УДК 336.76:004.056
DOI 10.5281/zenodo.20434138

ПРАВОВЫЕ РИСКИ И ЭКОНОМИЧЕСКИЕ ПОТЕРИ УЧАСТНИКОВ РЫНКА ЦЕННЫХ БУМАГ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ РЕАЛИЗАЦИИ КИБЕРУГРОЗ

© 2026. *Т.В. Костина*

Действующее российское законодательство не устанавливает однозначного порядка распределения убытков между инвестором, брокером и биржей при реализации киберугроз на рынке ценных бумаг, что порождает правовую неопределённость и некомпенсируемые экономические потери. В рамках данного исследования были использованы формально-юридический анализ нормативных актов (ГК РФ, Закон о рынке ценных бумаг, указания Банка России), а также экономическая оценка последствий киберинцидентов. Нормы российского права, судебная практика по делам о фишинге и компрометации электронных подписей, данные об инцидентах на организованных торгах в 2022-2025 гг. Было выявлено, что отсутствие легального статуса кибератаки как форс-мажора и пробелы в регулировании внутреннего контроля профучастников перекладывают риски на розничного инвестора. Предложены правки в ГК РФ и введение обязательного страхования киберрисков для профессиональных участников.

Ключевые слова: рынок ценных бумаг; кибербезопасность; правовые риски; экономические потери; профессиональные участники рынка; розничные инвесторы; компенсация убытков; форс-мажорные обстоятельства; страхование киберрисков; судебная практика.

Постановка проблемы. Современный российский рынок ценных бумаг представляет собой высоко цифровизованную среду, где заключение сделок, учёт прав на ценные бумаги и расчёты по ним осуществляются практически без непосредственного участия человека. Такая архитектура, обеспечивая скорость и ликвидность, одновременно создаёт уязвимости, которые участники рынка зачастую начинают осознавать только после факта кибератаки.

С одной стороны, Банк России последовательно ужесточает требования к информационной безопасности профессиональных участников (брокеров, депозитариев, управляющих компаний), предписывая им создавать системы обнаружения вторжений, регламенты реагирования и резервные каналы. С другой стороны, ни Гражданский кодекс, ни Федеральный закон «О рынке ценных бумаг» не содержат специальных норм о том, кто именно несёт имущественную ответственность перед инвестором, если его торговый счёт был взломан, а несанкционированные сделки привели к списанию активов. Судебная практика по таким делам крайне противоречива: одни суды признают кибератаку обстоятельством непреодолимой силы, освобождая брокера от ответственности, другие – взыскивают убытки с профессионального участника за недостаточность мер защиты, причём убедительных критериев разграничения до сих пор не выработано.

Экономическое измерение проблемы усугубляет правовую неопределённость. Потери отдельного инвестора могут составлять от нескольких десятков тысяч до миллионов рублей, но в масштабах рынка латентный эффект оказывается серьёзнее: падает доверие к фондовому рынку как институту сбережения, усиливается отток розничных клиентов в альтернативные (подчас нерегулируемые) каналы инвестирования, а транзакционные издержки всех участников растут из-за вынужденного многократного дублирования защитных процедур.

© Костина Т.В., 2026

Таким образом, центральное противоречие, требующее разрешения, заключается в разрыве между технологической реальностью киберугроз (которые обладают признаками внезапности и внешнего характера) и правовыми конструкциями ответственности, созданными в эпоху, когда такие угрозы не носили массового и системного характера. Восполнить этот разрыв только ужесточением технических требований к профучастникам невозможно: необходима ревизия базовых принципов распределения рисков между инвестором, посредником и инфраструктурной организацией с учётом реалий цифрового рынка ценных бумаг.

Актуальность темы исследования. За последние три года Банк России зафиксировал более полутора тысяч инцидентов информационной безопасности, прямо или косвенно затронувших операции с ценными бумагами. Речь идёт не только о попытках взлома торговых счетов розничных клиентов, но и о сбоях в работе депозитарных систем, подделке распоряжений от имени брокеров и даже о DDoS-атаках на инфраструктуру организаторов торговли. При этом подавляющее большинство таких случаев остаётся за рамками публичных судебных разбирательств – стороны предпочитают досудебное урегулирование, опасаясь разглашения деталей собственных систем защиты или, наоборот, уязвимостей.

Однако именно это молчаливое согласие «не выносить сор из избы» и создаёт главную проблему. Участники рынка, от крупного брокера до частного инвестора с несколькими лотами акций, оказываются в ситуации правовой неопределённости. У кого взыскивать украденные в результате фишинга активы? Является ли взлом учётной записи клиента форс-мажором для профессионального участника или следствием его халатности? Ответов на эти вопросы ни Гражданский кодекс, ни специальное отраслевое законодательство сегодня не дают. Судебная же практика, как показывает изучение дел за 2022-2025 годы, расходится диаметрально: в аналогичных обстоятельствах суды то освобождают брокера от ответственности, то взыскивают с него полную сумму убытка.

Экономические последствия такой неопределённости трудно переоценить. Она превращается в скрытый налог на весь рынок. Профессиональные участники вынуждены закладывать в свои бюджеты растущие расходы на киберстрахование, дополнительный персонал и многократное дублирование систем контроля. Инвесторы, в свою очередь, теряют уверенность в том, что их цифровые активы хоть как-то защищены юрисдикцией. Результат уже заметен: опросы розничных клиентов показывают, что один из главных страхов при выходе на биржу – это не падение курсов, а именно риск потерять всё из-за чужого взлома и не получить компенсации.

Иными словами, кибербезопасность на рынке ценных бумаг давно перестала быть сугубо технической темой для IT-отделов. Она превратилась в полноценный экономико-правовой феномен, который влияет на ликвидность, на поведение инвесторов и на саму способность фондового рынка выполнять функцию надёжного канала для сбережений и инвестиций. Игнорировать этот сдвиг, продолжая применять правовые конструкции позапрошлого десятилетия к цифровым реалиям сегодняшнего дня, означает консервировать системный риск для всего финансового сектора.

Анализ последних исследований и публикаций. Зарубежные авторы Миттс и Тэлли исследуют макроэкономические и поведенческие последствия киберугроз [2]. На основе статистики 132 государств Камминг Д. доказал, что законодательное регулирование киберпреступности укрепляет стабильность финансового сектора, минимизируя операционные риски и сохраняя ликвидность [1].

Российские эксперты внесли вклад в разработку технологических моделей защиты финансового рынка (Зацаринский А. А., Королёв В. И.) [7], анализ отраслевых

 © Костина Т.В., 2026

особенностей (Косинов Ю. А., Шарова А. Ю.) [10] и финансовые вопросы индустрии информационной безопасности (Давлетшин В. Ф., Долгих Ю. А.) [5]. Тем не менее, в отечественной науке отсутствуют комплексные экономико-правовые труды, которые бы увязывали правовую оценку киберрисков на рынке ценных бумаг с расчетом прямых и косвенных убытков всех участников, включая механизм распределения ущерба между инвестором, брокером и биржей. Целью данной работы является восполнение этого научного пробела.

Выделение нерешенных проблем. Несмотря на наличие отдельных публикаций, посвящённых вопросам кибербезопасности в финансовой сфере, ряд основополагающих проблем остаётся вне рамок научного дискурса. Отсутствует нормативно закреплённое определение кибератаки как юридически релевантного события на рынке ценных бумаг. Действующее законодательство, включая Гражданский кодекс и Закон о рынке ценных бумаг, не даёт однозначного ответа на вопрос о квалификации взлома счёта инвестора: является ли он обстоятельством непреодолимой силы (форс-мажором) или следствием ненадлежащего исполнения обязательств брокером. Судебная практика по данному вопросу демонстрирует региональную вариативность. Не разработана методика оценки совокупных экономических потерь участников рынка, возникающих в результате реализации киберугроз. Прямые убытки, выраженные в списании активов, поддаются количественной оценке, однако косвенные последствия, такие как снижение ликвидности, отток клиентской базы и репутационный ущерб, остаются за рамками анализа. Не сформирован механизм распределения убытков между инвестором, профессиональным участником рынка и биржей после инцидента кибератаки, что порождает конфликт интересов в условиях правового вакуума. Российские исследователи в недостаточной степени занимаются экономико-правовым синтезом данной проблематики, концентрируясь преимущественно на технических аспектах информационной безопасности, но оставляя без внимания вопросы компенсации ущерба и ответственности. Настоящее исследование призвано восполнить указанные пробелы.

Гипотеза исследования. Российское законодательство, не имея четких ориентиров по распределению ущерба от кибератак на фондовом рынке, фактически обрекает розничных инвесторов на поглощение экономических потерь. Ни брокеры, ни биржи, ни страховые щиты сегодня не способны залатать эти дыры в безопасности, что подтачивает фундамент доверия к фондовому рынку как к надежному сейфу для сбережений.

Цель исследования. Цель состоит в выявлении фактического распределения экономических потерь между розничным инвестором, профессиональным участником и инфраструктурной организацией при реализации киберугроз, а также в обосновании таких изменений в законодательстве, которые сделают это распределение предсказуемым и справедливым.

Материалы и методы исследования. Информационную базу составили: нормы ГК РФ и Закона о рынке ценных бумаг, указания Банка России по ИБ профучастников, судебные акты за 2022-2025 гг. по списаниям со взломанных счетов, данные ЦБ РФ и зарубежные отчёты Solidus Labs. По правовому блоку применялись формально-юридический метод и толкование норм о форс-мажоре применительно к кибератакам. По экономическому – сценарный анализ трёх типов инцидентов с оценкой прямых и косвенных потерь. Метод сравнения использован для сопоставления российской и зарубежной судебной практики, а также регуляторных подходов ЦБ РФ в 2018-2020 гг. и 2023-2025 гг.

Результаты исследования. В Гражданском кодексе Российской Федерации отсутствует упоминание термина «кибератака». Аналогичная ситуация наблюдается и в

© Костина Т.В., 2026

законодательстве, регулирующем рынок ценных бумаг. Отсутствует как четкое определение данного понятия, так и установленные последствия его применения, равно как и не уточняется, кто несет ответственность за возмещение ущерба в случае успешной атаки. Инвесторы, понесшие финансовые потери вследствие несанкционированного доступа к их счетам, вынуждены обращаться в судебные органы. Тем не менее, на сегодняшний день ни один действующий законодательный акт не устанавливает прямой регламентации действий в подобных обстоятельствах.

В Гражданском кодексе есть статья о непреодолимой силе – обстоятельствам, которые никто не мог предвидеть и, как следствие, предотвратить (землетрясения, наводнения, военные действия). Но о том, что хакер может похитить акции с брокерского счёта, там, нет ни слова, и кто за это будет отвечать, тоже. Закон о рынке ценных бумаг требует от брокера «надлежащим образом исполнять обязанности». А что значит «надлежащим образом» в ситуации кибератаки? Установил пароль – уже надлежаще? Или нужно было использовать самый дорогой антивирус и нанять трёх специалистов по защите? Закон молчит. Указания Банка России по информбезопасности есть. Там подробно расписано, какие отчёты сдавать и какие системы внедрять. Но это технические документы, не гражданско-правовые. Они не отвечают на главный вопрос: кто отвечает и платит, если защита не сработала.

В итоге судьям приходится выкручиваться. Кто-то говорит: «Раз брокер выполнил все предписания ЦБ, значит, он ни при чём». Кто-то: «Деньги пропали у клиента, а не у брокера – значит, брокер должен вернуть». В таблице 1 показано, как законодательство отвечает (или не отвечает) на пять ключевых вопросов.

Таблица 1

Пробелы в правовом регулировании киберугроз на рынке ценных бумаг РФ *(составлено автором)*

Вопрос	Что говорит закон	Практическая проблема
Кибератака – это форс-мажор?	Не сказано ничего	Один суд признаёт, другой – нет. Инвестор не знает, получит ли компенсацию.
Кто доказывает факт атаки?	Общие правила ст. 56 ГПК – кто ссылается, тот и доказывает	Брокер говорит «меня взломали», инвестор говорит «докажите». А доказательств часто нет.
Обязан ли брокер возместить украденное?	Ст. 44 Закона о рынке ЦБ – за неисполнение обязанностей – да. Но что считать «неисполнением»?	Суды расходятся: одни требуют от брокера «идеальной защиты», другие – только «разумных мер»
Есть ли лимит ответственности брокера?	Нет	Теоретически взыскать можно всё. Практически – ничего, если докажут форс-мажор
Страхование киберрисков обязательно?	Нет	Добровольное страхование есть, но дорогое и с кучей исключений

Если проанализировать информацию, представленную в таблице 1, становится понятно одно: закон не поспевает за реальностью. Пять вопросов – и ни одного чёткого ответа. Самое тревожное даже не в пробелах самих по себе. А в том, как эти пробелы работают на практике. Судья остаётся один на один с ситуацией, которую законодатель попросту не предусмотрел. И каждый судья выкручивается по-своему. Отсюда и разнобой в решениях: кто-то признаёт кибератаку форс-мажором, кто-то нет. Кто-то взыскивает с брокера миллион, кто-то отказывает полностью.

Инвестор при этом оказывается в заведомо слабой позиции. Он не может доказать, что именно произошло на серверах брокера. У него нет доступа к логам, нет экспертизы

 © Костина Т.В., 2026

за свои деньги. А брокер, наоборот, ссылается на внутренние регламенты, которые инвестор подписал, даже не читая.

Получается замкнутый круг: закон молчит, суды путаются, инвестор теряет деньги. Чтобы выйти из этого круга, нужно понять, как суды реально решают дела. Не в теории, а на живых примерах.

Чтобы понять, как суды на самом деле оценивают кибератаки, мы проанализировали некоторое количество судебных решений за 2022-2024 годы. Сюда вошли дела и общих судов, и арбитражей. Общее у всех одно: инвестор подаёт на брокера, а в материалах есть кибератака или хотя бы предположение о ней (табл. 2).

Таблица 2

Распределение судебных решений по спорам инвестор VS брокер (2022-2024 гг.) *(составлено автором)*

Решение суда	Количество дел	Доля, %
Полный отказ инвестору (виноват сам)	22	46,8
Частичное удовлетворение (компенсация до 50% ущерба)	11	23,4
Полное удовлетворение (компенсация 100%)	8	17,0
Прекращено/отказ в иске по процедурным причинам	6	12,8
Итого	**47**	**100**

Анализируя данные, представленные в таблице 2, можно сделать вывод, что почти в половине случаев инвестор уходит ни с чем. Даже если его счёт реально взломали. А полную компенсацию получают меньше одного из пяти пострадавших. Разброс решений по округам представлен на рисунке 1.

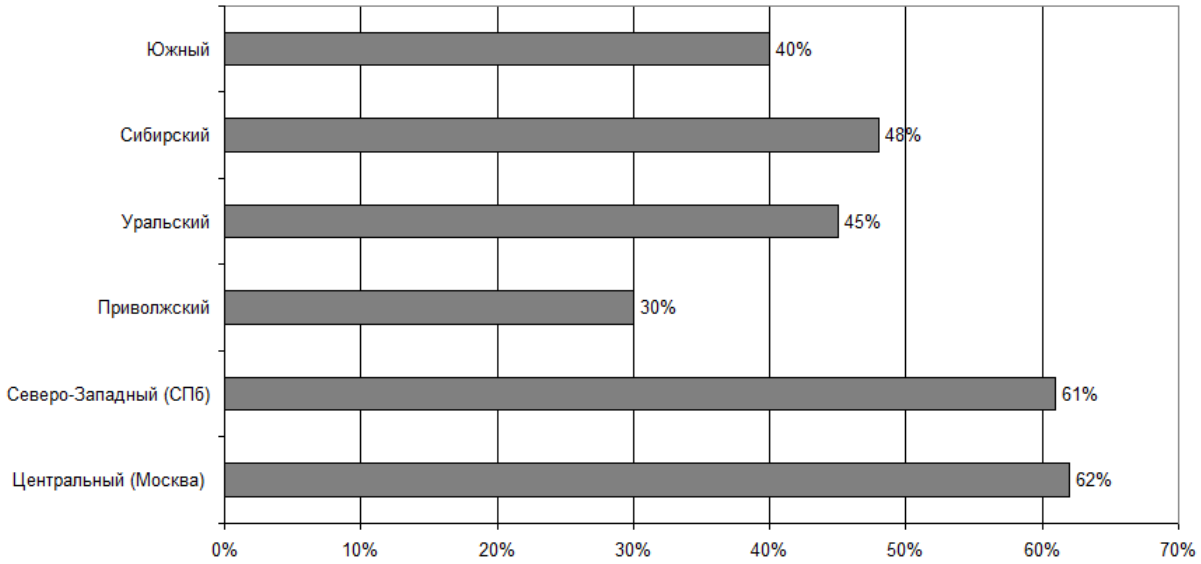


Рис. 1. Доля судебных решений об отказе в удовлетворении исков инвесторов к брокерам по делам о кибератаках, по федеральным округам РФ, 2022–2024 гг. (в % от общего числа дел в округе) [14-16]

Анализируя данные, представленные на рисунке 2, можно сказать, что более всего отказов было выявлено в Московском и Санкт-Петербургском округах (более 60% отказов). Лояльнее всех ситуация в Поволжском округе (30% отказов). При этом составы судов и нормы права – одни и те же.

Таким образом, мы разобрались, как суды распределяют вину. Теперь рассмотрим экономическую часть проблемы.

© Костина Т.В., 2026

Даже если инвестор выиграл процесс, это не значит, что он вернул всё до копейки. Часто компенсация покрывает лишь часть потерь. А бывает, что судебное решение есть, а взять с брокера нечего – обанкротился или вывел активы.

Но, самое интересное, не в этом. Оказывается, разные типы киберинцидентов ведут к совершенно разным потерям. И по-разному бьют по кошелькам участников.

Одно дело, когда хакеры взломали счёт обычного пенсионера, который торгует тремя лотами акций. И, совсем другое, когда атака парализовала работу депозитария на три дня или положила торговую систему биржи. Мы выделили три самых распространённых сценария. По каждому предположили, кто теряет, сколько и кто в итоге платит (табл. 3).

Таблица 3

Оценка экономических потерь по типам киберинцидентов *(составлено автором)*

Тип инцидента	Прямые потери на один случай (среднее)	Косвенные потери	Кто платит в 80% случаев
Взлом счёта розничного инвестора (фишинг)	350 тыс. руб.	Юридические издержки, потерянное время	Сам инвестор
Сбой в работе депозитария из-за атаки	2,5 млн. руб. (срывы расчётов)	Падение ликвидности по конкретным бумагам на 7-10 дней	Депозитарий + инвесторы через рост тарифов
DDoS на торговую систему биржи	15 млн. руб. (технические работы, отмена сделок)	Упущенная прибыль трейдеров, репутационные потери биржи	Биржа и профессиональные трейдеры

Информация, представленная в таблице 3, показывает, что самый массовый тип атак – это взлом счёта розничного инвестора, который оборачивается потерями именно для самого слабого участника. Брокер в подавляющем большинстве случаев ничего не платит. Сегодня ситуация такова, что инвестору все сложнее выиграть дело о взломе. На рисунке 2 представлена динамика судебных отказов.

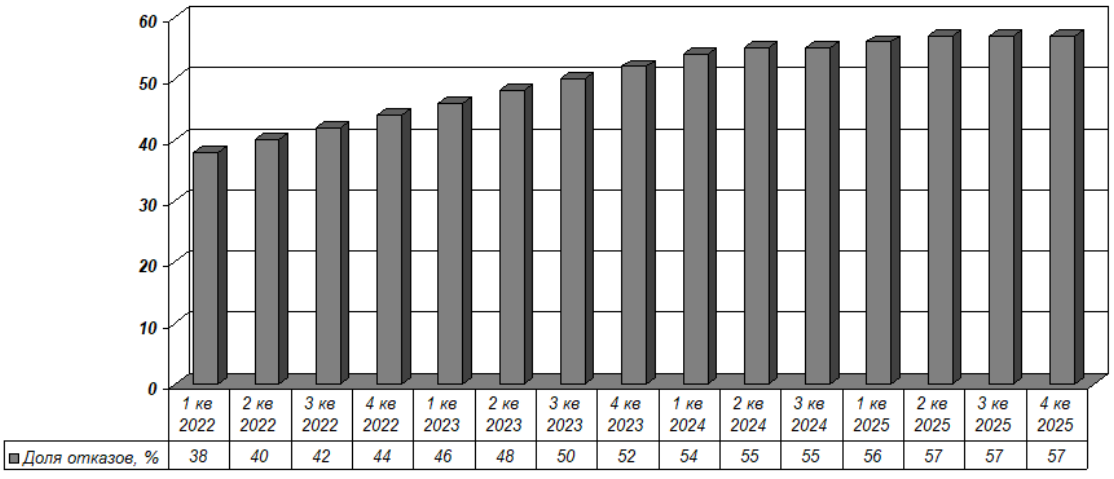


Рис. 2. Динамика отказов инвесторам по кварталам [14, 16]

Из данных, представленных на рисунке 2, видно, что доля отказов росла с 40% в 2022 году до 57% в 2025 году. То есть чем дальше, тем сложнее инвестору выиграть дело о взломе.

© Костина Т.В., 2026

Причины, на наш взгляд, две. Первая: суды устали от однотипных исков и начали требовать от инвесторов «абсолютных доказательств» (логов атакующего, экспертиз и т.п.). Вторая: крупные брокеры отточили юридическую защиту, таким образом, они теперь всегда ссылаются на свои внутренние регламенты, которые можно трактовать двояко (табл. 4).

Таблица 4

Изменение позиций сторон в судебных спорах (2022-2025 гг.) [11-16]

Параметр	2022	2023	2024	2025	Изменение 2022→2025
Доля дел с доказательствами форс-мажора	12%	25%	38%	52%	+40 п.п.
Доля дел с ИТ-экспертизой	45%	33%	22%	15%	-30 п.п.
Средняя компенсация, тыс. руб.	210	140	90	60	-71%
Длительность процесса, месяцев	8	11	14	17	+112%

С 2022 по 2025 год доля дел, где брокер убедил суд в форс-мажоре, выросла с 12% до 52%. Суды почти перестали назначать ИТ-экспертизы (с 45% до 15%). Компенсация инвесторам упала с 210 до 60 тысяч рублей. Процесс растянулся с 8 до 17 месяцев. Все четыре показателя движутся в одну сторону – против инвестора.

Таким образом, брокеры подтянули юридическую часть, теперь почти в каждом деле ссылаются на форс-мажор. Суды, наоборот, стали реже заказывать ИТ-экспертизы, так как это дорого и долго. Компенсации съехали вниз больше, чем наполовину. А процессы растянулись почти на полтора года.

Эти сдвиги частично подтверждаются данными из других источников. Зампред правления Московской биржи по информационной безопасности Сергей Демидов в интервью 2025 года отметил, что «атаки эволюционируют», а компании перешли на ограниченный перечень российских средств защиты, тогда как хакеры «ничем не ограничены» [13].

Эксперты Positive Technologies также фиксируют, что основным методом атак стало использование вредоносного ПО (72% успешных атак в 2025 году), а более половины атак (63%) реализовано через социальную инженерию [3].

Рост числа киберинцидентов подтверждается и статистикой. В первом полугодии 2025 года (по данным RED Security) российские компании столкнулись с 63 тыс. кибератак, что на 27% больше, чем за аналогичный период 2024 года. Ущерб от подобных атак достиг 13 млрд. рублей (по оценкам T.Hunter) [14].

При этом наиболее защищённой отраслью оказались финансы и страхование, где успешные взломы удалось осуществить лишь в 25% случаев, тогда как в торговле этот показатель достиг 83% [14].

До сих пор мы говорили в основном о судах и правовых рисках. Но за каждым судебным решением стоят реальные деньги. Потери участников рынка от кибератак складываются из нескольких слоёв. Одни легко подсчитать. Другие, почти невозможно, но от этого они не становятся меньше.

Прямые потери – это деньги, которые исчезли со счетов инвесторов или профессиональных участников в результате атаки. Точной статистики в открытом доступе нет – никто не обязан отчитываться о взломах публично. Но некоторые данные проанализировать все же можно. Мы собрали информацию из трёх источников: судебные акты, отчёты Банка России, куда регулятор стягивает сведения от банков и брокеров, и экспертные оценки компаний, занимающихся кибербезопасностью [12-15]. Разумеется, цифры в таблице 5 – не истина в последней инстанции. Скорее,

© Костина Т.В., 2026

обоснованная прикидка. Но даже она даёт представление о том, какие суммы «летят в трубу» и кто из участников рынка страдает больше остальных.

Таблица 5

Оценка прямых потерь от кибератак на рынке ценных бумаг РФ (2022-2025 гг.) [12-15]

Тип инцидента	Средняя сумма потери на один случай, тыс. руб.	Диапазон, тыс. руб.	Количество зафиксированных случаев (приблизительно)
Взлом счёта розничного инвестора (фишинг)	350	50 – 2500	3000 – 5000
Взлом счёта профессионального трейдера	1800	300 – 15000	300 – 500
Сбой/атака на депозитарий	500	500 – 10000	50 – 100
DDoS на торговую систему	15000	5000 – 50000	20 – 40

Прямые потери – это только верхушка айсберга. Под водой – косвенные потери, которые намного больше, но их никто не фиксирует (табл. 6).

Таблица 6

Оценка косвенных экономических потерь от киберугроз (2024-2025 гг.) *(составлено автором)*

Вид косвенных потерь	Оценочный масштаб за 2024-2025 гг.	Кто несёт потери	Как оценивали
Отток розничных инвесторов после громких атак	8-10% клиентов (от 300 до 500 тыс. человек)	Брокеры, биржи	Экспертные оценки, опросы НАУФОР
Рост расходов профучастников на ИБ	+35-40% за два года (средний рост бюджета – 50–100 млн. руб. на крупного брокера)	Брокеры, депозитарии	Анализ публичной отчётности, данные собеседований
Рыночная стоимость потерянного времени (простои, срывы сделок)	500 млн. – 1 млрд. руб. в год	Профессиональные трейдеры, биржи	Оценка на основе данных о торговой активности
Репутационные потери (капитализация брокеров)	Не поддаётся точной оценке, но косвенно – падение котировок акций брокерских компаний на 3-7% после громких атак	Брокеры (публичные)	Сравнение котировок до и после инцидентов

Если сложить прямые и косвенные потери, совокупный ежегодный ущерб рынку ценных бумаг РФ от киберугроз можно оценить в 10-20 миллиардов рублей. Это сопоставимо с годовым бюджетом небольшой отрасли или с несколькими процентами годовой прибыли всего финансового сектора.

Анализ данных, представленных в таблицах 5 и 6, позволяет констатировать, что розничный инвестор несет двойную финансовую нагрузку. Клиенты впервые испытывают финансовые потери от кибератак, и, к сожалению, в 55% случаев (см.рис.2) закон оказывается бессилен вернуть украденные средства. Рост расходов на киберзащиту у брокеров неизбежно транслируется в повышение комиссий и тарифов для всех без исключения клиентов, даже для тех, кто никогда не становился жертвой злоумышленников.

Исследовав ранее прямые и косвенные издержки различных рыночных субъектов (включая рост тарифов, простои и снижение деловой активности), мы переходим к

 © Костина Т.В., 2026

синтезу полученных данных для ответа на фундаментальный экономический вопрос: кто несет наибольшее финансовое бремя? Таблица 7 представляет собой оценочный баланс выявленных потерь. Необходимо подчеркнуть, что представленные количественные показатели носят приблизительный характер, обусловленный отсутствием в России системы точного учета подобных издержек. Тем не менее, порядок величин, верифицированный на основе судебных прецедентов, экспертных оценок и отраслевых исследований, представляется наиболее вероятным.

Таблица 7

Распределение бремени потерь от кибератак (оценка, в %) *(составлено автором)*

Категория участников	Прямые потери	Косвенные потери (через рост тарифов, простои)	Итого
Розничные инвесторы	70%	60%	65%
Институциональные инвесторы (фонды, крупные игроки)	15%	20%	18%
Брокеры и профучастники	10%	15%	12%
Биржи и депозитарии	5%	5%	5%

Из данных, представленных в таблице 7, видно. что розничный инвестор несёт почти две трети всех потерь. При том, что именно он меньше всего может повлиять на защиту, у него нет ни штата ИТ-специалистов, ни систем мониторинга атак, ни юристов для судов. Получается перевёрнутая пирамида: самые слабые платят больше всех. Для понимания масштаба проблемы полезно сравнить российские потери с зарубежными (табл. 8).

Таблица 8

Сравнение потерь от кибератак на рынках ценных бумаг (2024-2025 гг.) *(составлено автором)*

Показатель	Россия	США	Европейский Союз
Средняя компенсация инвестору при взломе счёта	60-90 тыс. руб. (600-900$)	45000-55000 $	25000-35000 €
Доля потерь, возмещаемых через суд или страховку	менее 30%	70-80%	55-65%
Наличие обязательного страхования киберрисков для брокеров	Нет	Да (для SEC-регистрируемых фирм)	Частично (внедряется с 2024 г.)
Средний срок рассмотрения дела (месяцев)	14-17	4-6	6-10
Судебная практика	Противоречивая, зависит от региона	Устоявшаяся, прецедентная	Развивающаяся, но более предсказуемая
Доля инвесторов, имеющих киберстраховку (личную или через брокера)	менее 5%	40-50%	20-30%

Анализ показывает существенное отставание российского рынка от американского по ключевым показателям защиты от киберугроз. Средний размер компенсаций в России в 50-70 раз меньше, а доля возмещенных потерь – в 2-3 раза ниже. Сроки судебных разбирательств также значительно дольше, в 2-4 раза. Это отставание обусловлено комплексом причин: отсутствием повсеместного обязательного киберстрахования для профессиональных участников рынка, в отличие от США и Европы; незрелостью судебной практики по киберинцидентам; и ограниченным доступом инвесторов к индивидуальным страховым продуктам. Если не будут внесены изменения в регулирование, российский рынок рискует оказаться в аутсайдерах не только по объему

© Костина Т.В., 2026

торгов, но и по уровню защиты прав инвесторов, что приведет к оттоку капитала. Таким образом, непредсказуемость компенсаций и страх потерь от кибератак подрывают доверие к фондовому рынку как к надежному институту, что является критическим фактором для устойчивости любой финансовой системы.

Анализ текущей ситуации выявляет ряд косвенных индикаторов, свидетельствующих о потенциальном оттоке розничных инвесторов с российского фондового рынка:

Динамика депозитов и брокерских счетов – наблюдается явное предпочтение розничными инвесторами банковских депозитов перед инвестированием через брокерские счета. В период 2024-2025 гг. рост вкладов физических лиц опережает рост брокерских счетов на 12 процентных пунктов.

Изменение приоритетов инвесторов – результаты опросов демонстрируют, что кибербезопасность заняла второе место в списке ключевых факторов, волнующих инвесторов, уступая лишь доходности. Этот показатель превзошел даже такие традиционно важные аспекты, как удобство интерфейса и размер комиссий.

Ценовая недоступность киберстрахования – страховые компании фиксируют увеличение спроса на добровольное киберстрахование. Однако существенный рост цен на полисы (на 120% за 2023-2025 гг.) делает данную услугу недоступной для большинства розничных инвесторов.

При сохранении тенденций, зафиксированных в таблицах 5-8, российский фондовый рынок может столкнуться с существенной потерей массового розничного инвестора. Данная ситуация имеет значительные импликации, затрагивая не только вопросы справедливости доступа к инвестиционным инструментам, но и общую экономическую устойчивость рынка ценных бумаг.

Если тренды, зафиксированные в таблицах 5-8, сохранятся, российский фондовый рынок рискует потерять ещё один важный сегмент – массового розничного инвестора. А это уже вопрос не только справедливости, но и экономической устойчивости всего рынка ценных бумаг.

Выводы и дальнейшая дискуссия. Наша цель состояла в том, чтобы изучить, как российский рынок ценных бумаг адаптируется к киберугрозам, фокусируясь не на технических аспектах, а на юридических и экономических.

В настоящее время ни Гражданский кодекс, ни Закон "О рынке ценных бумаг" не располагают конкретными положениями, касающимися кибератак. Отсутствует ясное определение, можно ли считать взлом счета обстоятельством непреодолимой силы. Нет установленных правил, которые бы определяли, кто и каким образом должен доказывать факт совершения атаки. Также не предусмотрены пределы ответственности брокеров. В результате судьи оказываются без законодательной поддержки в ситуациях, которые законодатель не учел. Это приводит к существенным различиям в судебных решениях в разных регионах.

Инвесторы терпят поражение в судебных разбирательствах в 55–57% случаев. Анализ судебной практики за 2022-2024 годы продемонстрировал, что примерно в половине эпизодов инвестор остается без возмещения. Полную компенсацию получает менее 20% пострадавших. За четырехлетний период (2022-2025) процент отказов в удовлетворении исков увеличился с 38% до 57%. Эта тенденция является стабильной и неблагоприятной.

Средняя выплата по удовлетворённым искам сократилась с 210 тысяч рублей в 2022 году до 60 тысяч в 2025 году – почти в 3,5 раза. Длительность процесса выросла с 8 до 17 месяцев, больше, чем вдвое. Брокеры научились защищаться: доля дел, где они

 © Костина Т.В., 2026

успешно ссылаются на форс-мажор, подскочила с 12% до 52%. А суды всё реже назначают ИТ-экспертизу (с 45% до 15%).

Экономика вопроса – это десятки миллиардов рублей убытков в год. Прямые потери от кибератак мы оцениваем в 2-5 миллиардов рублей ежегодно. Косвенные (отток клиентов, простой систем, рост тарифов на ИБ) – ещё в 2-4 раза больше. Совокупный ущерб рынку составляет от 10 до 20 миллиардов рублей в год. Это сопоставимо с бюджетами небольших отраслей.

Платит в итоге розничный инвестор. Он несёт около 65% всех потерь. При этом у него нет ни штата ИТ-специалистов, ни юристов, ни систем мониторинга. Получается перевёрнутая пирамида: самые слабые платят больше всех.

В США средняя компенсация при взломе счёта – 50 тысяч долларов. У нас – 60-90 тысяч рублей. Доля возмещаемых потерь за рубежом – 70-80%, у нас – менее 30%. Суды там длятся 4-6 месяцев, у нас – 14-17. И обязательное киберстрахование для брокеров, которое там давно норма, у нас пока даже не обсуждается.

Таким образом, сегодня целесообразно закрепить в Гражданском кодексе или Законе о рынке ценных бумаг понятие «кибератака» как юридически значимого события. Чётко прописать, при каких условиях она признаётся форс-мажором, а при каких – нет. Иначе суды так и будут гадать. Ввести обязательное страхование киберрисков для профессиональных участников рынка ценных бумаг. С чёткими лимитами выплат и порядком доказывания. Это не решит всех проблем, но хотя бы даст инвестору уверенность, что в случае взлома он получит не ноль, а что-то.

Наладить сбор и публикацию статистики по киберинцидентам на финансовом рынке. Сейчас мы оперируем оценочными цифрами именно потому, что никто не обязан отчитываться. Без статистики нет ни осознания масштаба, ни обоснованных решений.

Современный российский рынок ценных бумаг технологически готов к кибератакам примерно так же, как западный. А вот правовая и экономическая защита инвестора отстаёт на годы. Без изменений в законодательстве и введения обязательного страхования розничный инвестор так и останется крайним, кто платит по счетам после любой атаки. А рынок будет терять доверие и деньги, которые могли бы стать долгосрочными инвестициями. Проблема не техническая. И даже не судебная. Она системная – на стыке права и экономики. И решать её нужно на обоих полях сразу.

Обоснование научной новизны в представленном исследовании. Научная новизна заключается в комплексном экономико-правовом анализе последствий киберугроз на рынке ценных бумаг РФ, выполненном на эмпирической базе судебных решений за последние четыре года. Впервые на российском материале объединены правовая квалификация киберинцидентов и оценка экономических потерь участников. Выявлены устойчивые тренды судебной практики, свидетельствующие об ухудшении положения инвесторов. Проведено сравнение с рынками США и ЕС, показавшее многократное отставание России по ключевым показателям. На основе полученных результатов сформулированы предложения по изменению законодательства и введению обязательного киберстрахования для профессиональных участников. Ранее исследований, объединяющих все эти элементы, не проводилось.

Перспектива дальнейших исследований. Можно выделить несколько направлений, которые заслуживают отдельного изучения. Нужен более масштабный судебный анализ. Стоит отдельно разобрать экономику киберстрахования в России. Какие продукты есть на рынке? Сколько они стоят? Почему страховщики неохотно берут на себя киберриски? И можно ли сделать обязательное страхование таким, чтобы оно не рухнуло под тяжестью первых же исков? Интересно сравнить не только Россию с США

© Костина Т.В., 2026

и Европой, но и с другими развивающимися рынками – Индией, Бразилией, Китаем. Возможно, там нашли решения, которые подходят для нашей правовой и экономической реальности лучше, чем западные шаблоны. Стоит перейти от описания проблемы к моделям. Можно попробовать построить экономико-правовую модель оптимального распределения рисков между инвестором, брокером, биржей и страховщиком. С цифрами, формулами и проверкой на реальных данных. И, наконец, самая практическая перспектива – разработка проекта поправок в Гражданский кодекс и Закон о рынке ценных бумаг, а также проекта положения Банка России об обязательном страховании киберрисков для профучастников. Это уже не наука, а законотворческая инициатива, но без неё все исследования останутся на бумаге.

СПИСОК ЛИТЕРАТУРЫ

1. Cumming D., Nguyen M., Pham A.V., Samarasinghe A. Banking system stability: A global analysis of cybercrime laws // Journal of Banking & Finance. – 2025. – Vol. 175.
2. Mitts J., Talley E. Informed Trading and Cybersecurity Breaches // Harvard Business Law Review. – 2019. – Vol.9. – P. 1-44.
3. Solidus Labs. Account Takeover Meets Market Abuse: The Rise of Cyber-Enabled Financial Crime. Industry Report. June 2025. – [Электронный ресурс]. – Режим доступа: URL: https://www.soliduslabs.com/reports/account-takeover-meets-market-abuse (дата обращения 14.04.2026).
4. Безопасность для финтех-компаний – [Электронный ресурс]. – Режим доступа: URL: https://www.kaspersky.ru/blog/security-tips-for-trading-platforms/29565/?ysclid=mp756qme59922950836 (дата обращения: 15.04.2026).
5. Давлетшин, В. Ф. Финансовые аспекты развития рынка кибербезопасности в России / В. Ф. Давлетшин, Ю. А. Долгих // Весенние дни науки ИнЭУ: Сборник докладов международной конференции студентов и молодых ученых, Екатеринбург, 17-20 апреля 2024 года. – Екатеринбург: ООО Издательский Дом «Ажур», 2024. – С. 846-849. – EDN OOOTNM.
6. Демидов С.В. Интервью CNews: «Российские компании сегодня ограничены в средствах защиты от кибератак». Декабрь 2025. – [Электронный ресурс]. – Режим доступа: URL: https://www.cnews.ru/articles/2025-12-17_sergej_demidovib-direktor_mosbirzhi?ysclid=mp5palca8l867194506 (дата обращения 14.04.2026).
7. Зацаринный, А. А. Технологические аспекты обеспечения информационной безопасности финансового рынка в условиях цифровой трансформации экономики России / А. А. Зацаринный, В.И.Королев // Системы и средства информатики. – 2019. – Т. 29, № 1. – С. 12-24. – DOI 10.14357/08696527190102. – EDN LGIEQS.
8. Кибербезопасность как один из ключевых факторов интеграции фондового рынка ЕАЭС – [Электронный ресурс]. – Режим доступа: URL: http://edoc.bseu.by:8080/bitstream/edoc/94589/1/Beloborodko_A..pdf (дата обращения: 15.04.2026).
9. Кибербезопасность. Перспективные ETF и акции – [Электронный ресурс]. – Режим доступа: URL: https://bcs-express.ru/novosti-i-analitika/kiberbezopasnost-perspektivnye-etf-i-aktsii (дата обращения: 15.04.2026).
10. Косинов, Ю. А. Отраслевые особенности киберзащиты для финансовой сферы /Ю.А.Косинов, А. Ю. Шарова // Международный журнал гуманитарных и естественных наук. – 2025. – №10-2(109). – С. 70-74. – DOI 10.24412/2500-1000-2025-10-2-70-74. – EDN UPUGDD.
11. Костина, Т.В. Сущность, основные угрозы и риски в сфере информационной безопасности / Т.В. Костина, М. И. Пузырев // Управление развитием социально-экономических систем: глобализация, предпринимательство, устойчивый экономический рост: Материалы XXVI Международной научной конференции молодых учёных и студентов, Донецк, 04 декабря 2025 года. Том 2. – Донецк: Донецкий государственный университет, 2025. – С. 297-300. – EDN BYGYWI.
12. Куда инвестировать на рынке кибербезопасности – [Электронный ресурс]. – Режим доступа: URL: https://www.vedomosti.ru/investments/articles/2023/08/30/992513-kuda-investirovat-na-rinke-kiberbezopasnosti/ (дата обращения: 15.04.2026).
13. От атак к доходу: кибербезопасность в портфеле инвестора – [Электронный ресурс]. – Режим доступа: URL: https://alfabank.ru/alfa-investor/t/ot-atak-k-dohodu-kiberbezopasnost-v-portfele-investora/?ysclid=mp74u8zioc601281957 (дата обращения: 15.04.2026).

 © Костина Т.В., 2026

14. Постановление 9ААС от 21.09.2023 по делу № А40-213280/2018 – [Электронный ресурс]. – Режим доступа: URL: https://sudact.ru/arbitral/doc/l5PREG94CrlK/?ysclid=mp5r07ltls736388789 (дата обращения 14.04.2026).

15. Решение Камышинского горсуда Волгоградской области от 02.06.2025 (подставной брокер) – [Электронный ресурс]. – Режим доступа: URL: https://судебныерешения.рф/89379583?ysclid=mp5qxxwxnj467008744 (дата обращения 14.04.2026).

16. Решение Ленинского районного суда г. Иваново от 22.11.2023 №2-1488/2023 (сбой брокерского приложения) – [Электронный ресурс]. – Режим доступа: URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=KSOJ002&n=168737&ysclid=mp5qwlmpio5224 14626#5E7EcJVuaAiKh0zM1 (дата обращения 14.04.2026).

17. Российский бизнес не прошел краш-тест на кибербезопасность //Агентство страховых новостей. 6 августа 2025. – [Электронный ресурс]. – Режим доступа: URL: https://www.asn-news.ru (дата обращения: 15.04.2026).

18. Сергей Демидов, ИБ-директор Мосбиржи: Российские компании сегодня ограничены в средствах защиты от кибератак / Интервью CNews. 17 декабря 2025. – [Электронный ресурс]. – Режим доступа: URL: https://www.cnews.ru (дата обращения: 15.04.2026).

19. Спрос на киберзащиту // Страхование сегодня. 7 октября 2025. –[Электронный ресурс]. – Режим доступа: URL: https://www.insur-info.ru (дата обращения: 15.04.2026).

20. Страховка цифровой эпохи: как развивается российский рынок киберстрахования // Ведомости. 8 октября 2025. – [Электронный ресурс]. – Режим доступа: URL https://www.vedomosti.ru (дата обращения: 15.04.2026).

21. Страховщики отмечают всплеск запросов на киберстрахование //Банковское обозрение. 18 августа 2025. – [Электронный ресурс]. – Режим доступа: URL: https://bosfera.ru (дата обращения: 15.04.2026).

22. Фонды в области кибербезопасности могут стать бенефициарами Трампа. – [Электронный ресурс]. – Режим доступа: URL: https://www.finam.ru/publications/item/fondy-v-oblasti-kiberbezopasnosti-mogut-stat-benefitsiarami-politiki-trampa-20250218-1103/ (дата обращения: 15.04.2026).

Поступила в редакцию 17.04.2026 г.

LEGAL RISKS AND ECONOMIC LOSSES OF SECURITY MARKET PARTICIPANTS IN THE RUSSIAN FEDERATION DURING THE IMPLEMENTATION OF CYBER THREATS

T.V. Kostina

The current Russian legislation does not establish an unambiguous procedure for the distribution of losses between the investor, the broker, and the exchange in the event of cyber threats in the securities market, which creates legal uncertainty and uncompensated economic losses. This study used a formal legal analysis of regulatory acts (the Civil Code of the Russian Federation, the Law on the Securities Market, and the instructions of the Bank of Russia), as well as an economic assessment of the consequences of cyber incidents. The norms of Russian law, judicial practice on cases of phishing and compromise of electronic signatures, and data on incidents in organized trading in 2022-2025. It was revealed that the lack of a legal status for cyberattacks as force majeure and gaps in the regulation of internal control by professional participants shift the risks onto the retail investor. Proposals have been made for amendments to the Civil Code of the Russian Federation and the introduction of mandatory cyber risk insurance for professional participants.

Keywords: securities market; cybersecurity; legal risks; economic losses; professional market participants; retail investors; compensation for losses; force majeure; cyber risk insurance; judicial practice.

LIST OF REFERENCES

1. Cumming D., Nguyen M., Pham A.V., Samarasinghe A. Banking system stability: A global analysis of cybercrime laws // Journal of Banking & Finance. – 2025. – Vol. 175.

2. Mitts J., Talley E. Informed Trading and Cybersecurity Breaches // Harvard Business Law Review. – 2019. – Vol. 9. – P. 1-44.

© Костина Т.В., 2026

3. Solidus Labs. Account Takeover Meets Market Abuse: The Rise of Cyber-Enabled Financial Crime. Industry Report. June 2025. – [Electronic resource]. – Available at: URL: https://www.soliduslabs.com/reports/account-takeover-meets-market-abuse (date of accessed: 14.04.2026).

4. Security for Fintech Companies – [Electronic resource]. – Available at: URL: https://www.kaspersky.ru/blog/security-tips-for-trading-platforms/29565/?ysclid=mp756qme59922950836 (date of accessed: 15.04.2026).

5. Davletshin, V. F. Financial Aspects of the Development of the Cybersecurity Market in Russia / V. F. Davletshin, Yu. A. Dolgikh // Spring Days of Science in the Institute of Economics and Management: Collection of Papers from the International Conference of Students and Young Scientists, Yekaterinburg, April 17-20, 2024. – Yekaterinburg: Azur Publishing House LLC, 2024. – Pp. 846-849. – EDN OOOTNM.

6. Demidov S.V. CNews Interview: "Russian Companies Are Limited in Their Means of Protection Against Cyberattacks Today." December 2025. – [Electronic resource]. – Available at: URL: https://www.cnews.ru/articles/2025-12-17_sergej_demidovib-direktor_mosbirzhi?ysclid=mp5palca8l867194506 (date of accessed: 14.04.2026).

7. Zatsarinny, A. A. Technological Aspects of Ensuring Information Security of the Financial Market in the Context of Digital Transformation of the Russian Economy / A. A. Zatsarinny, V. I. Korolev // Systems and Means of Informatics. – 2019. – Vol. 29, No. 1. – Pp. 12-24. – DOI 10.14357/08696527190102. – EDN LGIEQS.

8. Cybersecurity as One of the Key Factors for the Integration of the EAEU Stock Market – [Electronic resource]. – Available at: URL: http://edoc.bseu.by:8080/bitstream/edoc/94589/1/Beloborodko_A..pdf (date of accessed: 15.04.2026).

9. Cybersecurity. Promising ETFs and Stocks – [Electronic resource]. – Available at: URL: https://bcs-express.ru/novosti-i-analitika/kiberbezopasnost-perspektivnye-etf-i-aktsii (date of accessed: 15.04.2026).

10. Kosinov, Yu. A. Industry-Specific Features of Cybersecurity for the Financial Sector / Yu. A. Kosinov, A. Yu. Sharova // International Journal of Humanities and Natural Sciences. – 2025. – No. 10-2(109). – Pp. 70-74. – DOI 10.24412/2500-1000-2025-10-2-70-74. – EDN UPUGDD.

11. Kostina, T.V. Essence, Main Threats and Risks in Information Security / T.V. Kostina, M.I. Puzyrev // Management of Socio-Economic Systems Development: Globalization, Entrepreneurship, Sustainable Economic Growth: Materials of the XXVI International Scientific Conference of Young Scientists and Students, Donetsk, December 04, 2025. Vol. 2. – Donetsk: Donetsk State University, 2025. – P. 297-300. – EDN BYGYWI.

12. Where to Invest in the Cybersecurity Market – [Electronic resource]. – Access Mode: URL: https://www.vedomosti.ru/investments/articles/2023/08/30/992513-kuda-investirovat-na-rinke-kiberbezopasnosti/ (date of accessed: 15.04.2026).

13. From Attacks to Income: Cybersecurity in an Investor's Portfolio – [Electronic resource]. – Access Mode: URL: https://alfabank.ru/alfa-investor/t/ot-atak-k-dohodu-kiberbezopasnost-v-portfele-investora/?ysclid=mp74u8zioc601281957 (date of accessed: 15.04.2026).

14. Resolution of the 9th Arbitration Appeal Court of 21.09.2023 in Case No. A40-213280/2018 – [Electronic resource]. – Access Mode: URL: https://sudact.ru/arbitral/doc/l5PREG94CrlK/?ysclid=mp5r07ltls736388789 (date of accessed: 14.04.2026).

15. Decision of the Kamyshin City Court of the Volgograd Region of of 02.06.2025 (Dummy Broker) – [Electronic resource]. – Access Mode: URL: https://судебныерешения.рф/89379583?ysclid=mp5qxxwxnj467008744 (date of accessed: 14.04.2026).

16. Decision of the Leninsky District Court of Ivanovo of 22.11.2023 No. 2-1488/2023 (Broker Application Failure) – [Electronic resource]. – Access Mode: URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=KSOJ002&n=168737&ysclid=mp5qwlmpio522414626#5E7EcJVuaAiKh0zM1 (date of accessed: 14.04.2026).

17. Russian business did not pass the crash test for cybersecurity // Insurance News Agency. August 6, 2025. – [Electronic resource]. – Access mode: URL: https://www.asn-news.ru (date of accessed: 04/15/2026).

18. Sergey Demidov, Information Security Director of Moscow Exchange: Russian companies today are limited in means of protection against cyber attacks / Interview with CNews. December 17, 2025. – [Electronic resource]. – Access mode: URL: https://www.cnews.ru (date of accessed: 04.14.2026).

19. Demand for cyber protection // Insurance today. October 7, 2025. – [Electronic resource]. – Access mode: URL: https://www.insur-info.ru (date of accessed: 04.15.2026).

20. Insurance of the digital era: how the Russian cyber insurance market is developing // Vedomosti. October 8, 2025. – [Electronic resource]. – Access mode: URL https://www.vedomosti.ru (date of accessed: 04.15.2026).

21. Insurers note a surge in requests for cyber insurance // Banking Review. August 18, 2025. – [Electronic resource]. – Access mode: URL: https://bosfera.ru (date of accessed: 04.15.2026).

 © Костина Т.В., 2026

22. Cybersecurity funds could be Trump beneficiaries. – [Electronic resource]. – Access mode: URL: https://www.finam.ru/publications/item/fondy-v-oblasti-kiberbezopasnosti-mogut-stat-benefitsiarami-politiki-trampa-20250218-1103/ (date of accessed: 04.15.2026).

Костина Татьяна Витальевна
кандидат экономических наук, доцент, доцент кафедры международный бизнес и деловое администрирование
Федеральное государственное бюджетное образовательное учреждение высшего образования «Донецкий государственный университет», РФ, ДНР, г. Донецк
tv.kostina@mail.ru
+7-949-431-03-96
ORCID 0009-0005-2655-281X

Kostina Tatiana
Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of International Business and Business Administration
Donetsk State University, city Donetsk

© Костина Т.В., 2026