Вячеславовна, выпускница 4-го курса бакалавриата кафедры «Экономики и управления» направление специальности «Экономическая безопасность» Владивостокского государственного университета
Владивостокский государственный университет (690014, Россия, Владивосток, улица Гоголя 41, e-mail amorekova@bk.ru)

ПОШИВАЙЛО Игорь Владимирович, выпускник 4-го курса бакалавриата кафедры «Экономики и управления» направление специальности «Экономическая безопасность» Владивостокского государственного университета
Владивостокский государственный университет (690014, Россия, Владивосток, улица Гоголя 41, e-mail: poshik_666@vk.com)

Аннотация. В статье представлено исследование угроз кибермошенничества в системе экономической безопасности кредитных организаций и способы развития технологий краудсорсинга в банковском управлении. Информация, полученная в результате данного исследования, может быть потенциально полезна в принятии управленческих решений по улучшению системы безопасности банков и развитии деятельности по защите конфиденциальных данных пользователей. Материалами исследования выступают статистические данные, учебные пособия по банковскому делу, публикуемые Центральным Банком России. Сделаны выводы о том, что подавляющее большинство инцидентов вызвано человеческим фактором, а не техническими уязвимостями. Также в данной статье рассмотрены специфические особенности функционирования системы безопасности банка, включая использование методов краудсорсинга в борьбе с кибермошенничеством. Полученные результаты могут способствовать разработке комплексной системы защиты данных на основе краудсорсинга, что, в свою очередь, сократит инциденты, связанные с кибермошенничеством.

Ключевые слова: краудсорсинг, кибермошенничество, система безопасности, операции без согласия клиентов, деятельность по защите конфиденциальных данных

ACCESSIBILITY OF BANKING SERVICES TO SMALL AND MEDIUM-SIZED BUSINESSES

KRIVOSHAPOVA Svetlana Valerievna, candidate of Economic Sciences, associate professor of the department of Economics and Management, Vladivostok State University
Vladivostok State University (690014, Russia, Vladivostok, street Gogolya, 41, e-mail: *svetlana.krivoshapova@vvsu.ru*)

PATKINA Arina Vyacheslavovna, graduate of the 4th year of bachelor's degree of the department of «Economics and management» specialty «Economic Security»
Vladivostok State University (690014, Russia, Vladivostok, street Gogolya, 41, e-mail ak-i@list.ru)

POSHIVAILO Igor Vladimirovich, graduate of the 4th year of bachelor's degree of the department of «Economics and management» specialty « Economic Security »
Vladivostok State University (690014, Russia, Vladivostok, street Gogolya, 41, e-mail poshik_666@vk.com)

Abstract. The article presents a study of the threats of cyberbullying in the economic security system of credit institutions and ways to develop crowdsourcing technologies in banking management. The information obtained as a result of this research can be potentially useful in making managerial decisions to improve the security system of banks and develop activities to protect confidential user data. The research materials are statistical data and textbooks on banking published by the Central Bank of Russia . It is concluded that the vast majority of incidents are caused by human factors rather than technical vulnerabilities. This article also discusses the specific features of the bank's security system, including the use of crowdsourcing methods in the fight against cyberbullying. The results obtained can contribute to the development of a comprehensive crowdsourcing-based data protection system, which, in turn, will reduce incidents related to cyberbullying.

Keywords: crowdsourcing, cyberbullying, security system, operations without customer consent, activities to protect confidential data

ВВЕДЕНИЕ

Сегодня особенно тревожной тенденцией в рамках экономической безопасности финансовых организаций является рост несанкционированных операций по переводам денежных средств через системы банковского обслуживания. Исследование экономической безопасности кредитных организаций РФ в связи с увеличением количества несанкционированных операций по переводам денежных средств помогает определить причины роста кибермошенничества в экономической среде.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

Теоретической и методической основой исследования послужили труды отечественных учёных в области экономической безопасности кредитных организаций, таких как Т.Е Даниловских [1], А.В.Корень [2], В. А. Водопьянова [3], В.С.Просалова [4] и др.

Информационной базой исследования послужили данные, полученные на сайтах кредитных организаций РФ, статистические данные и финансовая отчетность Центрального Банка РФ, и нормативно-правовые акты РФ.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Особенно тревожной тенденцией, выявленной в рамках анализа экономической безопасности кредитных организаций является рост несанкционированных операций по переводам денежных средств через системы дистанционного банковского обслуживания. По итогам анализа объема кибератак на финансовые организации с середины 2023 года по конец первой половины 2024-го, представленного на рисунке 1, было зафиксировано, что 65% объявлений касаются именно банковских организаций [5]. Остальную долю атакуемых финансовых организаций на теневом рынке составляют страховые компании (11%), кредитные организации (6%), операторы платежных систем (2%) и другие предприятия (16%), в число которых входят профессиональные участники рынка ценных бумаг, инвестиционные фонды и др.

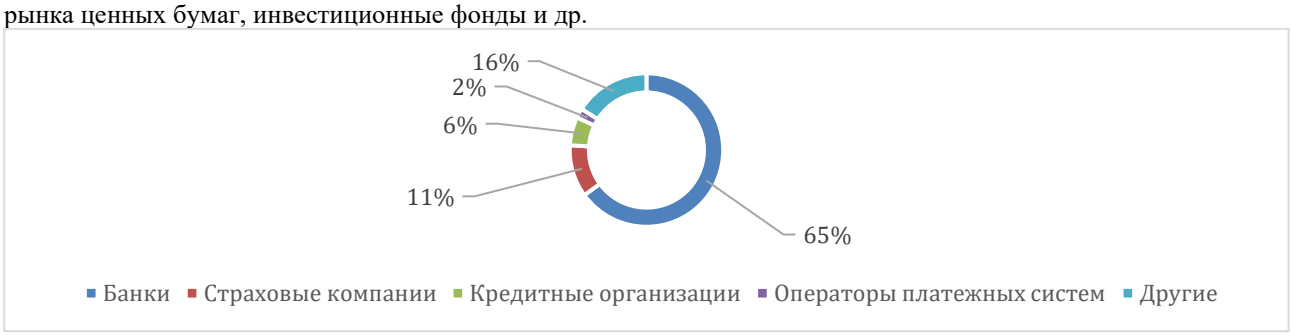

Рисунок 1 - Категории финансовых организаций подвергшихся кибератакам в 2023 г. и 1-2 квартале 2024 г. [11]

В обзоре Центрального банка, посвящённом операциям без согласия клиентов, зафиксирован рекордный показатель за всю историю ведения соответствующей статистики. В 2024 году отмечается значительный рост числа случаев мошенничества, связанных с хищением денежных средств с банковских счетов граждан Российской Федерации. Общий ущерб, причинённый в результате этих преступлений, составил 27,5 миллиарда рублей, что на 74,4% превышает аналогичный показатель за 2023 год [1]. В таблице 1 на примерах представлено, как мошенники модернизируют схемы обмана согласно современной информационной повестке [6].

Таблица 1- Ключевые макроэкономические сценарии 2024 г.

Событие норматива	Схема обмана
Пандемия COVID-19	Предложение о выгодной покупке специальных лекарств или выплате социальных пособий
Ежегодная сдача налоговых деклараций о доходах за прошлый год	Рассылка электронных писем с требованием оплатить налоги
Частичная мобилизация	Предложение приобрести отсрочку от призыва.
Отключение международных систем Visa и Mastercard	Предложение оформить международную банковскую карту для оплаты за рубежом

Для более подробного анализа объёмов хищения денежных средств обратимся к рисунку 2.

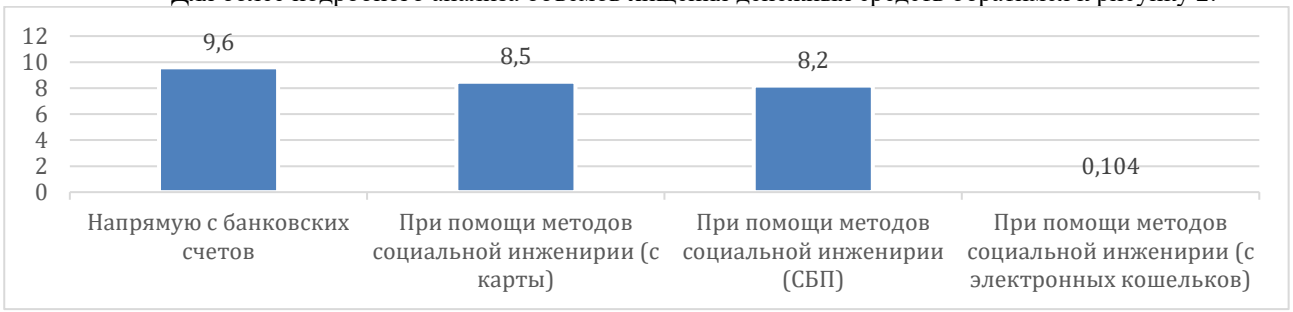

Рисунок 2 - Состав и объем хищения денежных средств в России в 1 и 2 квартале 2024 году, в млрд руб. [7]

В последнее время злоумышленники всё чаще атакуют не только клиентские платёжные приложения, но и саму информационную инфраструктуру банков. В связи с этим в обиход вошёл термин «киберриски».

Киберриски — это опасности, связанные с несанкционированным доступом и сбоями в работе банковских информационных систем. Согласно статистике с официального сайта Банка России, объем проведенных операций без добровольного согласия физических лиц увеличился в 2024 году на 74,36%, что наглядно представлено на рисунке 3.

Рисунок 3 - Операции без добровольного согласия физических и юридических лиц в 2023-2024 году.[5]

Каждый банк разрабатывает свои условия страхования рисков и защиты от кибератак, опираясь на внутренние экспертные оценки и учитывая специфику угроз в киберпространстве, что делает этот сегмент гибким и адаптивным. По итогам 2024 года Центральный Банк РФ зафиксировал следующие компьютерные инциденты и кибератаки, представленные на рисунке 4. Из данных рисунка становится ясно, что методы манипуляции поведением людей — это ключевой инструмент злоумышленников. Он включает фишинг, поддельные сообщения, выдачу себя за доверенных лиц и другие тактики. Высокий процент указывает на критическую важность обучения пользователей и сотрудников распознаванию таких атак.

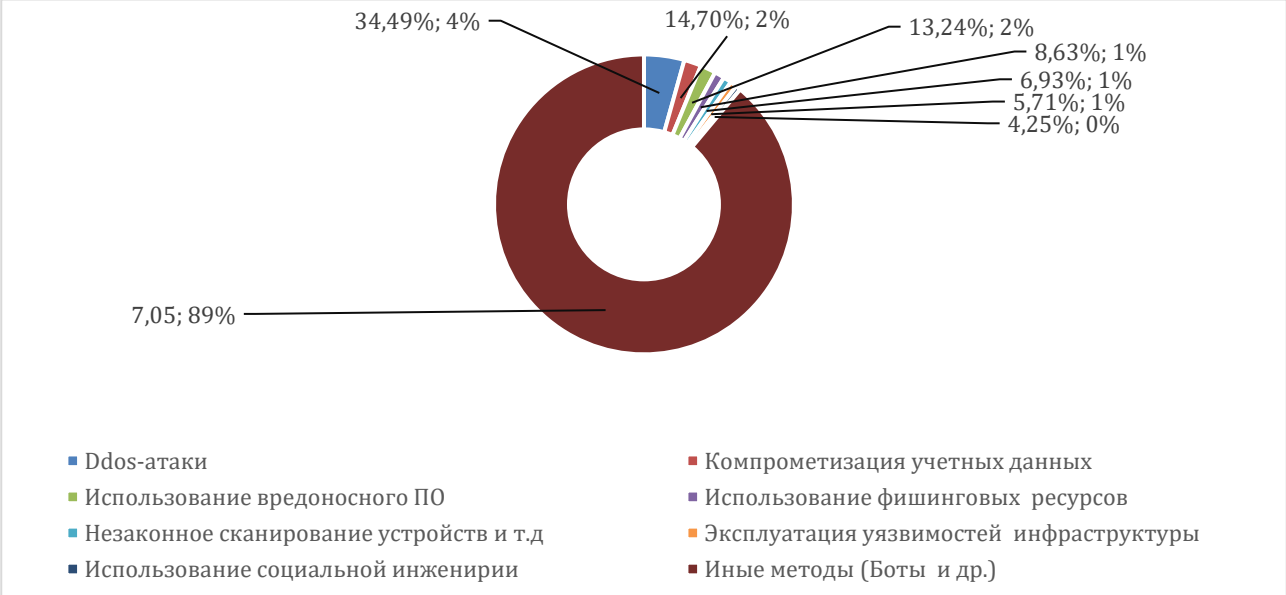

Рисунок 4 - Операции без добровольного согласия физических и юридических лиц в 2023-2024 году.[6]

Цифровые трансформации и рост объема обрабатываемых данных, сталкивают банки с широким спектром угроз информационной безопасности [7]. Мошеннические атаки все чаще направлены не только на клиентские платежные приложения, но и на информационную инфраструктуру самих банков. Злоумышленники стремятся получить доступ к критически важным данным, чтобы использовать их для кражи средств, распространения вредоносного программного обеспечения или саботажа. Согласно представленным данным на официальном сайте Банка России в 90% случаев мошеннических действий осуществляется психологическое давление на жертву [6]. Свыше 97% жертв пострадали по причине неосторожного обращения с личными данными. На рисунке 5 отражены виды данных, которые были получены в результате утечек из финансовых учреждений в 2023 и 1-2 квартале 2024 г.

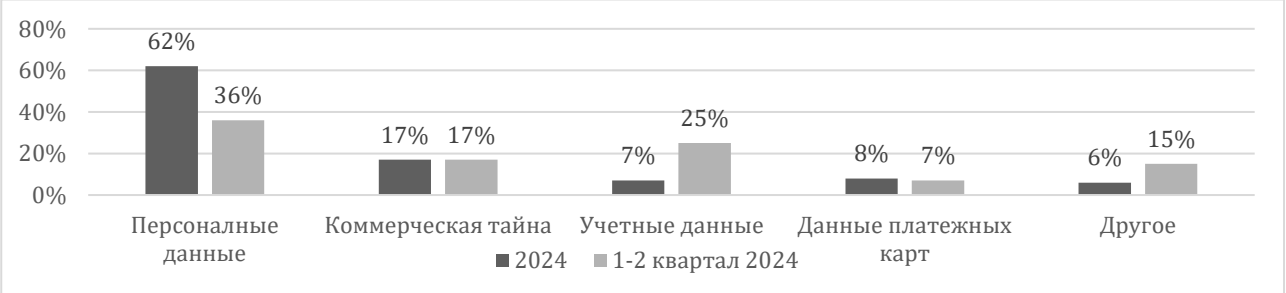

Рисунок 5 - Виды данных, полученные в результате утечек из финансовых учреждений в 2023 и 1-2 квартале 2024 г. [6]

Борьба с киберугрозами — это непрерывный процесс, требующий комплексного подхода. Важно не только внедрять современные технологии защиты инфраструктуры, но и уделять внимание человеческим ресурсам. Специалисты по кибербезопасности должны постоянно обновлять системы защиты, следить за новыми угрозами и оперативно реагировать на инциденты. В связи с постоянным ростом случаев мошенничества посредством краж личных данных большую популярность обрела идея интеграции механизма краудсорсинга в систему безопасности банков с целью предотвращения краж денежных средств. Краудсорсинг — это метод выявления и предотвращения мошенничества в цифровой среде, основанный на использовании коллективного интеллекта и добровольного участия пользователей для обнаружения подозрительных действий и потенциальных мошеннических схем [9]. Однако у краудсорсинга есть как достоинства, так и недостатки таблица 2.

Таблица 2- Недостатки и достоинства применения краудсорсинга в кредитных организациях РФ

Достоинства		Недостатки	
1.Снижение затрат	Кредитные организации могут получить доступ к знаниям и опыту широкого круга людей, что может привести к появлению новых идей для продуктов, услуг и бизнес-процессов.	1.Проблемы с конфиденциальностью	Обмен конфиденциальной информацией с большим количеством людей может привести к утечке данных и снижению уровня безопасности.
2.Доступ к широкому кругу специалистов	позволяет сократить затраты на разработку новых продуктов, маркетинг и оценку рисков, привлекая к решению задач внешних участников.	2. Качество работы	Не всегда возможно обеспечить высокий уровень качества работы, так как участники могут не иметь достаточной квалификации или мотивации.
3Повышение вовлеченности клиентов	Вовлечение клиентов в процесс разработки новых продуктов и услуг может повысить их лояльность и удовлетворенность.	3.Координация усилий	Управление большим количеством участников может быть сложной задачей, требующей значительных усилий по координации и контролю.
4Улучшение репутации банка	Участие в краудсорсинговых проектах может повысить репутацию так как это демонстрирует открытость и инновационность.	4.Проблемы с мотивацией	Сложно мотивировать участников, особенно если вознаграждение невелико или отсутствует.
5 Масштабируемость	позволяет быстро масштабировать команду, привлекая необходимое количество участников для решения конкретной задачи.	5.Необходимость адаптации	Краудсорсинг не всегда подходит для всех задач, особенно для тех, которые требуют высокой степени конфиденциальности или специфических знаний.
		6.Этические соображения	Краудсорсинг может поднимать вопросы о справедливости вознаграждения и защите интеллектуальной собственности.

Краудсорсинг, может быть необходимым инструментом для борьбы с кибермошенничеством в кредитных организациях, но необходимо тщательно планировать и учитывать риски банков. Скрупулезно прорабатывать направления, которые можно решить с помощью краудсорсинга.

В таблице 3 представлены и систематизированы методы и инструменты краудсорсинга, которые включают использование искусственного интеллекта и машинного обучения для анализа транзакций и выявления подозрительных операций.

Таблица 2- Направления и инструменты выявления и предотвращения мошенничества в кредитных организациях РФ при использовании краудсорсинга. [10]

Метод	Инструменты
Финансовый мониторинг	Мониторинг транзакций – постоянное наблюдение за финансовыми операциями для выявления аномальных или нестандартных действий
	Анализ частоты операций – отслеживание необычных паттернов в частоте и объеме транзакций
	Проверка профиля клиента – сопоставление операций с типичной деятельностью клиента
Верификация клиентов	Идентификация личности - тщательная проверка подлинности документов клиентов
	Проверка источников дохода - анализ финансовых документов и справок о доходах
	Проверка благонадежности - сверка с базами данных и черными списками
Внедрение систем безопасности в продукты Банка	Проверка кредитных заявок - автоматизированный анализ на этапе рассмотрения
	Обнаружение несоответствий - выявление противоречий в документах и заявках
	Кросс-проверка данных - сопоставление информации из разных источников
	Работа с черными списками - автоматическое сравнение с базами данных мошенников
	Защита от внутреннего мошенничества - контроль за действиями сотрудников
Техническое оснащение	Системы анализа данных - использование ПО для обработки больших массивов информации
	Машинное обучение - применение алгоритмов для автоматического выявления аномалий
	Искусственный интеллект - использование ИИ для прогнозирования мошеннических действий
	Двухфакторная аутентификация - усиление защиты аккаунтов клиентов
	Биометрические технологии - внедрение современных методов идентификации
Организационные меры	Обучение персонала - регулярное повышение квалификации сотрудников
	Кибербезопасность - внедрение современных технологий защиты данных
	Сотрудничество с правоохранительными органами - обмен информацией и совместные расследования
	Корпоративная культура - формирование этических норм и ценностей

Все описанные в таблице методы и инструменты интегрируются между собой для создания комплексной защиты банка от мошенничества, что обеспечивает повышение надежности внутренних процессов, снижение рисков и улучшение качества обслуживания клиентов.

ВЫВОДЫ

Стремительное развитие цифровых технологий и распространение доступности интернета увеличило объемы кибермошенничества. Технологические инновации, такие как мобильные приложения и онлайн-платежи, повысила онлайн-активность пользователей, делая их потенциальными жертвами киберпреступников.

Анализ инцидентов показывает, что основной причиной большинства нарушений безопасности является человеческий фактор, а не технические уязвимости. Тем не менее, устаревшие информационные системы и недостаточная защита критически важной инфраструктуры, включая банкоматы и цепочки поставок программного обеспечения, представляют значительные риски для стабильности и безопасности всей банковской экосистемы.

Кибербезопасность кредитных организаций является критически важным аспектом их устойчивости и конкурентоспособности. Экономические риски, связанные с киберугрозами, требуют постоянного внимания и инвестиций в защиту данных. Учитывая растущую сложность кибератак, банки должны активно внедрять современные технологии краудсорсинга. Таким образом комплексный подход к кибербезопасности позволит минимизировать риски и обеспечить долгосрочную стабильность в условиях цифровой экономики.

Список источников:

1. Направления совершенствования методики оценки финансовой устойчивости коммерческого банка в современных условиях конкурентной среды / В. А. Водопьянова, Т. Е. Даниловских, Т. С. Короткоручко [и др.] // Фундаментальные исследования. – 2023. – № 8. – С. 18-23. – DOI 10.17513/fr.43489. – EDN SWHIAM.
2. [19:03, 20.06.2025] Водопьянова: Koren, A. V. Approaches to enhance the investment attractiveness of multinational organizations / A. V. Koren, V. A. Vodopyanova // Revista de Investigaciones Universidad del Quindio. – 2022. – Vol. 34, No. S3. – P. 215-221. – DOI 10.33975/riuq.vol34nS3.961. – EDN MXCFIU.
3. [19:04, 20.06.2025] Водопьянова: Koren, A. V. Análisis de métodos para aumentar el atractivo de inversión de las empresas transnacionales / A. V. Koren, V. A. Vodopyanova // Revista Electrónica de Investigación en Ciencias Económicas. – 2024. – Vol. 9, No. 18. – P. 32-43. – DOI 10.5377/reice.v9i18.18049. – EDN LJWFUA.

4. Проблемы и перспективы развития региональной платежной инфраструктуры при использовании пластиковых карт Кривошаповат С.В., Просалова В.С., Москаленко А.С. Фундаментальные исследования. 2022. № 7. С. 57-63.
5. Финансовые угрозы в финансовой индустрии во втором полугодии 2023 — первом полугодии 2024 [Электронный ресурс] / Positive Technologies. — Режим доступа: https://ptsecurity.com/ru-ru/research/analytics/financial-industry-security-h2-2023-h1-2024/#id1 (дата обращения: 22.06.2025).
6. Обзор ключевых показателей развития информационного банкинга за III квартал 2023 года [Электронный ресурс] / Центральный банк Российской Федерации. – Режим доступа: https://cbr.ru/statistics/ib/review_3q_2023 (дата обращения: 02.06.2025).
7. Дербенев В. А. Правовое регулирование электронной коммерции в России и за рубежом [Электронный ресурс] / В. А. Дербенев // Финансово-банковский журнал. – 2013. – Режим доступа: https://finbiz.spb.ru/wp-content/uploads/2013/01/derben.pdf (дата обращения: 02.06.2025).
8. Международный опыт противодействия мошенничеству в сфере высоких технологий: учебное пособие / Н. В. Доронина, А. В. Егоров, А. В. Мартынов, А. В. Рябинин. – Тольятти: Изд-во СГАУ, 2019. – Режим доступа: https://repo.ssau.ru/bitstream/Sovremennoe-mezhdunarodnoe-pravo/Mezhdunarodnopravovoe-protivodeistvie-moshennichestvu-v-sfere-vysokih-tehnologii-113630/1/978-5-7883-2061-8_2024-318-327.pdf/ (дата обращения: 02.06.2025). – ISBN 978-5-7986-0555-5.
9. Тренды цифровой трансформации бизнеса [Электронный ресурс] // РБК Тренды. – Режим доступа: https://trends.rbc.ru/trends/innovation/60d1b8059a7947c4c6cf7b5d?from=copy (дата обращения: 02.06.2025).
10. Международный опыт противодействия мошенничеству в сфере высоких технологий: учебное пособие / Н. В. Доронина, А. В. Егоров, А. В. Мартынов, А. В. Рябинин. – Тольятти: Изд-во СГАУ, 2019. – Режим доступа: https://repo.ssau.ru/bitstream/Sovremennoe-mezhdunarodnoe-pravo/Mezhdunarodnopravovoe-protivodeistvie-moshennichestvu-v-sfere-vysokih-tehnologii-113630/1/978-5-7883-2061-8_2024-318-327.pdf/ (дата обращения: 02.06.2025). – ISBN 978-5-7986-0555-5.