DOI: 10.37930/1990-9780-2026-1-87-153-175

А. Н. Литвиненко[1], Л. А. Гузикова[2]

ПРОБЛЕМЫ И ПРОТИВОРЕЧИЯ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРМОШЕННИЧЕСТВУ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Статья посвящена проблемам и противоречиям в сфере противодействия кибермошенничеству в условиях цифровой экономики. Обсуждаются проблемы формирования понятийного аппарата, используемого для описания и характеристики киберпреступлений, проблемы координации действий субъектов противодействия киберпреступности, проблемы оценки эффективности действий по предотвращению, выявлению и раскрытию кибермошенничества. Даны экономические оценки ущерба от кибермошенничества. Предлагаются пути решения выявленных проблем и преодоления противоречий. Обоснована целесообразность экономического подхода к борьбе с киберпреступностью и направления его применения.

Ключевые слова: цифровизация экономики, цифровая преступность, киберпреступность, кибермошенничество, противодействие кибермошенничеству, межведомственная координация.

УДК 336.7; 343.72

Развитие технологий открывает перед экономикой и обществом новые возможности для роста благосостояния, удовлетворения потребностей и раскрытия созидательного потенциала общества и отдельных лиц. Однако широкое распространение и доступность технологий сопряжены с риском, что технологические достижения могут быть поставлены на службу не только прогрессу и позитивно-созидательным целям общества, но и негативно-деструктивным для него и его составляющих криминальным целям асоциальных и антисоциальных лиц, преступных групп, враждебных организаций и структур. Цифровизация экономики не только предоставила многочисленные новые возможности для роста эффективности производства, создания новых видов товаров и услуг, повышения качества социального взаимодействия, но и породила мощную волну противоправной активности, изменившую общую картину преступности в мире и в России, в частности, и оказывающую значительное влияние на экономику и общество.

Современные информационно-коммуникационные технологии (ИКТ) базируются на цифровом представлении информации в сочетании с сетевым характером ее формирования, распространения и использования. Пропорции, в которых указанные два свой-

[1] *Литвиненко Александр Николаевич*, профессор кафедры экономической безопасности Санкт-Петербургского университета МВД (198206, Россия, Санкт-Петербург, ул. Летчика Пилютова, д. 1), д-р экон. наук, e-mail: lanfk@mail.ru

[2] *Гузикова Людмила Александровна*, профессор Высшей инженерно-экономической школы Санкт-Петербургского политехнического университета Петра Великого (195251, Россия, Санкт-Петербург, ул. Политехническая, д. 29), д-р экон. наук, e-mail: guzikova_la@spbstu.ru

ства сочетаются между собой, могут быть различными в разных сферах. В качестве примеров «предельных» ситуаций можно рассматривать автономно работающее цифровое устройство, в частности компьютер, или сетевое взаимодействие, выстраиваемое через «магические письма», распространяемые без использования цифровых устройств.

По своей природе цифровые технологии ориентированы на применение в больших масштабах: цепочка обработки данных способна эффективно работать, если при переходе от одного этапа к другому не требуется изменять форму представления информации, а сеть, связывающая субъекты, работающие с данными, имеет тем большую ценность, чем большее число участников в нее включено и, благодаря этому, потенциально достижимо. Вместе с тем достаточно очевидно, что универсальный способ физического представления данных делает их удобным объектом для криминальных действий, а сформированная сеть облегчает преступникам коммуникацию с потенциальными жертвами.

Сахабутдинова А.С. и Корчагин А.Г. пишут, что «развивая и формируя цифровое общество, цифровые технологии характеризуются существенными положительными и отрицательными изменениями, которые происходят в обществе и процессы введения которых не только формируют новые правила, но и имеют в себе достаточно большой потенциал криминологических рисков» [1].

Агентство Cybersecurity Ventures, систематически освещающее глобальную киберэкономику, включая вопросы кибербезопасности, в 2020 году опубликовало прогноз, в соответствии с которым в течение следующих пяти лет ожидался рост глобальных издержек от киберпреступлений на 15% в год, в результате чего в 2025 году они должны были составить 10,5 трлн долларов. Это представляет собой крупнейший в истории переток экономического богатства, ставит под угрозу стимулы для инноваций и инвестиций, в разы превышает ущерб, наносимый стихийными бедствиями за год, и превышает по уровню прибыли всю мировую наркоторговлю[3]. По образному выражению главного редактора журнала Cybercrime Magazine С.Моргана «Если бы киберпреступность представляла собой страну, то с размером экономики, равным 6 трлн долларов, что соответствует ущербу от киберпреступности в 2021 году, она стала бы третьей по величине экономикой мира после США и Китая»[4].

Указывая на то, что с развитием общества растет и его цифровая составляющая, а информационные сети становятся неотъемлемой частью социальной жизни, Сидорова Е.З. и Усов Е.Г. делают вывод об актуальности исследования цифровой преступности [2]. Для того, чтобы «в дальнейшем выявить и изучить криминологические особенности цифрового преступника и его жертвы с целью разработки эффективных мер противодействия таким преступлениям» [2], необходимо исследовать цифровую преступность объективно, всесторонне и целенаправленно.

В последнее десятилетие киберпреступность находится в фокусе научных исследований. Рост числа работ, зарегистрированных на портале e-library, содержащих слово «киберпреступность» в названии, ключевых словах или аннотации отражен на рис. 1. Проблемы киберпреступности рассматриваются в мультидисциплинарном поле, включающем правовые, экономические, социологические и психологические аспекты, однако

[3] Steve Morgan., 2020. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[4] Ibid.

говорить о системном понимании явления и формировании системного подхода к его изучению пока преждевременно.

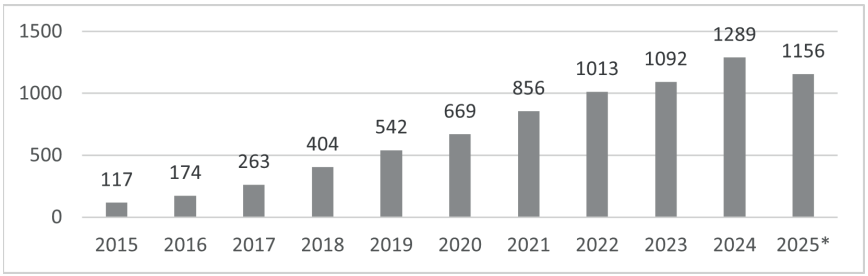

Рис. 1. Динамика числа опубликованных работ, посвященных киберпреступности

* – состояние на 10.12.2025 (*Источник*: составлено авторами по данным сайта Научной электронной библиотеки elibrary.ru[5])

Киберпреступность – это актуальная и обостряющаяся проблема во всем мире. Киберпреступления становятся все более распространенными и изощренными и имеют более серьезные экономические последствия, чем многие традиционные преступления. К наиболее массовым видам киберпреступлений относятся такие как взлом компьютерных систем, кража личных данных и различные формы финансового мошенничества. Несмотря на рост числа и негативных последствий киберпреступлений с использованием информационно-коммуникационных технологий (ИКТ), «эффективных мер и законодательства для их предотвращения или борьбы с ними крайне мало» [3].

Настоящая статья имеет целью выявление проблем и противоречий, осложняющих противодействие наиболее распространенному виду киберпреступлений, направленных на похищение денежных средств физических лиц, – кибермошенничеству – в России.

Авторами были рассмотрены и проанализированы следующие проблемы, усложняющие борьбу с киберпреступностью:

– проблемы, связанные с формированием понятийного аппарата, используемого для описания и характеристики киберпреступений, отсутствие которого затрудняет разработку классификации киберпреступлений, отражающей различия как в методах и инструментах их совершения, так и в методах и инструментах противодействия;

– проблемы, связанные с практическим отсутствием межведомственной координации в противодействии киберпреступности, в частности кибермошенничеству, жертвами которого становятся физические лица;

– проблемы, связанные с рамочными условиями, в которых действуют государственные органы и организации, и другие субъекты противодействия киберпреступности, и с пониманием населением своих интересов.

Анализ проведен на основе публикаций, посвященных противодействию киберпреступности, и количественных данных о кибермошенничестве в России.

[5] https://elibrary.ru/defaultx.asp

Основные результаты

Цифровая преступность многообразна, поэтому для исследования необходимо четко определить это явление, очертить его границы, выделить атрибутивные характеристики, на основе которых возможны типологизация и классификация его частных проявлений и ситуаций, в которых эти проявления имеют место.

В настоящее время в научном обороте используется большое число терминов, относящихся к преступлениям, совершаемым с использованием цифровых ИКТ. К числу таких терминов, наряду с термином цифровая преступность, относятся «киберпреступность», «интернет-преступность», «преступность в сфере информационно-коммуникационных технологий», «информпреступность, и т.д. В работах [4; 5], например, приводится ряд терминов, конкретизирующих технические и технологические особенности действий преступников. В статистике Министерства внутренних дел (МВД) РФ выделяется группа «Преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации» с разбиением в соответствии с отдельными видами преступлений, предусмотренных разными статьями Уголовного Кодекса (УК) РФ.

Разные авторы отдают предпочтение разным обобщающим терминам. Сахабутдинова А.С. и Корчагин А.Г. пишут, что «совокупность общественно-опасных деяний, совершенных в информационно-коммуникационной среде с использованием цифровой информации и информационных технологий» следует называть цифровой преступностью [1]. Квятковский К.С. отмечает, что «киберпреступления остаются самым широким понятием из представленных, охватывая не только преступления, связанные с использованием компьютерных технологий и сетей, но и деяния, осуществляемые другими средствами доступа к киберпространству» [6].

Ст. 2 Модельного закона о противодействии киберпреступности (далее – Модельный закон) определяет киберпреступление как «преступление, совершенное в киберпространстве»[6].

В свою очередь, термин «киберпространство» получил применение для описания среды «взаимодействия индивидов и групп посредством электронных сетей, соединенных средствами информационно-коммуникационных технологий» [7], причем киберпространство часто отождествляется с интернет-пространством как с вполне определенным видом электронной сети. Добринская Д.Е. пишет, что «киберпространство, или по-другому цифровая среда, – это пространство функционирования продуктов информационно-коммуникационных технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения информации, обмена и управления ею, а также осуществления коммуникаций в условиях множества различных сетей» [7].

По нашему мнению, следует согласиться с Сидоровой Е.З. и Усовым Е.Г., которые отождествляют понятия цифровая преступность и киберпреступность и при этом выражают мнение, что «вопрос о классификации киберпреступлений носит практикоориентированный характер, поскольку от этого зачастую зависит комплекс реализуемых превентивных мероприятий» [2]. Последнее представляется абсолютно верным в связи

[6] Модельный закон «О противодействии киберпреступности» (принят на пятьдесят пятом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (постановление № 55-20 от 14 апреля 2023 г.)) https://base.garant.ru/411235105/

с тем, что «цифровизация глобальной экономики и российского общества кардинально изменили криминальный ландшафт, масштабы, структуру и качественные характеристики преступности» [8].

Авторы [9] указывают, что многообразие киберпреступлений и вариантов их совершения, быстрая видоизменяемость и сложность используемых преступниками средств и техник затрудняют разделение киберпреступлений на отдельные категории, однако без решения этой задачи на основе выявления существенных атрибутов киберпреступлений и основных вариантов их изменения задачи выявления и противодействия киберпреступности значительно усложняются.

Ст. 2 Модельного закона содержит широкий, но не исчерпывающий перечень деяний, относимых к киберпреступлениям[7]:

1) неправомерный доступ к цифровой информации;

2) неправомерное завладение цифровой информацией;

3) неправомерное воздействие на цифровую информацию;

4) нарушение функционирования информационно-коммуникационных сетей;

5) создание, использование и распространение вредоносных программ;

6) неправомерное воздействие на критическую информационную инфраструктуру;

7) несанкционированный доступ к персональным данным с использованием ИКТ;

8) неправомерные производство, импорт, продажа или предоставление паролей, кодов доступа или иных аналогичных данных;

9) предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели;

10) неправомерное изменение идентификационного кода абонентского устройства подвижной радиотелефонной связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства;

11) хищение имущества с использованием ИКТ;

12) вымогательство с использованием ИКТ;

13) легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем, с использованием ИКТ;

14) изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием ИКТ;

15) склонение к самоубийству или доведение до его совершения с использованием ИКТ;

16) создание и использование цифровой информации для введения пользователя в заблуждение;

17) подстрекательство к подрывной или вооруженной деятельности с использованием ИКТ;

18) преступления террористической направленности с использованием ИКТ;

19) преступления экстремистской направленности с использованием ИКТ;

20) хулиганство с использованием ИКТ;

21) преступления, связанные с распространением наркотических средств и психотропных веществ, совершенные с использованием ИКТ;

[7] Ibid.

22) преступления, связанные с незаконным оборотом оружия, совершенные с использованием ИКТ;

23) реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности с использованием ИКТ;

24) нарушение авторских и смежных прав с использованием ИКТ;

25) иные преступления, совершенные в киберпространстве.

Анализ приведенного перечня подтверждает высказанное в [1] мнение, что «цифровые преступления часто имеют факультативный характер, совершаясь наряду с иными общественно-опасными деяниями. Это объясняется тем, что цифровые преступники, пользуясь цифровой информацией в качестве средства совершения преступления, «превращают» её в предмет другого преступления, например, хищение персональных данных для последующего вымогательства» [1].

С точки зрения конечной направленности Сидорова Е.З и Усов Е.Г. выделяют четыре группы цифровых преступных посягательств [2]:

1) преступные посягательства, направленные на хищение имущества граждан и организаций;

2) общественно опасные деяния в сфере компьютерной информации;

3) незаконное изготовление и распространением порнографической продукции, материалов и предметов, в том числе с несовершеннолетними, посредством сети Интернет;

4) дистанционное распространение наркотических средств, психотропных и сильнодействующих или ядовитых веществ.

Мордвинов К.В. и Удавихина У.А. указывают на такие особенности киберпреступлений, отличающие их от традиционных преступлений, как транснациональность, анонимность и мгновенное распространение информации [10]. Транснациональность подразумевает возможность нахождения места совершения преступления на значительном отдалении от места нанесения ущерба, вплоть до принадлежности этих мест к разным юрисдикциям. По нашему мнению, данную особенность более точно можно обозначить как дистанционный характер преступлений. Анонимность снижает риски киберпреступников и создает возможности для ухода от ответственности. Мгновенное распространение информации среди большого числа пользователей с минимальными затратами обусловливает особую опасность киберпреступности [11].

Следует отметить, что в перечень киберпреступлений, предусмотренных Модельным законом, включены деяния, не квалифицируемые явным образом в качестве преступлений уголовным законодательством Российской Федерации, и напротив, некоторые деяния, определяемые УК РФ как преступления, не упоминаются явно в перечне Модельного закона. К числу последних относится мошенничество, притом, что в российской практике большинство киберпреступлений, непосредственно направленных на физических лиц, квалифицируются как мошенничество.

По мнению Капинус О.С. «современная криминологическая реальность требует смены векторов уголовной политики, трансформации базовых уголовно-правовых положений и институтов, уточнения существующих уголовно-правовых запретов и криминализации новых общественно опасных деяний, т.е. полномасштабной реформы уголовного права» [8].

Денежные средства всегда были и продолжают оставаться активом, наиболее привлекательным для криминалитета в качестве объекта незаконного присвоения, способы которого могут быть различными. В настоящее время «общество сталкивается с возрастающей угрозой кибермошенничества, которое может затронуть любого человека, независимо от его личных характеристик и социального статуса» [12] – возраста, пола, образования, социального статуса, дохода, местности проживания. Авторы [13] пишут, что «кибермошенничество проникает в повседневную жизнь населения в виде различного рода атак, приводящих к возникновению финансовых потерь и хищению персональных данных» [13].

Давыдов В.О. и Тишутина И.В., рассматривая киберпреступность с криминалистической точки зрения, отмечают, что «элементами привлекательности для преступников, помимо отсутствия непосредственного контакта с потерпевшим, выступают: высокий уровень прибыли, краткосрочность контакта и неограниченное их количество, низкая активность потерпевших по взаимодействию с правоохранительными органами в силу стыда, нежелания обнаружить собственную вину, неграмотность и внушаемость» [14].

В табл. 1 приведены статистические данные о преступлениях в киберпространстве за 2024 год. По сравнению с 2023 годом снижение, иногда значительное в процентном отношении, произошло главным образом по малочисленным категориям. Видно, что по всем категориям преступлений наибольший вклад в выявление вносят органы внутренних дел. Необходимо отметить, что за 10 месяцев 2025 года МВД впервые зафиксировало снижение количества киберпреступлений: всего было предотвращено 27 млн мошеннических операций, что на 9,5% меньше, чем за аналогичный период предыдущего года[8].

Таблица 1

Статистика преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, 2024 год (Источник: [15])

Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	Зарегистрировано (в отчетном периоде)		В том числе, выявленных сотрудниками		
	Всего	+/– в %	следственных органов Следственного комитета РФ	органов внутренних дел	органов Федеральной службы безопасности
Всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	765365	13,1	2862	755094	4890
из них тяжких и особо тяжких	369267	7,8	1847	363375	3060

[8] РИА Новости. МВД предотвратило более 27 миллионов мошеннических операций в 2025 году. 8.12.2025. https://ria.ru/20251218/moshenniki-2063055665.html

Окончание таблицы 1

Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	Зарегистрировано (в отчетном периоде)		В том числе, выявленных сотрудниками		
	Всего	+/– в %	следственных органов Следственного комитета РФ	органов внутренних дел	органов Федеральной службы безопасности
в том числе совершенных с использованием или применением: расчетных (пластиковых) карт	115469	-13,1	339	114734	242
компьютерной техники	42347	16,4	225	40357	1197
программных средств	13461	10,6	82	13023	251
фиктивных электронных платежей	615	-61,8	4	536	63
сети «Интернет»	649064	23,2	2273	640897	4035
средств мобильной связи	346035	14,3	560	344070	980
в том числе кража ст. 158 УК РФ	105937	-11,1	454	105330	27
мошенничества ст. 159, 159.3, 159.6 УК РФ	380344	6,8	222	379445	278
из них мошенничества ст. 159 УК РФ	379762	7,5	213	378887	267
мошенничества с использованием электронных средств платежа ст. 159.3 УК РФ	273	-88,9	6	261	2
мошенничества в сфере компьютерной информации ст. 159.6 УК РФ	309	-25,9	3	297	9

По официальной статистике сегодня, каждое третье преступление в стране совершается в цифровой среде, причем около 80% из них составляют дистанционные хищения. По данным Банка России в 2024 году мошенники похитили с банковских счетов 27,5 млрд руб., причем основной объем денежных средств был украден со счетов физических лиц – это 26,9 млрд руб.[9]

Унукович А.С. объясняет повышенную виктимность граждан, во-первых, тем, что они имеют значительно меньше ресурсов для защиты от преступлений, совершаемых с использованием ИКТ, чем имеют в своем распоряжении киберпреступники, а во-вторых, тем, что, несмотря на заинтересованность в собственной защите от киберпреступлений, они часто не готовы «тратить денежные средства на приобретение, например, лицензионной антивирусной продукции, ограничиваясь использованием пиратской, не поддерживаемой официальным производителем» [16].

[9] ЦБ зафиксировал рекордную сумму хищений у банковских клиентов в 2024 году. https://www.rbc.ru/finances/18/02/2025/67b489749a794780d1527516

Формы дистанционного мошенничества приобретают всё большую изощрённость и масштабность (рис. 2). Ущерб, наносимый такими преступлениями (рис. 3), принимает огромные размеры, что негативно сказывается на стабильности финансовой сферы и снижает уровень доверия к финансовым институтам и оказываемым ими электронным услугам.

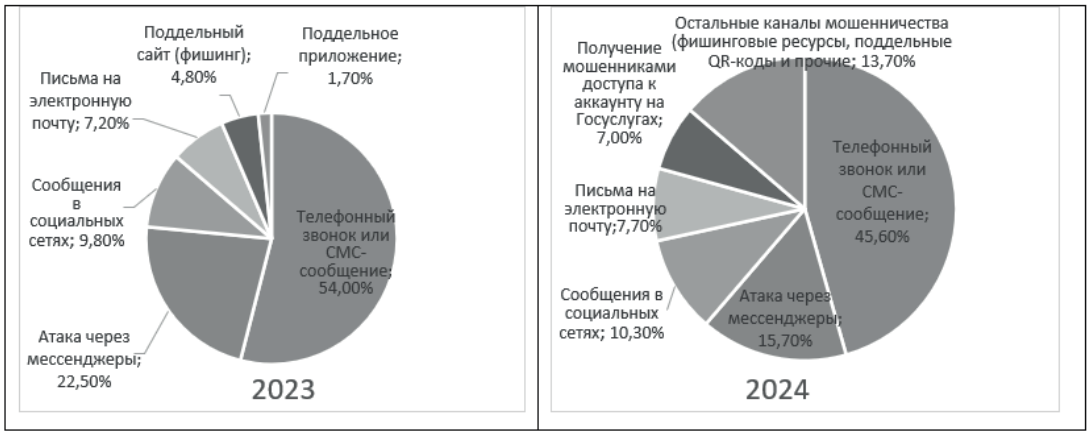

Рис. 2. Структура каналов общения кибермошенников с потенциальными жертвами

Источник: построено авторами по данным Банка России[10,11]

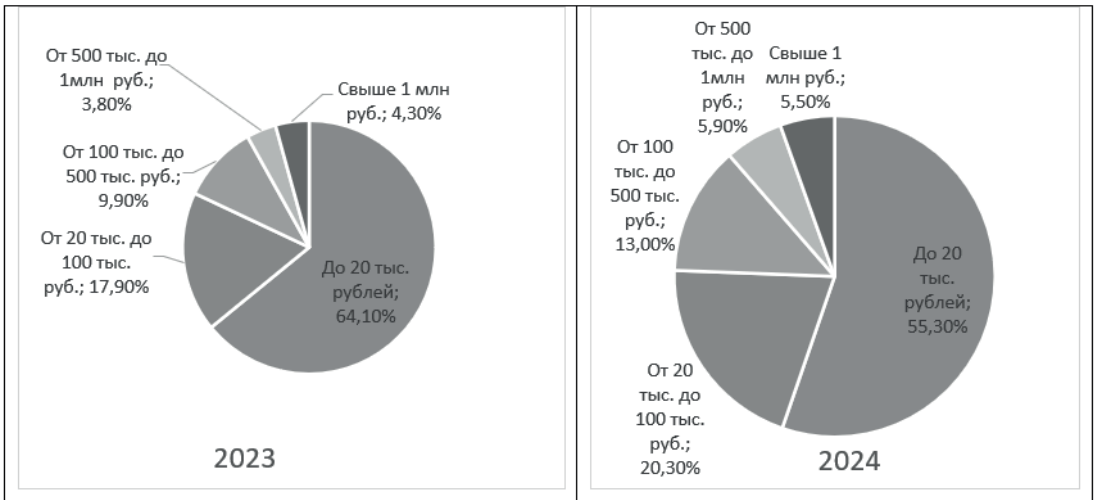

Рис. 3. Структура ущерба от кибермошенничества в отношении граждан

Источник: построено авторами по данным Банка России[12,13]

[10] Банк России, 2024. Кибермошенничество: портерт пострадавшего. https://www.cbr.ru/statistics/information_security/cyber_portrait/2023/

[11] Банк России, 2025. Кибермошенничество: портерт пострадавшего. https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/

[12] Банк России, 2024. Кибермошенничество: портерт пострадавшего. https://www.cbr.ru/statistics/information_security/cyber_portrait/2023/

[13] Банк России, 2025. Кибермошенничество: портерт пострадавшего. https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/

Шевко Н.Р. и Лукина М.А. отмечают, что «официальные статистические данные свидетельствуют о широком распространении данного вида преступности не только на территории России, но и в мире» [17] и указывают на стремительный рост материального ущерба от кибермошенничества и низкий уровень раскрываемости киберпреступлений.

В зависимости от роли – активной или пассивной, которую сам потерпевший играет в совершаемом преступлении, Братусин А.Р. и Власенко Е.Е. предлагают подразделять все виды мошенничества «на «техногенные мошенничества» – от жертвы преступления ничего не зависит; и «человекогенные мошенничества» – если человек сам предпринимает ошибочные действия, приводящие к потере его денег» [18].

Шевко Н.Р. и Лукина М.А. формулируют основную задачу борьбы с кибермошенничеством на современном этапе как «эффективное и оперативное противостояние преступности, к каким бы способам и методам не прибегали злоумышленники» [17]. Поскольку «противодействие кибермошенничеству представляет собой важное для страны и требующее постоянного к себе внимания направление работы» [19], необходим комплексный охват эффективными мерами противодействия пространства, в котором совершается кибермошенничество, для чего следует, по нашему мнению, выделить следующие компоненты киберпространства:

1) физическую – совокупность технических средств, устройств, оборудования, носителей информации и иных материальных компонентов киберпространства;

2) информационную – программы и данные, форматы представления информации, стандарты, протоколы и процедуры обработки и передачи информации;

3) социальную – взаимодействия между людьми, обусловленные их совместной деятельностью и/или общностью интересов, предусматривающие обмен информацией.

Перечисленные компоненты определяют среду противостояния киберпреступников и их жертв, а также киберпреступников и правоохранительных органов. Для успешного противодействия кибермошенничеству необходимо обеспечить преимущество по меньшей мере в одном из аспектов при паритете в остальных. Вопросы соответствия технического оснащения и программно-информационного обеспечения правоохранительных органов вызовам, исходящим от быстро прогрессирующей в этих отношениях киберпреступности, требуют специального анализа, а имеющиеся проблемы – скорейшего решения.

Согласно Глобальному индексу кибербезопасности[14] сильными сторонами России в сфере обеспечения кибербезопасности и противодействия киберпреступности являются принимаемые правовые и организационные меры, а также меры по развитию потенциала, однако технические меры и меры сотрудничества являются более слабыми и требуют дальнейшего развития.

В мировой практике известны случаи, когда заметный прогресс в борьбе с киберпреступностью достигался после перехода на сторону правоохранительных органов представителей преступных групп, например, К.Митника, который после осуждения и отбытия наказания за многочисленные компьютерные преступления стал консультантом по компьютерной безопасности одной из крупных компаний, или К.Поулсена, проделавшего аналогичный путь[15].

[14] Global Cybersecurity Index 2024. 5th Edition. https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

[15] Mitnick Security: Kevin Mitnick from the World Most Wanted to Its Most Trusted. https://www.mitnicksecurity.com/about-kevin-mitnick

В Руководстве по киберустойчивости инфраструктуры финансовых рынков Банка международных расчетов[16] представлена динамическая модель обеспечения киберустойчивости, предложенная Банком международных расчетов (Bank of International Settlements, BIS). Внутренний контур модели предполагает циклическое выполнение действий (рис. 4), а внешний контур задает постоянно выполняющиеся процессы – тестирование, повышение ситуационной осведомленности, обучение и развитие.

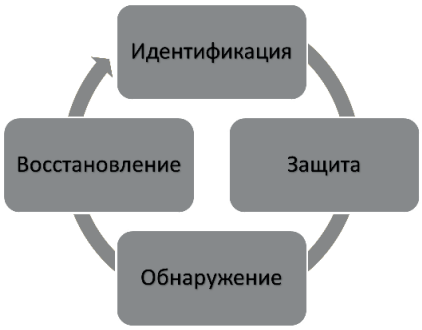

Рис. 4. Внутренний контур модели повышения киберустойчивости

Источник: построено авторами на основе Руководства по киберустойчивости инфраструктуры финансовых рынков Банка международных расчетов[17]

Во внутреннем контуре выполняются:

– идентификация рисков и угроз, причем не только как быстрое обнаружение новых схем и приемов мошенников, но и проактивное предвидение будущих рисков и угроз, базирующееся на выявлении потенциальных уязвимостей;

– защита, т.е. устранение уязвимостей, которые уже были обнаружены киберпреступниками и выявленных в проактивном режиме идентификации;

– обнаружение фактов совершения преступлений;

– восстановление, ограничение масштаба ущерба и/или его компенсация.

Имеется ряд системных факторов, усложняющих противодействие государственных органов киберпреступности в целом и кибермошенничеству в частности (табл. 2).

Таблица 2

Факторы, усложняющие борьбу с киберпреступностью

1. Гибкость vs бюрократия	
Мошенники действуют как стартапы:	Государство реагирует медленно:
Быстро тестируют новые схемы, адаптируются к изменениям, используют agile-подход.	Принятие законов требует времени (обсуждения, чтения, согласования).
Не связаны законами, процедурами и бюджетными ограничениями	Внедрение новых защитных механизмов (например, в банковской сфере) часто отстаёт на месяцы или годы.

[16] Bank for International Settlements, OICU-IOSCO. Committee on Payments and Market Infrastructures. Board of the International Organization of Securities Commissions. Guidance on cyber resilience for financial market infrastructures, 2016. https://www.iosco.org/library/pubdocs/pdf/ioscopd535.pdf

[17] Ibid.

Окончание таблицы 2

2. Технологическое превосходство мошенников	
Мошенники первыми осваивают новые технологии:	Государственные системы защиты устаревают до внедрения:
Используют ИИ для генерации фейковых звонков (deepfake), автоматизируют фишинг через ботов.	Пока разрабатывается новый стандарт безопасности, мошенники уже нашли способ его обойти
Эксплуатируют уязвимости быстрее, чем их успевают закрыть (например, уязвимость нулевого дня).	
3. Глобальность vs национальные ограничения	
Мошенники работают трансгранично:	Государство ограничено юрисдикцией:
Используют зарубежные сервера, VPN, криптовалюты для отмывания денег.	Законы РФ не действуют за границей, а международное сотрудничество (например, экстрадиция) часто затруднено.
Даже если РФ блокирует один канал (например, определённый мессенджер), они мгновенно переключаются на другой.	
4. Человеческий фактор – слабое звено	
Мошенники играют на психологии, а не взламывают код:	Государство не успевает обучать население:
Социальная инженерия (например, звонок «из банка») эффективнее техничных хакерских атак.	Даже если появляются образовательные программы, многие пользователи остаются все равно беспечными, думая о том, что их это не коснется.
Люди по-прежнему доверяют, кликают на ссылки и верят в «бесплатные подарки».	

Источник: [21].

На наш взгляд, к числу факторов первой группы следует добавить дефицит скоординированного взаимодействия между субъектами предупреждения киберпреступности, в частности межведомственного взаимодействия между государственными правоохранительными органами.

В зависимости от предназначения и целей деятельности субъектов предупреждения киберпреступности Сидорова Е.З. и Усов Е.Г. разделяют их на специализированные и неспециализированные, относя к специализированным правоохранительные и силовые ведомства Российской Федерации, включая Федеральную службу безопасности, Службу внешней разведки, Министерство обороны, Росгвардию, МВД, Федеральную службу охраны, а к неспециализированным – государственные и общественные органы, организации, объединения и общественные институты, вносящие вклад в деятельность по предупреждению киберпреступности, хотя это не является для них основным видом деятельности и целью их создания [5]. К субъектам второго рода в [5] отнесены органы государственной власти и местного самоуправления, образовательные организации, институт семьи, средства массовой информации, отдельные граждане и в целом общество.

По нашему мнению, к неспециализированным субъектам, заинтересованным в противодействии кибермошенничеству в отношении граждан, следует относить финансовые институты, включая Банк России и все субъекты экономической деятельности, так как в случае, когда их клиенты и/или сотрудники становятся объектами атак кибермошенников, их деятельности угрожают дезорганизация, прямые или косвенные финансовые потери и репутационный ущерб.

В числе неспециализизированных субъектов следует выделить Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор, РКН) как государственный орган, отвечающий за физический уровень взаимодействия, и операторов связи.

Описанная выше модель повышения киберустойчивости должна работать в циклическом режиме на всех уровнях системы кибербезопасности – индивидуальном, уровне предприятий и организаций, уровне финансовых институтов, уровне государства, – и у всех без исключения субъектов предупреждения киберпреступности. Однако для того, чтобы данная модель работала эффективно, она должна получать «информационную подпитку» за счет обмена информацией как в пределах каждого уровня, так и между смежными уровнями.

Сегодня эффективность мер по противодействию дистанционному мошенничеству существенно ограничивается отсутствием единой системы координации между ключевыми субъектами, такими как финансовые организации, правоохранительные органы и регуляторные институты. Фрагментированность взаимодействия приводит к задержкам в обмене оперативной информацией, что создает условия для модификации мошеннических схем и ухода преступников от ответственности. Оптимизация данного аспекта требует разработки централизованной платформы, обеспечивающей оперативный мониторинг, анализ и обмен данными между всеми заинтересованными сторонами.

Рассматривая межведомственное взаимодействие в борьбе с киберпреступностью с позиций оперативно-розыскной деятельности, Яровиков А.С. приходит к выводу, что «нужны определенные изменения как правовой основы, так и организации взаимодействия между правоохранительными органами» [22] и полагает, что «информационное взаимодействие различных правоохранительных органов объективно необходимо для успешной и эффективной реализации стоящих перед ними задач и полностью отвечает Стратегии информационного развития государства» [22].

Несмотря на то, что потенциальные жертвы кибермошенничества заинтересованы в обеспечении безопасности своих денежных средств, их права и удобства вступают в противоречия с мерами, которые предлагаются и предпринимаются для защиты их интересов финансовыми институтами, регулирующими и правоохранительными органами. Имеются также противоречия между предусмотренными законодательством и нормативно-правовыми актами требованиями и процедурами и необходимостью оперативного выявления мошеннических действия и скорейшего раскрытия преступлений. К числу указанных противоречий можно отнести следующие:

1) Противоречие между безопасностью и удобством (табл. 3).

Хисамова З.И. и Бегишев И.Р. отмечают, что «правильное поведение человека в цифровом пространстве (равно как и в реальном) способствует предотвращению распространения различных угроз в виртуальном мире (как и в физической среде)» [23]

и считают, что соблюдение информационной безопасности должно обеспечиваться на основе повышения киберграмотности и поддержания на должном уровне цифровой гигиены [23].

На практике же соображения цифровой гигиены достаточно часто уступают стремлению упростить процедуры доступа к данным вплоть до полной отмены дополнительных уровней защиты ради комфортного использования сервисов и приложений. Такое поведение облегчает мошенникам доступ к данным и повышает риски мошеннических действий с реальным причинением ущерба.

Таблица 3

Баланс между безопасностью и удобством пользователей

Аспект	Усиление безопасности	Повышение удобства
Методы	Многоэтапная проверка, биометрия, CAPTCHA	Минимальные проверки, упрощённый вход
Преимущества	Защита от мошенничества, повышение надёжности	Быстрый и простой доступ, комфорт клиента
Недостатки	Сложность, возможное отторжение со стороны пользователей	Увеличение уязвимости, отключение защитных механизмов
Итог	Снижение числа мошеннических случаев	Повышение рисков инцидентов и репутационных потерь

Источник: составлено авторами.

2) Противоречие между защитой персональных данных и необходимостью анализа для выявления мошенничества (табл. 4).

Таблица 4

Конфликт между защитой данных и необходимостью их анализа для борьбы с мошенничеством

Параметр	Анализ данных для безопасности	Требования к защите данных
Цель	Обнаружение мошенничества, снижение финансовых потерь	Сохранение конфиденциальности, соблюдение законодательства
Инструменты	Большие данные, алгоритмы машинного обучения	Шифрование, анонимизация, ограничение доступа
Ограничения	Регуляторные требования, ограничения по объёму данных	Запрет на избыточный сбор, согласие клиента
Итог	Более эффективный мониторинг и реагирование	Минимизация рисков нарушения прав и штрафов

Источник: составлено авторами

Для выявления и предотвращения мошеннических схем финансовые организации и регулирующие органы нуждаются в глубоком анализе больших массивов информации

о клиентах и операциях. Современные методы, такие как машинное обучение и аналитика поведения, требуют обработки значительного объёма персональных данных. Однако законодательство в области защиты данных – например, Общий регламент по защите данных (General Data Protection Regulation, GDPR) – строго ограничивает сбор, хранение и использование информации, защищая права клиентов на конфиденциальность. Это создаёт серьёзное противоречие: эффективность превентивных мер по борьбе с мошенничеством зависит от доступности данных, но их использование ограничено для сохранения приватности. Решение данного конфликта возможно через внедрение технологий анонимизации, минимизации собираемых данных и прозрачных процедур обработки. Отмечается важность внедрения современных технологий, протоколов и процедур всеми субъектами противодействия кибермошенничеству, включая операторов связи, обеспечивающих физический уровень передачи данных [24].

3) Противоречие между необходимостью оперативной блокировки мошеннических операций и соблюдением правовых норм (табл. 5).

Таблица 5

Противоречие между скоростью блокировки мошенников и соблюдением законности

Критерий	Быстрая блокировка	Соблюдение правовых процедур
Цель	Быстрое предотвращение ущерба	Законное доказательство и преследование
Метод	Автоматические системы мониторинга и блокировки	Тщательное расследование, сбор доказательств
Риски	Ложные срабатывания, ухудшение клиентского опыта	Задержки в реагировании, возможные потери
Итог	Снижение финансовых рисков с вероятностью ошибок	Законность действий с риском упущений

Источник: составлено авторами.

Для минимизации ущерба от дистанционных мошеннических действий важна максимально быстрая блокировка подозрительных транзакций. Это позволяет значительно снизить финансовые потери, однако ускоренные меры нередко приводят к ошибочным блокировкам, что вызывает недовольство клиентов и увеличивает количество жалоб. При этом правовые процедуры требуют аккуратного сбора доказательств, времени на расследование и соблюдения регламентов, что затягивает процесс преследования преступников. В то же время мошенники действуют мгновенно, что создаёт острую дилемму: как совместить необходимость быстрого реагирования и законность действий. Решение лежит в комплексном использовании автоматизированных систем с последующим экспертным анализом и контролем. Как указывают Давыдов В.О. и Тишутина И.В., «эффективность выявления, раскрытия и расследования дистанционного мошенничества во многом зависит от возможностей правоохранительных органов по грамотному обнаружению, изъятию, исследованию цифровых следов» [25].

К числу факторов, осложняющих решение проблемы кибермошенничества, и подтверждающих актуальность обеспечения межведомственного взаимодействия, можно отнести и существенное расхождение данных о масштабах киберпреступности. В табл. 6 приведены данные МВД и Банка России относительно объема средств, похищенных мошенниками у населения. Для характеристики расхождения в данных были рассчитаны индексы несоответствия, как отношения значений показателей, сообщаемых МВД к показателям, публикуемым Банком России. Можно заметить, что данные МВД об объемах похищенных у населения средств систематически кратно превышают данные Банка России, что может косвенно характеризовать объем средств населения, хранимых вне банковской системы. Показатели темпов прироста объемов похищенных средств также существенно различаются, а потому не позволяют создать единую картину динамики явления. Кузина С.И., Пухкалова М.О. и Цыкора А.В. считают, что латентны преступления с наименьшим ущербом, но вместе с тем полагают, что «если мы посчитаем комплексный ущерб от мошенничеств небольшой тяжести в сумме, то официальная статистика увеличится еще в несколько раз» [15].

Таблица 6

Расхождение в оценках объема средств, похищенных у граждан

Показатель	Год				
	2020	2021	2022	2023	2024
Объем похищенных средств по данным МВД, млрд руб.	90	100	120	160	200
Темп прироста, %		11,11	20,00	33,33	25,00
Объем похищенных средств по данным Банка России, млрд руб.	9,8	13,6	14,2	15,8	27,5
Темп прироста, %		38,78	4,41	11,27	74,05
Индекс несоответствия объемов	9,18	7,35	8,45	10,13	7,27
Индекс несоответствия темпов прироста		0,29	4,53	2,96	0,34

Источник: рассчитано авторами по данным Сбера[18]

Условная оценка средневзвешенного объема «удачной» мошеннической операции может служить характеристикой «эффективности» мошеннических действий. Приведенные в табл. 7 значения этого показателя были рассчитаны следующим образом: для оценки средней величины ущерба в первых четырех диапазонах взято среднее граничных значений, а для последнего диапазона в качестве средней величины ущерба принято значение 2 млн руб., далее с использованием долей, приходящихся на каждую группу ущерба в общем числе преступлений, было рассчитано средневзвешенное значение. Можно заметить, что при принятых допущениях средневзвешенная условная сумма ущерба выросла в 2024 году по сравнению с предшествующим годом более чем на 25%, что отражает смещение структуры ущерба в сторону больших значений.

[18] Сбер: Анализ системы вывода денежных средств, похищенных у граждан. https://www.sberbank.ru/ru/person/kibrary/investigations/analiz-sistemy_vyvoda_denezhnyh_sredstv

Таблица 7

Показатель «эффективности» мошеннических действий

Диапазон ущерба	Доля в общем числе преступлений, %		Условная величина ущерба, руб.	Условная оценка ущерба, руб.	
	2023	2024		2023	2024
До 20 тыс. рублей	64,10	55,30	10000	6410	5530
От 20 тыс. до 100 тыс. руб.	17,90	20,30	60000	10740	12180
От 100 тыс. до 500 тыс. руб.	9,90	13,00	300000	29700	39000
От 500 тыс. до 1 млн руб.	3,80	5,90	750000	28500	44250
Свыше 1 млн руб.	4,30	5,50	2000000	86000	110000
Средневзвешенная условная оценка ущерба, руб.				161350	210960

Источник: рассчитано авторами по данным Банка России[19,20]

Азбиева У.Р., Мамаева А.А., Кувшинова Ю.А. считают, что «полностью искоренить кибермошенничество невозможно», и прогнозируют, что «оно будет эволюционировать вместе с технологиями» [21], однако они полагают, что масштабы кибермошенничества можно снизить. Снизить степень экономической и социальной опасности кибермошенничества можно за счет тотального характера противодействия, поддержания на современном уровне технико-технологического и кадрового обеспечения ключевых субъектов противодействия и проактивных действий в рамках модели повышения киберустойчивости.

Выводы

Проведенный анализ позволил сделать ряд выводов.

Динамика киберпреступности как она отражается в количестве фиксируемых преступлений и ущербе от них показывает, что в настоящее время в технологическом соревновании государство и общество оказываются в роль догоняющего как в аппаратно-программной сфере, так и в накоплении опыта социально-психологических манипуляций.

Использование цифровых ИКТ при совершенствовании преступлений имущественной направленности имеет под собой как экономические, так и социальные основы, которые недостаточно освещены в теории, но имеют неоспоримое практическое значение, а потому требуют изучения с учетом развития технико-технологических возможностей киберпространства, геополитической динамики, социальных трендов и государственной политики.

[19] Банк России, 2024. Кибермошенничество: портрет пострадавшего. https://www.cbr.ru/statistics/information_security/cyber_portrait/2023/

[20] Банк России, 2025. Кибермошенничество: портрет пострадавшего. https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/

Выявление существенных атрибутов киберпреступлений и основанная на его результатах классификация позволят создать систему сбора информации о киберпреступлениях и применять при их предотвращении, выявлении и расследовании статистические методы, технологии больших данных и искусственного интеллекта.

В условиях рыночной экономики физические лица владеют большей частью располагаемого капитала, в том числе в денежной форме, и должны становиться его поставщиками в экономику через инвестиционные механизмы. Покушения кибермошенников на денежные средства населения подрывают экономическую стабильность и выводят эти средства в нелегальный оборот, в частности могут переводить их во враждебные зарубежные структуры, что в конечном счете разрушает экономическую безопасность страны.

Физические лица становятся объектом манипулирования со стороны кибермошенников, а потому снижение уязвимости граждан к кибермошенничеству за счет повышения цифровой грамотности является важнейшей задачей. С социальной точки зрения следует принимать во внимание, что меры, принимаемые финансовыми организациями и правоохранительными органами, направленные на защиту имущественных интересов граждан, не должны восприниматься как ограничение их прав и свобод, для чего необходима масштабная разъяснительная работа.

Меры, принимаемые для выявления и профилактики киберпреступности, должны быть направлены на организацию системного противодействия киберпреступности и иметь комплексный характер. Такие меры должны всесторонне оцениваться с экономических позиций, что подразумевает, с одной стороны, обеспечение эффективность затрат на борьбу с киберпреступностью в сопоставлении с ее результатами, а с другой стороны – создание условий, при которых киберпреступления станут экономически невыгодны преступникам.

Существует ряд противоречий между интересами и возможностями специализированных субъектов противодействия киберпреступности, осуществляющих борьбу с киберпреступностью как основной вид деятельности, и неспециализированных субъектов, которые, будучи заинтересованными в устранении киберпреступности, не готовы предпринимать для этого серьезные меры, совершать затраты, отказываться от удобств и привычных подходов.

Среди факторов, ограничивающих возможности государственных органов в борьбе с киберпреступностью, имеются такие, которые представляются трудноустранимыми, в частности низкая скорость законодательного реагирования и проблемы взаимодействия между юрисдикциями. Развитие технических возможностей противодействия киберпреступности должно иметь проактивную направленность.

В рамках противодействия кибермошенничеству необходимо наладить как межведомственное взаимодействие между специализированными субъектами противодействия киберпреступности, так и взаимодействие между этими субъектами и ключевыми неспециализированными субъектами, прежде всего Банком России, коммерческими банками, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, операторами связи, которые, действуя в рамках своих полномочий должны принимать меры по предотвращению актов кибермошенничества и минимизации ущерба в ситуациях, когда предотвратить киберпреступления не удалось.

Направления дальнейших исследований

Данная статья является первой в цикле работ, задуманных авторами с целью раскрытия проблем и противоречий киберпреступности с позиций ее влияния на экономику и социальную среду.

В дальнейшем предполагается исследовать социально-экономические предпосылки киберпреступности, экономическую мотивацию киберпреступности и меры по устранению экономических стимулов преступной деятельности в киберпространстве, территориальный аспект киберпреступности в увязке с региональными социально-экономическими показателями.

Список литературы

1. *Сахабутдинова, А.С.* Цифровая преступность: причины, виды, тенденции преступности, личность преступника, меры противодействия / А.С. Сахабутдинова, А.Г. Корчагин // Аграрное и земельное право. – 2023. – № 8(224). – С. 25-28.

2. *Сидорова, Е.З.* Цифровая преступность: понятие, криминологическая характеристика, предупреждение (часть 1) / Е.З. Сидорова, Е.Г. Усов // Сибирский юридический вестник. – 2024. – № 2 (105). – С. 89-93.

3. *Lee, S.-H.* Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? / S.-H. Lee, I. Kang, H.-W. Kim //Technology in Society. – 2023. – Volume 75. ¬ 102361.

4. *Ищук, Я.Г.* Цифровая криминология: учеб. пособие. / Я.Г. Ищук, Т.В. Пинкевич, Е.С. Смольянинов – М.: Акад. управления МВД РФ. – 2021. – 244 с

5. *Сидорова, Е.З.* Цифровая преступность: понятие, криминологическая характеристика, предупреждение (часть 2) / Е.З. Сидорова, Е.Г. Усов // Сибирский юридический вестник. – 2024. – № 3 (106). – С. 81-87.

6. *Квятковский, К.С.* Преступления в сфере компьютерной информации, компьютерные преступления и киберпреступность: соотношение понятий / К.С. Квятковский // Молодой ученый. – 2022. – № 42. – С. 108–112.

7. *Добринская, Д.Е.* Киберпространство: территория современной жизни / Д.Е. Добринская // Вестник Московского университета. Серия 18. Социология и политология. – 2018. – Т. 24. № 1. – С. 52-70.

8. *Капинус, О.С.* Цифровизация преступности и уголовное право // Baikal Research Journal. – 2022. – Т. 13, № 1.

9. *Гурьянова, В.Р.* Противодействие преступлениям, совершаемым с использованием современных информационно-телекоммуникационных технологий: отдельные аспекты. Учебное пособие / В.Р. Гурьянова, Г.А. Тугузбаев, А.С. Ишмеева, М.А. Рахматуллин, И.Р. Диваева, Р.И. Пейзак, Р.Р. Абдразяпов, Э.Д. Нугаева, З.И. Харисова, С.Р. Низаева, А.Р. Лонщакова – Уфа. – 2023. – 48 с.

10. *Мордвинов, К.В.* Киберпреступность в современной России: актуальные вызовы и успешные практики борьбы с киберпреступностью / К.В. Мордвинов, У.А. Удавихина //Теоретическая и прикладная юриспруденция. – 2022. – №1(11). – С. 83-88.

11. *Соломонова, В.В.* Киберпреступность в современной России: масштабы и последствия / В.В. Соломонова // Территория науки. – 2025. – № 4. – С. 49-52.

12. *Самойличенко, Е.Е.* Социальный портрет жертвы мошенничества, совершенного с использованием информационно-коммуникационных технологий, в современной России /

Е.Е. Самойличенко, М.О. Дятлева, Е.А. Цыкина // Society and Security Insights. – 2024. – Т. 7. № 4. – С. 157-171.

13. *Крутова, Н.А*. Защита от кибермошенничества и возможности обеспечения национальной безопасности современной России / Н.А. Крутова, А.Н. Крутов, Ю.И. Минина, Д.А. Крутова //Вестник Самарского муниципального института управления. – 2025. – № 1. – С. 7-16.

14. *Давыдов, В.О*. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий / В.О. Давыдов, И.В. Тишутина //Криминалистика: вчера, сегодня, завтра. – 2020. – № 2(14). – С. 81-91.

15. *Кузина, С.И*. Мошенничество в цифровом пространстве и его особенности / С.И. Кузина, М.О. Пухкалова, А.В. Цыкора // Северо-Кавказский юридический вестник. – 2025. – № 2. – С. 112-124.

16. *Унукович, А.С*. Меры предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий в отношении граждан / А.С. Унукович // Научный вестник Омской академии МВД России. – 2023. – Т. 29. № 2(89). – С. 98-102.

17. *Шевко, Н.Р*. Кибермошенничество: новые методы, старые цели / Н.Р. Шевко, М.А. Лукина // Виктимология. – 2025. – Т. 12. № 2. – С. 250-259.

18. *Братусин, А.Р.* О проблемах, характерных индивидуально-типологических особенностях и поведенческих паттернах личности типичных жертв финансового мошенничества / А.Р. Братусин, Е. Е. Власенко // Проблемы современного педагогического образования. – 2019. – № 64/4. – С. 292-295.

19. *Алексеева, А.П*. Современные способы совершения кибермошенничеств и основные пути противодействия им / А.П. Алексеева, О.И. Белокобыльская //Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2025. – № 1(79). – С. 78-84.

20. *Косарев, А.С*. Проблемные вопросы раскрытия мошеннических действий, совершенных с использованием информационных телекоммуникационных технологий / А.С. Косарев, М.А. Саенко // Проблемы правоохранительной деятельности. – 2022. – № 3. – С. 42-46.

21. *Азбиева, У.Р.* Цифровая грамотность и кибермошенничество: новые вызовы для российской экономики знаний / У.Р. Азбиева, А.А. Мамаева, Ю.А. Кувшинова //Вестник Национального Института Бизнеса. – 2025. – № 2 (58). – С. 341-350.

22. *Яровиков, А.С*. Проблемы ведомственного взаимодействия правоохранительных органов в сфере информационного поиска при осуществлении оперативно-розыскной деятельности / А.С. Яровиков // Вестник Алтайской академии экономики и права. – 2021. – № 1-2. – С. 210-215.

23. *Хисамова, З.И*. Цифровая преступность в условиях пандемии: основные тренды / З.И. Хисамова, И.Р. Бегишев // Всероссийский криминологический журнал. – 2022. – Т. 16, № 2. – С. 185-198.

24. *Зароденков, Н.С*. Особенности цифрового мошенничества в России / Н.С. Зароденков // В сборнике: 19. Konferenz Wissenschaft und Bildung: in- und ausländische Erfahrung. Conference Proceedings. Gelsenkirchen. – 2025. – С. 73-78.

25. *Давыдов, В.О.* Цифровые следы в расследовании дистанционного мошенничества / В.О. Давыдов, И.В. Тишутина // Известия Тульского государственного университета. Экономические и юридические науки. – 2020. – № 3. – С. 20-27.

References

1. Sakhabutdinova A. S., Korchagin A. G. (2023) Tsifrovaya prestupnost': prichiny, vidy, tendentsii prestupnosti, lichnost' prestupnika, mery protivodeystviya [Digital Crime: Causes, Types, Crime Trends, Criminal's Identity, Countermeasures]. Agrarian and Land Law, 8 (224), pp. 25-28.

2. Sidorova E. Z., Usov E. G. (2024) Tsifrovaya prestupnost': ponyatiye, kriminologicheskaya kharakteristika, preduprezhdeniye (chast' 1) [Digital Crime: Concept, Criminological Characteristics, Prevention (Part 1)]. Siberian Legal Bulletin, 2 (105), pp. 89-93.

3. Lee S.-H., Kang I., Kim H.-W. (2023) Understanding Cybercrime from a Criminal's Perspective: Why and How Do Suspects Commit Cybercrimes? Technology in Society, 75, 102361.

4. Ishchuk Y. G., Pinkevich T. V., Smolyaninov E. S. (2021) Tsifrovaya kriminologiya: uchebnoye posobiye [Digital Criminology: Study Guide]. Moscow: Academy of Management of the Ministry of Internal Affairs of the Russian Federation. 244 p.

5. Sidorova E. Z., Usov E. G. (2024) Tsifrovaya prestupnost': ponyatiye, kriminologicheskaya kharakteristika, preduprezhdeniye (chast' 2) [Digital Crime: Concept, Criminological Characteristics, Prevention (Part 2)]. Siberian Law Bulletin, 3 (106), pp. 81-87.

6. Kvyatkovsky K. S. (2022) Prestupleniya v sfere komp'yuternoy informatsii, komp'yuternyye prestupleniya i kiberprestupnost': sootnosheniye ponyatiy [Crimes in the Field of Computer Information, Computer Crimes, and Cybercrime: Relationship Between Concepts]. Young Scientist, 42, pp. 108-112.

7. Dobrinskaya D. E. (2018) Kiberprostranstvo: territoriya sovremennoy zhizni [Cyberspace: Territory of Modern Life]. Bulletin of Moscow University. Series 18. Sociology and Political Science, (1) 24, pp. 52-70.

8. Kapinus O. S. (2022) Tsifrovizatsiya prestupnosti i ugolovnoye pravo [Digitalization of Crime and Criminal Law]. Baikal Research Journal, (1) 13.

9. Guryanova V. R., Tuguzbaev G. A., Ishmeeva A. S., Rakhmatullin M. A., Divaeva I. R., Peyzak R. I., Abdrazyapov R. R., Nugaeva E. D., Kharisova Z. I., Nizaeva S. R., Lonshchakova A. R. (2023) Protivodeystviye prestupleniyam, sovershayemym s ispol'zovaniyem sovremennykh informatsionno-telekommunikatsionnykh tekhnologiy: otdel'nyye aspekty. Uchebnoye posobiye [Counteracting Crimes Committed with the Use of Modern Information and Telecommunication Technologies: Certain Aspects. Study Guide]. Ufa. 48 p.

10. Mordvinov K. V., Udavikhina U. A. (2022) Kiberprestupnost' v sovremennoy Rossii: aktual'nyye vyzovy i uspeshnyye praktiki bor'by s kiberprestupnost'yu [Cybercrime in Modern Russia: Current Challenges and Successful Practices in the Fight Against Cybercrime]. Theoretical and Applied Jurisprudence, 1 (11), pp. 83-88.

11. Solomonova V. V. (2025) Kiberprestupnost' v sovremennoy Rossii: masshtaby i posledstviya [Cybercrime in Modern Russia: Scale and Consequences]. Territory of Science, 4, pp. 49-52.

12. Samoilichenko E. E., Dyatleva M. O., Tsykina E. A. (2024) Sotsial'nyy portret zhertvy moshennichestva, sovershennogo s ispol'zovaniyem informatsionno-kommunikatsionnykh tekhnologiy, v sovremennoy Rossii [Social Portrait of a Victim of Fraud Committed Using Information and Communication Technologies in Modern Russia] Society and Security Insights, 4 (7), pp. 157-171.

13. Krutova N. A., Krutov A. N., Minina Y. I., Krutova D. A. (2025) Zashchita ot kibermoshennichestva i vozmozhnosti obespecheniya natsional'noy bezopasnosti sovremennoy Rossii [Protection Against Cyber Fraud and the Possibility of Ensuring National Security of Modern Russia]. Bulletin of the Samara Municipal Institute of Management, 1, pp. 7-16.

14. Davydov V. O., Tishutina I. V. (2020) Ob aktual'nykh problemakh kriminalisticheskogo obespecheniya raskrytiya i rassledovaniya moshennichestv, sovershennykh s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy [On Current Issues of Forensic Support for the

Detection and Investigation of Fraud Committed Using Information and Telecommunication Technologies]. Forensic Science: Yesterday, Today, Tomorrow, 2 (14), pp. 81-91.

15. Kuzina S. I., Pukhkalova M. O., Tsykora A. V. (2025) Moshennichestvo v tsifrovom prostranstve i yego osobennosti [Fraud in the Digital Space and Its Features]. North Caucasian Legal Bulletin, 2, pp. 112-124.

16. Unukovich A. S. (2023) Mery preduprezhdeniya prestupleniy, sovershayemykh s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy v otnoshenii grazhdan [Measures to Prevent Crimes Committed with the Use of Information and Telecommunication Technologies against Citizens]. Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia, 29, 2 (89), pp. 98-102.

17. Shevko N. R., Lukina M. A. (2025) Kibermoshennichestvo: novyye metody, staryye tseli [Cyberfraud: New Methods, Same Goals]. Victimology, 2 (12), pp. 250-259.

18. Bratusin A. R., Vlasenko E. E. (2019) O problemakh, kharakternykh individual'no-tipologicheskikh osobennostyakh i povedencheskikh patternakh lichnosti tipichnykh zhertv finansovogo moshennichestva [On the Problems, Characteristic Individual-Typological Features and Behavioral Patterns of the Personality of Typical Victims of Financial Fraud]. Problems of Modern Pedagogical Education, 64/4, pp. 292-295.

19. Alekseeva A. P., Belokobylskaya O. I. (2025) Sovremennyye sposoby sovershenia kibermoshennichestv i osnovnyye puti protivodeystviya im [Modern Methods of Committing Cyberfraud and the Main Ways to Counteract Them]. Bulletin of the Kaliningrad Branch of the St. Petersburg University of the Ministry of Internal Affairs of Russia, 1 (79), pp. 78-84.

20. Kosarev A. S., Saenko M. A. (2022) Problemnyye voprosy raskrytiya moshennicheskikh deystviy, sovershennykh s ispol'zovaniyem informatsionnykh telekommunikatsionnykh tekhnologiy [Problematic issues of detecting fraudulent actions committed using information telecommunication technologies]. Problems of Law Enforcement Activity, 3, pp. 42-46.

21. Azbieva U. R., Mamaeva A. A., Kuvshinova Y. A. (2025) Tsifrovaya gramotnost' i kibermoshennichestvo: novyye vyzovy dlya rossiyskoy ekonomiki znaniy [Digital Literacy and Cyber Fraud: New Challenges for the Russian Knowledge Economy]. Bulletin of the National Institute of Business, 2 (58), pp. 341-350.

22. Yarovikov A. S. (2021) Problemy vedomstvennogo vzaimodeystviya pravookhranitel'nykh organov v sfere informatsionnogo poiska pri osushchestvlenii operativno-rozysknoy deyatel'nosti [Problems of Departmental Interaction of Law Enforcement Agencies in the Field of Information Search During Operational-Search Activities]. Bulletin of the Altai Academy of Economics and Law, 1-2, pp. 210-215.

23. Khisamova Z. I., Begishev I. R. (2022) Tsifrovaya prestupnost' v usloviyakh pandemii: osnovnyye trendy [Digital Crime in a Pandemic: Main Trends]. All-Russian Criminological Journal, 2 (16), pp. 185-198.

24. Zarodenkov N. S. (2025) Osobennosti tsifrovogo moshennichestva v Rossii [Features of Digital Fraud in Russia]. In the collection: 19. Konferenz Wissenschaft und Bildung: In- und Ausländische Erfahrung. Conference Proceedings. Gelsenkirchen, pp. 73-78.

25. Davydov V. O., Tishutina I. V. (2020) Tsifrovyye sledy v rassledovanii distantsionnogo moshennichestva [Digital Traces in the Investigation of Remote Fraud]. Bulletin of Tula State University. Economic and Legal Sciences, 3, pp. 20-27.

A. N. Litvinenko[21], L. A. Guzikova[22]. Problems and Contradictions of the System for Countering Cyber Fraud in the Context of Economy Digitalization. The article examines the challenges and contradictions in combating cyber fraud in the digital economy. It discusses the development of a conceptual framework for describing and characterizing cybercrime, the challenges of coordinating the actions of cybercrime countermeasures, and assessing the effectiveness of efforts to prevent, detect, and uncover cyber fraud. Economic estimates of the damage caused by cyber fraud are provided. Solutions to respond challenges and to overcome contradictions are proposed. The feasibility of an economic approach to combating cybercrime and its possible applications are substantiated.

Keywords: digitalization of the economy, digital crime, cybercrime, cyber fraud, counteracting cyber fraud, interdepartmental coordination

[21] *Aleksandr N. Litvinenko,* Professor, Department of Economic Security, St. Petersburg University of the Ministry of Internal Affairs (1 Letchika Pilyutova ul., St. Petersburg, 198206, Russia), Doctor of Economics, e-mail: lanfk@mail.ru.

[22] *Liudmila A. Guzikova,* Professor, Higher School of Engineering and Economics, Peter the Great St. Petersburg Polytechnic University (29 Politekhnicheskaya ul., St. Petersburg, 195251, Russia), Doctor of Economics, e-mail: guzikova_la@spbstu.ru.