

КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

DOI: 10.17803/1994-1471.2026.190.9.119-131

Э. В. Шамехина*

Информационные технологии как источник коррупционной криминальной опасности

Аннотация. Современное развитие общества сопровождается масштабными преобразованиями, связанными с расширением возможностей и повсеместным использованием информационных технологий. Существенное изменение социальных условий приводит к качественной трансформации коррупционной преступности, в то время как традиционные подходы к противодействию ей утрачивают состоятельность. В этой связи актуальность приобретает формирование теории антикоррупционной криминологической безопасности, основная идея которой заключается в смещении акцентов с карательного реагирования на преступность как источник опасности на формирование целостной системы защитных механизмов, обеспечивающих устойчивость и адаптивность объектов охраны к изменяющемуся спектру коррупционных криминальных угроз. Двойственное положение в контексте данной теории занимают информационные технологии. Благодаря социальной и инфраструктурной значимости они выступают центральным объектом антикоррупционной криминологической безопасности. Одновременно с этим ввиду специфики функционирования и современного состояния правового регулирования информационные технологии также являются и источником коррупционной криминальной опасности. Диалектичность объекта безопасности и источника опасности предопределяет необходимость формирования комплексной стратегии обеспечения антикоррупционной криминологической безопасности информационных технологий, направленной на достижение баланса между технологическим прогрессом и управлением коррупционными рисками в условиях цифровизации общества.

Ключевые слова: информационные технологии; криминологическая безопасность; антикоррупционная безопасность; антикоррупционная криминологическая безопасность; источник опасности; источник угрозы; противодействие преступности; объект безопасности; коррупция; коррупционная опасность

Для цитирования: Шамехина Э. В. Информационные технологии как источник коррупционной криминальной опасности // Актуальные проблемы российского права. — 2026. — Т. 21. — № 9. — С. 119–131. — DOI: 10.17803/1994-1471.2026.190.9.119-131

© Шамехина Э. В., 2026

* Шамехина Эллада Владимировна, старший преподаватель кафедры деликтологии и криминологии Юридического института Сибирского федерального университета, директор Центра противодействия коррупции и правовых экспертиз Департамента по профилактике коррупционных правонарушений Сибирского федерального университета
ул. Маерчака, д. 6, г. Красноярск, Российская Федерация, 660075
lada.shamehina@mail.ru

Information Technology as a Source of Corruption-Related Criminal Danger

Ellada V. Shamekhina, Senior Lecturer, Department of Tort Law and Criminology, Law Institute, Siberian Federal University, Director, Center for Combating Corruption and Legal Expertise, Department for the Prevention of Corruption Offenses, Siberian Federal University, Krasnoyarsk, Russian Federation
lada.shamekhina@mail.ru

Abstract. The modern development of society is accompanied by large-scale transformations associated with the expansion of opportunities and the widespread use of information technology. Significant changes in social conditions lead to a qualitative transformation of corruption-related crime, while traditional approaches to countering it are losing their effectiveness. In this regard, the formation of a theory of anti-corruption criminological security becomes particularly relevant. The core idea of this theory is to shift the focus from punitive responses to crime as a source of danger to the development of an integrated system of protective mechanisms that ensure the resilience and adaptability of protected objects to the evolving spectrum of corruption-related criminal threats. Information technologies occupy a dual position in the context of this theory. Due to their social and infrastructural significance, they act as a central object of anti-corruption criminological security. At the same time, given the specifics of their functioning and the current state of legal regulation, information technologies also constitute a source of corruption-related criminal danger. The dialectical nature of an object of security and a source of danger determines the need to develop a comprehensive strategy for ensuring anti-corruption criminological security of information technologies. This strategy should aim to achieve a balance between technological progress and the management of corruption risks in the context of the digitalization of society.

Keywords: information technology; criminological security; anti-corruption security; anti-corruption criminological security; source of danger; source of threat; combating crime; security object; corruption; corruption threat

Cite as: Shamekhina EV. Information Technology as a Source of Corruption-Related Criminal Danger. Aktual'nye problemy rossijskogo prava. 2026;21(9):119-131. (In Russ.). DOI: 10.17803/1994-1471.2026.190.9.119-131

Современная эпоха характеризуется масштабными переменами и глубокими трансформациями всех сфер общественной жизни. Стремительное развитие информационных технологий привело к формированию принципиально новой реальности, в которой традиционные институты и правила функционирования общества подвергаются существенному переосмыслению. Эти процессы неизбежно затрагивают и феномен преступности, которая приобретает новые формы и виды под влиянием социальных новаций. Криминальный ландшафт претерпевает очевидные изменения,

выраженные в модификации традиционных и возникновении совершенно новых вариаций преступного поведения. В этой связи устоявшиеся подходы к противодействию преступности, сформировавшиеся в иных исторических и социальных условиях, во многом исчерпали свой практический ресурс и не в полной мере эффективны в новых реалиях.

В современной научной литературе всё чаще подчеркивается важность развития идей криминологической безопасности как нового научного направления в криминологии¹. Ключевой особенностью теории криминологической

¹ См.: Бабаев М. М. Уголовная политика и криминологическая безопасность // Научный портал МВД России. 2008. № 3. С. 53–58 ; Лебедев С. Я. Криминологическая безопасность личности, общества, государства // Правовая наука на рубеже XXI столетия: 1920–2000 : сборник научных трудов. Омск, 2000. С. 13–22 ; Плешаков В. А. Криминологическая безопасность и ее обеспечение в сфере взаимовлияния организованной преступности и преступности несовершеннолетних : дис. ... д-ра юрид. наук. М., 1998 ; Клейменов М. П. Прогнозирование криминологической безопасности // Закономерности преступности, стратегия борьбы и закон. М. : Российская криминологическая ассоциация, 2001. С. 41–45 ; Джафарли В. Ф. Теория

безопасности является принципиальное смещение акцентов с традиционных мер борьбы с преступностью на усиление защитных функций охраняемых объектов. Такой подход подразумевает смену парадигмы антикриминальной деятельности и переход от реактивной модели противодействия преступности (реакции на уже совершенное преступление) к проактивной стратегии обеспечения безопасности (действиям на опережение). В разрезе данной концепции необходимость борьбы с преступностью не ставится под сомнение, но дополняется системой мер, направленных на повышение криминологической устойчивости охраняемых объектов. Это предполагает создание условий, при которых реализация преступных намерений становится максимально затруднительной, а потенциальные жертвы обладают достаточными ресурсами для самозащиты и нейтрализации криминальных угроз. Полагаем, что теория криминологической безопасности способна стать основанием нового системного и междисциплинарного подхода к противодействию преступности, базирующегося на формировании устойчивых иммунитетов объектов защиты к криминальным угрозам.

Постепенно в контексте теории криминологической безопасности формируются концептуальные предпосылки для становления частнонаучной криминологической теории — теории антикоррупционной криминологической безопасности, основная идея которой заключается в изменении теоретико-методологических подходов к пониманию и построению матрицы научного познания, объясняющего закономерности взаимодействия объектов охраны с источниками криминальной коррупционной опасности, а также обеспечивающего научно обос-

нованные подходы к защите объекта охраны и противодействию источнику опасности².

Базовыми категориями применительно к рассматриваемой теории выступают «объект антикоррупционной криминологической безопасности» и «источник коррупционной криминальной опасности». Примечательно, что ряд объектов может представлять одновременно в двух качествах: как ценность, которая подлежит защите и охране, а также как источник опасности, от которой ее собственно защищают и охраняют. Полагаем, что таким объектом являются информационные технологии.

Глобальная роль информационных технологий в эпоху цифровой трансформации не ставится под сомнение. Ввиду их фундаментальной социальной ценности и критической значимости для функционирования современного общества информационные технологии надлежит относить к **объектам антикоррупционной криминологической безопасности**. Поскольку сегодня подавляющее большинство сфер человеческой деятельности так или иначе зависит от функционирования различных технологических устройств и информационных систем, коррупционные посяательства на них могут иметь значительные негативные последствия в масштабах всего общества и государства. Важно подчеркнуть, что в контексте обеспечения антикоррупционной безопасности информационные технологии должны подлежать защите и как носитель информации, которая обладает самостоятельной ценностью, и как инструмент, интегрированный в процессы аналитики, принятия решений и управления. Соответственно, антикоррупционная криминологическая безопасность информационных технологий должна обеспечиваться одновременно на содержатель-

криминологической безопасности как базовой научной категории обеспечения защиты от преступления // Ученые труды Российской академии адвокатуры и нотариата. 2020. № 2 (57). С. 82–86 ; Савельев А. И. Криминологическая безопасность как вид национальной безопасности // Вестник Омской юридической академии. 2019. Т. 16. № 1. С. 49–54 ; Лапин А. А. Криминологическая безопасность в стратегии национальной безопасности России // Вестник Российского университета дружбы народов. Серия «Юридические науки». 2015. № 1. С. 29–36.

² См.: Антикоррупционные меры безопасности / под ред. Н. В. Щедрина, И. А. Дамм. М. : Проспект, 2020 ; Дамм И. А. Антикоррупционная криминологическая безопасность как новое направление научных исследований // Всероссийский криминологический журнал. 2021. Т. 15. № 6. С. 739.

ном и процедурном уровнях, что подчеркивает сложную структуру защищаемого объекта.

В качестве **источника коррупционной криминальной опасности** информационные технологии на сегодняшний день исследованы недостаточно. Феномен опасности остается предметом научного осмысления, и в настоящее время выделяются различные подходы к его трактовке и содержательному наполнению³, а недостаточная развитость общетеоретического понимания категории «источник опасности» неизбежно создает сложности в определении сущностных характеристик его отраслевых проявлений⁴. В то же время имеющиеся теоретические наработки позволяют сделать вывод, что к источникам опасности относятся различные по своей природе объекты, субъекты и виды деятельности, которые обладают возможностью причинения вреда. С учетом данной характеристики возможность отнесения информационных технологий к категории источника коррупционной криминальной опасности будет зависеть от ответа на вопрос, обладают ли информационные технологии способностью к причинению вреда.

Полагаем, что информационным технологиям присущ определенный криминогенный потенциал ввиду следующих оснований. Во-первых, информационные технологии способствовали изменению традиционных и появлению качественно новых сфер, в которых возможна реализация коррупционных практик. Поскольку информационные технологии глубоко интегрированы во все области социальных взаимодействий, они выступают уже не просто техническим инструментарием, а инфраструк-

турой, в рамках которой строится повседневная социальная жизнь. С учетом того, что информационные технологии задействованы в системах электронного голосования, цифровых реестрах и онлайн-платформах государственных услуг, коррупционное воздействие на такие системы способно причинить ущерб фундаментальным демократическим ценностям и принципам справедливого государственного управления. Цифровая трансформация государственного управления создает критические точки уязвимости, где концентрация распорядительных функций в рамках автоматизированных систем открывает возможности для системных злоупотреблений.

Помимо трансформации уже существующих социальных сфер, информационные технологии способствовали возникновению принципиально новой среды, способной стать плацдармом для коррупционных практик. Метавселенные и платформы виртуальной реальности, представляющие собой децентрализованные цифровые экосистемы с собственными экономическими и социальными ценностями, порождают уникальные коррупционные риски. Помимо прочего, они также связаны с правовой неурегулированностью новых вселенных, а также анонимностью в виртуальном пространстве и существенно сниженными рисками обнаружения факта совершенного коррупционного деяния ввиду сложности и инновационности данных технологий. Кроме того, новые миры предоставляют широкие возможности для отмывания преступных доходов⁵, полученных в том числе коррупционным путем. В связи с возрастающими криминальными рисками объектом научного

³ См.: *Ирошников Д. В.* Безопасность как правовая категория : дис. ... д-ра юрид. наук. М., 2021 ; *Романович А. Л.* Концепция безопасного развития социоприродных систем (философско-методологический анализ) : дис. ... д-ра филос. наук. М., 2004 ; *Ярочкин В. И., Бузанова Я. В.* Теория безопасности. М. : Академический проект, 2005.

⁴ См.: *Дамм И. А.* Коррупционная преступность как источник опасности в теории антикоррупционной криминологической безопасности // Журнал Сибирского федерального университета. Серия «Гуманитарные науки». 2025. Т. 18. № 8. С. 1545 ; *Она же.* Категории «опасность» и «угроза» в контексте криминологической безопасности // Сибирский антропологический журнал. 2025. Т. 9. № 2. С. 93.

⁵ *Сидоренко Э. Л.* Легализация преступных доходов с использованием DeFi: типовые схемы и индикаторы риска // Russian Journal of Economics and Law. 2023. Т. 17. № 4. С. 832–833.

осмысления становится такое явление, как преступность в метавселенных⁶.

Во-вторых, информационные технологии в силу некоторых особенностей функционирования могут способствовать совершению коррупционных преступлений или облегчать их реализацию. В первую очередь это связано с относительной анонимностью и высокой степенью сложности современных технологий.

Анонимность в информационно-технологической среде представляет собой сложный, многоаспектный феномен, который формирует уникальные условия для развития и эскалации коррупционных практик. С криминологической точки зрения анонимность выступает как системообразующая детерминанта, создающая благоприятную среду для реализации коррупционных схем за счет существенного снижения рисков обнаружения, идентификации и привлечения к ответственности субъектов противоправной деятельности. В рамках теории рационального выбора преступности анонимность действует как фактор, кардинально изменяющий соотношение издержек и выгод при принятии решения о совершении коррупционного деяния. Снижение вероятности обнаружения и наказания приводит к увеличению ожидаемой полезности от коррупционного поведения, что стимулирует рост коррупционной активности среди потенциальных правонарушителей. В частности, именно на принципах анонимности владения основана концепция криптовалют, всё чаще используемых в совершении коррупционных преступлений.

Как справедливо отмечает Н. А. Лопашенко, «пришло время, когда человек не успевает за

запущенными собой же процессами, отстает от них, и чем дальше, тем это отставание будет больше»⁷. Современные информационные технологии характеризуются экспоненциально возрастающей сложностью, которая проявляется на множественных уровнях архитектуры, функционала и взаимодействия компонентов цифровых систем. Эта сложность создает уникальные возможности для коррупционных злоупотреблений, поскольку формирует асимметрию знаний между техническими специалистами, имеющими глубокое понимание системных процессов, и контролирующими субъектами, обладающими ограниченными компетенциями в сфере информационных технологий.

В управленческой и коммерческой деятельности всё чаще используют сложные алгоритмы машинного обучения, искусственного интеллекта и больших данных, функционирование которых характеризуется высокой степенью непрозрачности даже для их создателей. Этот «черный ящик» создает идеальные условия для сокрытия коррупционных манипуляций. Они могут выражаться в незаметном изменении параметров алгоритмов принятия решений в различных автоматизированных системах, например государственных закупок или распределения социальных выплат. Такие изменения могут обеспечивать системное преимущество определенных юридических или физических лиц при сохранении видимости объективности и справедливости автоматизированных процедур.

Коррупционные злоупотребления могут быть связаны с искажением алгоритмов машинного обучения с целью создания скрытых преферен-

⁶ См.: *Бегишев И. Р., Денисович В. В.* Метавселенные в уголовно-правовом измерении // *Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции*, Казань, 22 сентября 2023 г. : в 6 т. Казань : Познание, 2023. Т. 2. С. 40–44 ; *Ефремова М. А., Русскиевич Е. А.* Уголовно-правовые проблемы противодействия преступности в метавселенной: современное состояние и перспективы развития // *Journal of Digital Technologies and Law*. 2025. Т. 3. № 2. Р. 187–202.

⁷ *Лопашенко Н. А.* Новые реалии преступности в цифровом мире и в эпоху развития искусственного интеллекта и уголовно-правовая реакция на них: не стоит «прогибаться под изменчивый мир»? // *Уголовный закон в эпоху искусственного интеллекта и цифровизации : сборник трудов по материалам Всероссийской научно-практической конференции с международным участием в рамках I Саратовского международного юридического форума, посвященного 90-летию юбилею Саратовской государственной юридической академии*, Саратов, 9 июня 2021 г. Саратов : Саратов. гос. юрид. академия, 2021. С. 17.

ций для определенных категорий заявителей или участников конкурсных процедур. Поскольку современные системы искусственного интеллекта обучаются на больших массивах данных и используют сложные нейронные сети, выявление таких искажений требует глубокой технической экспертизы и значительных вычислительных ресурсов.

Существенная проблема заключается в том, что лица, ответственные за противодействие коррупции, как правило, не обладают необходимыми техническими знаниями для эффективного контроля IT-специалистов, что создает критическую уязвимость в системе безопасности. Компетентностный разрыв между управленческим звеном и техническими специалистами формирует неконтролируемые рискогенные зоны. Специалисты по противодействию коррупции, обладая в большей степени юридическими и управленческими компетенциями, в определенных случаях могут оказаться неспособными оценить правомерность действий технических специалистов. В это время технические специалисты, обладающие привилегированным доступом к критически важным информационным системам, имеют возможность стать ключевыми фигурами в новой архитектуре коррупционных рисков. Системные администраторы, программисты, разработчики баз данных, специалисты по информационной безопасности получают беспрецедентные возможности для коррупционных манипуляций, что актуализирует необходимость контроля их деятельности.

В-третьих, криминогенность информационных технологий связана с пробельностью нор-

мативно-правового регулирования цифровой среды. Стремительное развитие информационных технологий опережает формирование соответствующей правовой базы и создает правовые вакуумы, используемые в коррупционных целях. Особенно критичной является недостаточная регламентация применения технологий искусственного интеллекта, блокчейна и криптовалют.

Полагаем, что в части использования информационных технологий при совершении коррупционных преступлений необходима «цифровая настройка» УК РФ. Соглашаясь с мнением А. Е. Русскевича о том, что «цифровизация мало что добавляет и без труда “укладывается” в содержание законодательных моделей подавляющего большинства составов преступлений»⁸, полагаем: наличие информационных технологий в механизме совершения коррупционного преступления не образует некий новый, неизвестный уголовному праву состав преступления и не требует введения новых статей в УК РФ. В то же время возможны ситуации, когда некий новый цифровой объект играет существенную роль в совершении преступления, а его неотражение в диспозиции уголовно-правовой нормы влечет за собой невозможность квалифицировать данное деяние как преступное. Так, вызывал дискуссии вопрос о возможности отнесения криптовалют к предмету взятничества⁹ в связи с тем, что в ст. 290 УК РФ содержится исчерпывающий перечень объектов, в которых может быть выражена взятка, и криптовалюты на сегодняшний день невозможно безусловно отнести ни к од-

⁸ Русскевич Е. А. Цифровизация уголовного законодательства: непростые последствия простых решений // Вестник Университета имени О.Е. Кутафина (МГЮА). 2025. № 5 (129). С. 26–33.

⁹ См.: Антонов Т. Г. Некоторые проблемы квалификации преступлений, предусмотренных статьями 290–291.2 УК РФ, по предмету преступления // Уголовно-исполнительная система: педагогика, психология и право : материалы Всероссийской научно-практической конференции, Томск, 19–20 апреля 2018 г. : в 2 ч. / под общ. ред. В. А. Уткина. Вып. 6. Томск : Томский институт повышения квалификации работников ФСИН, 2018. Ч. 1. С. 46–49 ; Гринько С. Д. Проблемы квалификации коррупционных преступлений при использовании цифровой валюты в качестве взятки // Юрист. 2022. № 6. С. 13–16 ; Никонов П. В. Роль информационно-коммуникационных технологий и компьютерной информации в совершении коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 г. М. : Университет прокуратуры РФ, 2021. С. 132–136.

ной из представленных категорий. Разрешение данного вопроса предложено в законодательной инициативе Следственного комитета РФ о признании цифровых валют имуществом для целей Уголовного и Уголовно-процессуального кодексов РФ¹⁰. Полагаем, что в УК РФ следует отразить появление не только цифровых валют, но и иных цифровых объектов, представляющих как имущественную, так и иную ценность в современном мире. Помимо адаптации уголовного закона к нынешним социальным условиям, такое решение позволит закрыть правовые пробелы, способствующие совершению коррупционных деяний ввиду убежденности субъектов, что их действия не охватываются правовыми нормами и не влекут за собой наступление уголовной ответственности.

Следует также подчеркнуть, что осложняющим правовое регулирование элементом является транснациональный характер современных информационных технологий. В этой связи, как отмечает Т. Я. Хабриева, «возможность регулирования многих общественных отношений в пределах юрисдикции национального государства становится весьма относительной, заметно повышается роль международно-правовых регуляторов, хотя степень их воздействия на международные отношения и правовая природа инструментов отличаются большим разнообразием»¹¹. Что же касается международного сотрудничества в части противодействия высокотехнологичной преступности, то оно осложняется еще и отсутствием единой терминологической базы, поскольку «ученые-криминологи из

стран с романо-германской и англосаксонской правовыми системами используют различные термины для описания преступности в цифровой сфере»¹².

Показательным примером является попытка принятия международного акта в сфере противодействия преступности с использованием информационных технологий. С 2017 г. Российская Федерация выступает инициатором разработки универсального международного акта, который бы заложил основы для регулирования и международного сотрудничества в указанной сфере. В 2021 г. наша страна представила проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях¹³. Российские разработчики проекта стремились добиться максимального охвата различных преступных деяний, что отражает название конвенции. Однако в ходе переговоров, длившихся более трех лет, название конвенции было изменено, и в августе 2024 г. в ходе заключительной сессии был представлен уже Проект конвенции Организации Объединенных Наций против киберпреступности¹⁴. Представители России отметили, что не считают «заголовок конвенции корректным и правильным образом отражающим предмет и охват документа»¹⁵.

В совокупности перечисленное свидетельствует о том, что информационные технологии успешно могут быть интегрированы в коррупционную деятельность и связаны с причинением вреда охраняемым объектам. Вместе с тем коррупциогенный потенциал информационных

¹⁰ Законопроект № 859650-8 «О внесении изменений в Уголовный кодекс Российской Федерации» // URL: <https://sozd.duma.gov.ru/bill/859650-8> (дата обращения: 23.10.2025).

¹¹ Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9 (261). С. 8.

¹² Блокчейн в цифровой криминологии: постановка проблемы / А. П. Суходолов, Е. А. Антонян, М. В. Рукинов [и др.] // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 556.

¹³ Проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях // URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 19.10.2025).

¹⁴ Проект конвенции Организации Объединенных Наций против киберпреступности // URL: <https://documents.un.org/doc/undoc/gen/v24/055/08/pdf/v2405508.pdf> (дата обращения: 19.10.2025).

¹⁵ Киберпространство вписали в компромисс // URL: <https://www.kommersant.ru/doc/6890107> (дата обращения: 19.10.2025).

технологий ранее мог быть реализован только в ходе использования их человеком, который преследует преступные цели и задействует технологический инструментарий в криминальной деятельности. Полагаем допустимой аналогию с транспортным средством, которое в силу ст. 1079 ГК РФ отнесено к источникам повышенной опасности. При этом транспортное средство может рассматриваться в указанном качестве только в случае его использования по прямому функциональному назначению в ходе участия в дорожном движении. Стоящий с выключенным двигателем автомобиль не является источником повышенной опасности. В этой связи логично предположить, что вне практического использования, в стационарном состоянии информационные технологии несут определенную коррупционную криминальную опасность, однако потенциальную способность причинить вред объектам антикоррупционной криминологической безопасности приобретают только в ходе эксплуатации человеком.

Впрочем, с учетом стремительных темпов развития искусственного интеллекта и его способности функционировать без вмешательства человека поставленный вопрос о возможности информационных технологий выступать самостоятельным источником опасности требует дополнительного осмысления. Переход от классических информационных систем, полностью контролируемых оператором, к интеллектуальным платформам, обладающим элементами самоуправления и самовоспроизведения, может свидетельствовать о наличии опасности и вне поля человеческой деятельности. Возможны ситуации, при которых интеллектуальные системы будут способны самостоятельно развивать коррупционные сценарии. Такое допущение

подводит нас к дискуссии о способности искусственного интеллекта выступать субъектом права¹⁶.

Сказанное позволяет сделать вывод о потенциальной коррупционной криминальной опасности информационных технологий. При этом эскалация присущих им опасных свойств до степени реальной возможности адресного причинения вреда позволяет рассматривать информационные технологии в качественно новом состоянии **источника коррупционной криминальной угрозы**.

Полагаем: в ряде критически важных сфер степень потенциальной коррупционной опасности, порождаемой информационными технологиями, настолько высока, что фактически переходит в состояние адресной угрозы. Это происходит там, где зависимость социальных процессов от информационных технологий достигает максимума, а масштаб негативных последствий может быть критичным. К таким сферам могут быть отнесены государственное управление и политические процессы. Например, системы электронного голосования могут становиться объектом массовых атак, направленных на манипулирование результатами голосования. В данном случае опасность трансформируется в конкретную угрозу подрыва легитимности выборов.

Риски причинения вреда вследствие коррупционного использования информационных технологий крайне высоки также в сфере обеспечения защиты конфиденциальной информации. Проникновение в системы хранения и обработки конфиденциальных данных открывает широчайшие возможности неправомерного их использования, что существенно увеличивает уровень коррупционной опасности и переводит

¹⁶ См.: Шестак В. А., Волеводз А. Г., Ализаде В. А. О возможности доктринального восприятия системой общего права искусственного интеллекта как субъекта преступления: на примере уголовного законодательства США // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 547–554 ; Хисамова З. И., Бегишев И. Р. Правовое регулирование искусственного интеллекта // Baikal Research Journal. 2019. Т. 10. № 2 ; Жмуров Д. В. Грехи машин: у истоков робопреступности // Всероссийский криминологический журнал. 2023. Т. 17. № 6. С. 536–542 ; Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : дис. ... д-ра юрид. наук. М., 2018 ; Архипов В. В., Наумов В. Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. 2017. № 5. С. 157–170.

ее в состояние адресной угрозы. Неправомерный доступ к конфиденциальной информации может стать основой для системного шантажа и давления на отдельных лиц и институты. Например, получение доступа к личной медицинской, финансовой или корпоративной информации позволяет злоумышленникам устраивать «выбросы» компрометирующих сведений, инициировать информационные атаки, шантажировать должностных лиц или представителей крупного бизнеса, требуя взятки за неразглашение, или влиять на принятие решений.

Повышению степени опасности способствует тот факт, что «современные информационно-телекоммуникационные технологии могут быть использованы как средства террора, войны и оружия»¹⁷. Чрезвычайно опасным является риск неправомерного доступа к электросетям, системам коммунальных и транспортных инфраструктур, системам обеспечения жизнедеятельности и военно-промышленному комплексу, что способствует созданию угроз национального масштаба. Массовое вмешательство в эти системы может привести к сбоям, отключениям, авариям

и катастрофам, что не только ставит под угрозу жизни и здоровье граждан, но и подрывает основы национальной безопасности.

Таким образом, анализ свидетельствует о том, что информационные технологии занимают двойственное положение в системе теории антикоррупционной криминологической безопасности, представляя собой объект с выраженной дуалистичной природой. С одной стороны, они выступают ценностью, требующей защиты от коррупционных посягательств, ввиду их критической значимости для функционирования современного государства и общества. С другой стороны, информационные технологии обладают объективной способностью генерировать коррупционную криминальную опасность, которая в наиболее уязвимых значимых сферах может трансформироваться в адресную угрозу национальной безопасности. Единство объекта безопасности и источника опасности актуализирует необходимость формирования комплексной стратегии обеспечения антикоррупционной криминологической безопасности информационных технологий.

БИБЛИОГРАФИЯ

1. Антикоррупционные меры безопасности / под ред. Н. В. Щедрина, И. А. Дамм. — М. : Проспект, 2020. — 496 с.
2. Антонов Т. Г. Некоторые проблемы квалификации преступлений, предусмотренных статьями 290–291.2 УК РФ, по предмету преступления // Уголовно-исполнительная система: педагогика, психология и право : материалы Всероссийской научно-практической конференции, Томск, 19–20 апреля 2018 г. : в 2 ч. / под общ. ред. В. А. Уткина. Вып. 6. Ч. 1. — Томск : Федеральное казенное образовательное учреждение дополнительного профессионального образования «Томский институт повышения квалификации работников Федеральной службы исполнения наказаний», 2018. — С. 46–49.
3. Архипов В. В., Наумов В. Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. — 2017. — № 5. — С. 157–170.
4. Бабаев М. М. Уголовная политика и криминологическая безопасность // Научный портал МВД России. — 2008. — № 3. — С. 53–58.
5. Бегишев И. Р., Денисович В. В. Мета вселенные в уголовно-правовом измерении // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции, Казань, 22 сентября 2023 г. : в 6 т. Т. 2. — Казань : Познание, 2023. — С. 40–44.
6. Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. — Казань : Познание, 2020. — С. 103–104.

¹⁷ Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань : Познание, 2020. С. 103–104.

7. Блокчейн в цифровой криминологии: постановка проблемы / А. П. Суходолов, Е. А. Антонян, М. В. Рукинов [и др.] // Всероссийский криминологический журнал. — 2019. — Т. 13. — № 4. — С. 555–563.
8. *Гринько С. Д.* Проблемы квалификации коррупционных преступлений при использовании цифровой валюты в качестве взятки // Юрист. — 2022. — № 6. — С. 13–16.
9. *Дамм И. А.* Антикоррупционная криминологическая безопасность как новое направление научных исследований // Всероссийский криминологический журнал. — 2021. — Т. 15. — № 6. — С. 734–743.
10. *Дамм И. А.* Категории «опасность» и «угроза» в контексте криминологической безопасности // Сибирский антропологический журнал. — 2025. — Т. 9. — № 2. — С. 92–97.
11. *Дамм И. А.* Коррупционная преступность как источник опасности в теории антикоррупционной криминологической безопасности // Журнал Сибирского федерального университета. Серия «Гуманитарные науки». — 2025. — Т. 18. — № 8. — С. 1540–1551.
12. *Джафарли В. Ф.* Теория криминологической безопасности как базовой научной категории обеспечения защиты от преступления // Ученые труды Российской академии адвокатуры и нотариата. — 2020. — № 2 (57). — С. 82–86.
13. *Ефремова М. А., Русскевич Е. А.* Уголовно-правовые проблемы противодействия преступности в метавселенной: современное состояние и перспективы развития // Journal of Digital Technologies and Law. — 2025. — Т. 3. — № 2. — С. 187–202.
14. *Жмуров Д. В.* Грехи машин: у истоков робопреступности // Всероссийский криминологический журнал. — 2023. — Т. 17. — № 6. — С. 536–542.
15. *Ирошников Д. В.* Безопасность как правовая категория : дис. ... д-ра юрид. наук. — М., 2021. — 596 с.
16. *Клейменов М. П.* Прогнозирование криминологической безопасности // Закономерности преступности, стратегия борьбы и закон. — М. : Российская криминологическая ассоциация, 2001. — С. 41–45.
17. *Лапин А. А.* Криминологическая безопасность в стратегии национальной безопасности России // Вестник Российского университета дружбы народов. Серия «Юридические науки». — 2015. — № 1. — С. 29–36.
18. *Лебедев С. Я.* Криминологическая безопасность личности, общества, государства // Правовая наука на рубеже XXI столетия: 1920–2000 : сборник научных трудов. — Омск, 2000. — С. 13–22.
19. *Лопашенко Н. А.* Новые реалии преступности в цифровом мире и в эпоху развития искусственного интеллекта и уголовно-правовая реакция на них: не стоит «прогибаться под изменчивый мир»? // Уголовный закон в эпоху искусственного интеллекта и цифровизации : сборник трудов по материалам Всероссийской научно-практической конференции с международным участием в рамках I Саратовского международного юридического форума, посвященного 90-летию юбилею Саратовской государственной юридической академии, Саратов, 9 июня 2021 г. — Саратов : Саратовская государственная юридическая академия, 2021. — С. 15–31.
20. *Морхат П. М.* Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : дис. ... д-ра юрид. наук. — М., 2018. — 420 с.
21. *Никонов П. В.* Роль информационно-коммуникационных технологий и компьютерной информации в совершении коррупционных преступлений, связанных с дачей и получением взятки и иными видами незаконного вознаграждения // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 г. — М. : Федеральное государственное казенное образовательное учреждение высшего образования «Университет прокуратуры Российской Федерации», 2021. — С. 132–136.
22. *Плешаков В. А.* Криминологическая безопасность и ее обеспечение в сфере взаимовлияния организованной преступности и преступности несовершеннолетних : дис. ... д-ра юрид. наук. — М., 1998. — 323 с.
23. *Романович А. Л.* Концепция безопасного развития социоприродных систем (философско-методологический анализ) : дис. ... д-ра филос. наук. — М., 2004. — 418 с.

24. Русскевич Е. А. Цифровизация уголовного законодательства: непростые последствия простых решений // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2025. — № 5 (129). — С. 26–33.
25. Савельев А. И. Криминологическая безопасность как вид национальной безопасности // Вестник Омской юридической академии. — 2019. — Т. 16. — № 1. — С. 49–54.
26. Сидоренко Э. Л. Легализация преступных доходов с использованием DeFi: типовые схемы и индикаторы риска // Russian Journal of Economics and Law. — 2023. — Т. 17. — № 4. — С. 832–833.
27. Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. — 2018. — № 9 (261). — С. 5–16.
28. Хисамова З. И., Бегишев И. Р. Правовое регулирование искусственного интеллекта // Baikal Research Journal. — 2019. — Т. 10. — № 2.
29. Шамехина Э. В. Криптовалюты как предмет взяточничества: проблемы регулирования // Енисейские политико-правовые чтения : сборник научных статей по материалам XVI Всероссийской научно-практической конференции, Красноярск, 20–21 сентября 2024 г. — Красноярск : Красноярское региональное отделение общероссийской общественной организации «Ассоциация юристов России», 2024. — С. 404–412.
30. Шестак В. А., Волеводз А. Г., Ализаде В. А. О возможности доктринального восприятия системой общего права искусственного интеллекта как субъекта преступления: на примере уголовного законодательства США // Всероссийский криминологический журнал. — 2019. — Т. 13. — № 4. — С. 547–554.
31. Ярочкин В. И., Бузанова Я. В. Теория безопасности. — М. : Академический проект, 2005. — 173 с.

Материал поступил в редакцию 10 ноября 2025 г.

REFERENCES (TRANSLITERATION)

1. Antikorruptsionnye mery bezopasnosti / pod red. N. V. Shchedrina, I. A. Damm. — М.: Prospekt, 2020. — 496 s.
2. Antonov T. G. Nekotorye problemy kvalifikatsii prestupleniy, predusmotrennykh statyami 290–291.2 UK RF, po predmetu prestupleniya // Ugolovno-ispolnitelnaya sistema: pedagogika, psikhologiya i pravo: materialy Vserossiyskoy nauchno-prakticheskoy konferentsii, Tomsk, 19–20 aprelya 2018 g.: v 2 ch. / pod obshch. red. V. A. Utkina. Vyp. 6. Ch. 1. — Tomsk: Federalnoe kazennoe obrazovatelnoe uchrezhdenie dopolnitelnogo professionalnogo obrazovaniya «Tomskiy institut povysheniya kvalifikatsii rabotnikov Federalnoy sluzhby ispolneniya nakazaniy», 2018. — S. 46–49.
3. Arkhipov V. V., Naumov V. B. O nekotorykh voprosakh teoreticheskikh osnovaniy razvitiya zakonodatelstva o robototekhnike: aspekty voli i pravosubektnosti // Zakon. — 2017. — № 5. — S. 157–170.
4. Babaev M. M. Ugolovnaya politika i kriminologicheskaya bezopasnost // Nauchnyy portal MVD Rossii. — 2008. — № 3. — S. 53–58.
5. Begishev I. R., Denisovich V. V. Metavselennyye v ugolovno-pravovom izmerenii // Tsifrovyye tekhnologii i pravo: sbornik nauchnykh trudov II Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Kazan, 22 sentyabrya 2023 g.: v 6 t. T. 2. — Kazan: Poznanie, 2023. — S. 40–44.
6. Begishev I. R., Bikeev I. I. Prestupleniya v sfere obrashcheniya tsifrovoy informatsii. — Kazan: Poznanie, 2020. — S. 103–104.
7. Blokcheyn v tsifrovoy kriminologii: postanovka problemy / A. P. Sukhodolov, E. A. Antonyan, M. V. Rukinov [i dr.] // Vserossiyskiy kriminologicheskiy zhurnal. — 2019. — Т. 13. — № 4. — S. 555–563.
8. Grinko S. D. Problemy kvalifikatsii korruptsionnykh prestupleniy pri ispolzovanii tsifrovoy valyuty v kachestve vzyatki // Yurist. — 2022. — № 6. — S. 13–16.
9. Damm I. A. Antikorruptsionnaya kriminologicheskaya bezopasnost kak novoe napravlenie nauchnykh issledovaniy // Vserossiyskiy kriminologicheskiy zhurnal. — 2021. — Т. 15. — № 6. — S. 734–743.

10. Damm I. A. Kategorii «opasnost» i «ugroza» v kontekste kriminologicheskoy bezopasnosti // Sibirskiy antropologicheskij zhurnal. — 2025. — T. 9. — № 2. — S. 92–97.
11. Damm I. A. Korruptsiennaya prestupnost kak istochnik opasnosti v teorii antikorrupcionnoy kriminologicheskoy bezopasnosti // Zhurnal Sibirskogo federalnogo universiteta. Seriya «Gumanitarnye nauki». — 2025. — T. 18. — № 8. — S. 1540–1551.
12. Dzhafarli V. F. Teoriya kriminologicheskoy bezopasnosti kak bazovoy nauchnoy kategorii obespecheniya zashchity ot prestupleniya // Uchenye trudy Rossiyskoy akademii advokatury i notariata. — 2020. — № 2 (57). — S. 82–86.
13. Efremova M. A., Russkevich E. A. Ugolovno-pravovye problemy protivodeystviya prestupnosti v metavselennoy: sovremennoe sostoyanie i perspektivy razvitiya // Journal of Digital Technologies and Law. — 2025. — T. 3. — № 2. — S. 187–202.
14. Zhmurov D. V. Grekhi mashin: u istokov roboprestupnosti // Vserossiyskiy kriminologicheskij zhurnal. — 2023. — T. 17. — № 6. — S. 536–542.
15. Iroshnikov D. V. Bezopasnost kak pravovaya kategoriya: dis. ... d-ra yurid. nauk. — M., 2021. — 596 s.
16. Kleymenov M. P. Prognozirovaniye kriminologicheskoy bezopasnosti // Zakonomernosti prestupnosti, strategiya borby i zakon. — M.: Rossiyskaya kriminologicheskaya assotsiatsiya, 2001. — S. 41–45.
17. Lapin A. A. Kriminologicheskaya bezopasnost v strategii natsionalnoy bezopasnosti Rossii // Vestnik Rossiyskogo universiteta druzhby narodov. Seriya «Yuridicheskie nauki». — 2015. — № 1. — S. 29–36.
18. Lebedev S. Ya. Kriminologicheskaya bezopasnost lichnosti, obshchestva, gosudarstva // Pravovaya nauka na rubezhe XXI stoletiya: 1920–2000: sbornik nauchnykh trudov. — Omsk, 2000. — S. 13–22.
19. Lopashenko N. A. Novye realii prestupnosti v tsifrovom mire i v epokhu razvitiya iskusstvennogo intellekta i ugolovno-pravovaya reaktsiya na nikh: ne stoit «progibatsya pod izmenchivyy mir»? // Ugolovnyy zakon v epokhu iskusstvennogo intellekta i tsifrovizatsii: sbornik trudov po materialam Vserossiyskoy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem v ramkakh I Saratovskogo mezhdunarodnogo yuridicheskogo foruma, posvyashchennogo 90-letnemu yubileyu Saratovskoy gosudarstvennoy yuridicheskoy akademii, Saratov, 9 iyunya 2021 g. — Saratov: Saratovskaya gosudarstvennaya yuridicheskaya akademiya, 2021. — S. 15–31.
20. Morkhat P. M. Pravosubektnost iskusstvennogo intellekta v sfere prava intellektualnoy sobstvennosti: grazhdansko-pravovye problemy: dis. ... d-ra yurid. nauk. — M., 2018. — 420 s.
21. Nikonov P. V. Rol informatsionno-kommunikatsionnykh tekhnologiy i kompyuternoy informatsii v sovershenii korruptsionnykh prestupleniy, svyazannykh s dachey i polucheniem vzyatki i inymi vidami nezakonno go voznagrashdeniya // Tsifrovye tekhnologii v borbe s prestupnostyu: problemy, sostoyanie, tendentsii: sbornik materialov I Vserossiyskoy nauchno-prakticheskoy konferentsii, Moskva, 27 yanvarya 2021 g. — M.: Federalnoe gosudarstvennoe kazennoe obrazovatelnoe uchrezhdenie vysshego obrazovaniya «Universitet prokuratury Rossiyskoy Federatsii», 2021. — S. 132–136.
22. Pleshakov V. A. Kriminologicheskaya bezopasnost i ee obespechenie v sfere vzaimovliyaniya organizovannoy prestupnosti i prestupnosti nesovershennoletnikh: dis. ... d-ra yurid. nauk. — M., 1998. — 323 s.
23. Romanovich A. L. Kontseptsiya bezopasnogo razvitiya sotsioprirodnykh sistem (filosofsko-metodologicheskij analiz): dis. ... d-ra filos. nauk. — M., 2004. — 418 s.
24. Russkevich E. A. Tsifrovizatsiya ugolovnogo zakonodatelstva: neprostye posledstviya prostykh resheniy // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). — 2025. — № 5 (129). — S. 26–33.
25. Savelev A. I. Kriminologicheskaya bezopasnost kak vid natsionalnoy bezopasnosti // Vestnik Omskoy yuridicheskoy akademii. — 2019. — T. 16. — № 1. — S. 49–54.
26. Sidorenko E. L. Legalizatsiya prestupnykh dokhodov s ispolzovaniem DeFi: tipovye skhemy i indikatory riska // Russian Journal of Economics and Law. — 2023. — T. 17. — № 4. — S. 832–833.
27. Khabrieva T. Ya. Pravo pered vyzovami tsifrovoy realnosti // Zhurnal rossiyskogo prava. — 2018. — № 9 (261). — S. 5–16.

28. Khisamova Z. I., Begishev I. R. Pravovoe regulirovanie iskusstvennogo intellekta // Baikal Research Journal. — 2019. — Т. 10. — № 2.
29. Shamekhina E. V. Kriptovalyuty kak predmet vzyatochnichestva: problemy regulirovaniya // Eniseyskie politiko-pravovye chteniya: sbornik nauchnykh statey po materialam XVI Vserossiyskoy nauchno-prakticheskoy konferentsii, Krasnoyarsk, 20–21 sentyabrya 2024 g. — Krasnoyarsk: Krasnoyarskoe regionalnoe otделение obshcherossiyskoy obshchestvennoy organizatsii «Assotsiatsiya yuristov Rossii», 2024. — S. 404–412.
30. Shestak V. A., Volevodz A. G., Alizade V. A. O vozmozhnosti doktrinalnogo vospriyatiya sistemoy obshchego prava iskusstvennogo intellekta kak subekta prestupleniya: na primere ugovnogo zakonodatelstva SShA // Vserossiyskiy kriminologicheskiy zhurnal. — 2019. — Т. 13. — № 4. — S. 547–554.
31. Yarochkin V. I., Buzanova Ya. V. Teoriya bezopasnosti. — M.: Akademicheskii proekt, 2005. — 173 s.