УДК 332.1 (470):344.13:004
DOI 10.14258/epb202629

ПРОТИВОДЕЙСТВИЕ СОВРЕМЕННЫМ КИБЕРПРЕСТУПЛЕНИЯМ КАК ФАКТОР ОБЕСПЕЧЕНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РОССИИ

Л. В. Рахлина, Н. А. Логинова

Санкт Петербургский университет Министерства внутренних дел Российской Федерации
(Санкт Петербург, Россия)

В статье на основе динамического и содержательного анализа киберпреступности как негативного фактора социально-экономического развития России сформулированы предложения по противодействию киберпреступлениям с целью обеспечения социально-экономического развития России. Проведенный анализ позволил изучить теоретические и практические аспекты исследования киберпреступности, выявить эволюцию преступлений в информационном пространстве. Методологическую основу данного исследования составили общенаучные методы — анализ, синтез, дедукция, индукция и специфические методы — матричный, анкетирование, ранжирование. Результатом проведенного исследования являются следующие рекомендации противодействия киберпреступлениям: разработка обязательных норм кибербезопасности для компаний, работающих с персональными данными, и сертификацию отечественных IT-решений; расширение программ магистратуры и аспирантуры по кибербезопасности в ведущих вузах; популяризация профессии искусственный интеллект в обществе; мониторинг darknet; создание резервных «цифровых убежищ» для критически важных данных; обязательное страхование киберрисков для компаний из стратегических отраслей.

Ключевые слова: киберпреступность, экономическая безопасность, информационные технологии, преступления, социально-экономическое развитие России.

COUNTERING MODERN CYBERCRIMES AS A FACTOR IN ENSURING THE SOCIAL AND ECONOMIC DEVELOPMENT OF RUSSIA

L. V. Rakhlina, N. A. Loginova

Saint Petersburg University of the Ministry of Internal Affairs of the Russian Federation
(Saint Petersburg, Russia)

This article, based on a dynamic and substantive analysis, cybercrime as a negative factor in Russia's Socioeconomic Development, formulates proposals for combating cybercrime to ensure Russia's socioeconomic development. The analysis allowed us to examine the theoretical and practical aspects of cybercrime research and identify the evolution of crimes in the information space. The methodological basis of this study consists of general scientific methods — analysis, synthesis, deduction, induction and specific methods — matrix, questionnaires, and ranking. The study results in the following recommendations for combating cybercrime: developing mandatory cybersecurity standards for companies working with personal data and certifying domestic IT solutions; expanding master's and doctoral programs in cybersecurity at leading universities; popularizing the profession of artificial intelligence in society; monitoring the darknet; creating backup “digital havens” for critical data; and mandatory cyberrisk insurance for companies in strategic industries.

Keywords: cybercrime, economic security, information technology, crimes, socio-economic development of Russia.

Введение. Распространение глобализационых процессов и дальнейшее развитие информационных технологий, которые внедряются в нашу жизнь, расширяют возможности для новых способов воздействия на личность и общество. В глобализационных процессах, как и в любых других, есть свои положительные и отрицательные стороны. Так, благодаря глобализационным процессам значительно упрощается наша жизнь, появляются новые формы обеспечения безопасности личности и общества. Но, с другой стороны, развитие глобализационых процессов способствует возникновению и распространению по всему миру современных видов киберугроз. Увеличение частоты кибератак и инцидентов, связанных с утечкой конфиденциальных данных, подрывает стабильность как отдельных предприятий, так и целых секторов экономики, что способно спровоцировать негативные последствия для макроэкономической устойчивости, стабильности и развития. Обеспечение защиты от современных киберугроз выступает ключевым условием устойчивого социально-экономического развития Российской Федерации. Киберпреступность создает существенные риски для экономической безопасности государства и дальнейшего эффективного социально-экономического развития. В условиях цифровой трансформации экономики России борьба с киберпреступностью становится неотъемлемым элементом стратегии ее развития на последующие годы.

Результаты исследования. На фоне динамичного развития информационных технологий наблюдается формирование и экспансия новых криминальных феноменов, в частности, в области высоких технологий. В данном контексте информационно-коммуникационные технологии (ИКТ) выступают как в качестве объекта противоправных посягательств, так и в роли инструментария или метода совершения преступлений.

Необходимо отметить, что в современной научной парадигме отсутствует консенсус относительно дефиниции понятия «киберпреступность». Современные ученые определяют ее следующими синонимами: «компьютерная преступность», «интернет-преступность», «цифровая преступность», «высокотехнологичная преступность», «технотронная преступность» [1].

По мнению В. Ф. Джафарли, «киберпреступление — это совокупность объективных и субъективных факторов, характеризующихся посягательствами на специфичный основной (сфера инновационных информационно-коммуникационных технологий) и дополнительные объекты, предметом посягательства (чужие электронные ресурсы), а также реализуемых путем использования кибертехнологий (средств) и дистанционным способом основных общественно опасных действий и желаемых последствий, происходящих и наступающих исключительно в киберпространстве (обстановка и место преступления), во время сеанса связи злоумышленника с ИКТ-устройством» [2].

В. Ф. Джафарли классифицировал все преступления, совершаемые с использованием информационно-коммуникационных технологий, на три группы: «киберпреступления, основные действия и последствия которых происходят исключительно в киберпространстве, причем ИКТ-компонент формально установлен в конкретной норме; киберпреступления, основные действия и последствия которых могут происходить исключительно в киберпространстве, причем ИКТ-компонент формально не отражен в конкретной норме; преступления, действия в которых в той или иной мере связаны с использованием ИКТ-средств» (ИКТ-средства — это Средства информационно-коммуникационных технологий)» [2].

В Стратегии национальной безопасности Российской Федерации (Указ Президента РФ от 02.07.2021 № 400) отражен рост числа преступлений, совершаемых с использованием информационно-коммуникационных технологий. Рост числа преступлений данного типа рассматривается как одна из угроз национальной безопасности, а их предупреждение, выявление, пресечение является стратегическим национальным приоритетом [3].

Первый существенный всплеск интереса к вопросам киберпреступности был отмечен в 2017 году, когда мир подвергся массированным атакам программ-вымогателей, таких как *WannaCry, Petya* и *BadRabbit*, что повлекло за собой серьезные последствия для множества организаций как в России, так и за ее границами.

В 2021 году наблюдался новый подъем интереса, спровоцированный чередой инцидентов, связанных с утечками конфиденциальной информации, активностью группировок, использующих программы-вымогатели, и всплеском DDoS-атак. В 2022 году отмечался взрывной рост числа атак, направленных на российские компании и государственные структуры, что, безусловно, отразилось и на медиа-ландшафте. К 2024 году количество материалов, посвященных кибербезопасности, достигло пиковых значений. Наибольшее внимание в СМИ уделялось финансовой сфере, информационным технологиям и телекоммуникациям, что соответствует характеру реальных угроз.

Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие особенности [4]: повышенная латентность совершения преступления, обеспечиваемая спецификой сетевого информационного

пространства (развитые механизмы анонимности, сложность инфраструктуры и т. п.); преступники, их цели и жертвы могут находиться в разных странах одновременно, что делает борьбу с такими преступлениями международной задачей; сетевые преступники, как правило, обладают глубокими знаниями и навыками, их деятельность носит интеллектуальный характер; способы совершения преступлений и используемые инструменты постоянно меняются, становятся все более сложными и разнообразными, что затрудняет их выявление и предотвращение. Преступления могут совершаться автоматически, охватывая несколько мест одновременно; существует возможность объединения вычислительных мощностей множества компьютеров для создания мощного инструмента преступной деятельности.

Выступая на заседании коллегии МВД в марте 2025 года, Президент России В. В. Путин оценил ущерб от киберпреступлений, который в 2024 году составил примерно 200 млрд рублей [5], а уровень их раскрываемости — примерно 23%[1].

За отчетный период наблюдалось снижение доли случаев, представляющих наивысшую критичность, в общем числе кибернетических атак, которые, по статистике, происходили реже, чем в первой половине 2024 года.

Под высококритичными атаками подразумеваются случаи нарушения информационной безопасности, которые сами организации оценивают, как способные вызвать продолжительную остановку важных для бизнеса процессов или могут привести к финансовым убыткам, превышающим миллион рублей. Эксперты из *RED Security SOC* полагают, что это может указывать на улучшение общего уровня защищенности от киберугроз в российских компаниях. Распространение и использование различных средств защиты информации на внешнем контуре организаций дает возможность в автоматическом режиме отражать определенное количество атак и пресекать, по крайней мере, часть несанкционированных проникновений.

Наибольшая интенсивность хакерских атак в 2025 году была зарегистрирована в апреле и мае, что косвенно подтверждает наличие политической базы у злоумышленников и стремление «привязать» взломы к значимым государственным датам. Следовательно, действия хактивистов по-прежнему являются существенной частью киберугроз, с которыми сталкиваются российские организации, что предполагает решение задачи о необходимости системного подхода к защите экономических интересов.

Экономическая безопасность, под которой понимается устойчивость системы к внутренним и внешним угрозам, напрямую зависит от способности противостоять киберугрозам. В отчете вашингтонского Центра стратегических и международных исследований (CSIS) содержится оценка, касающаяся экономических последствий киберпреступности. Эксперты полагают, что когда ущерб от кибератак достигнет определенного уровня, компании и общество в целом утратят толерантность к данной проблеме и начнут настаивать на внедрении кардинальных решений. Критической отметкой, по мнению специалистов, является убыток, превышающий 2% от валового внутреннего продукта. Киберпреступная деятельность негативно сказывается на торговых операциях, конкурентной борьбе, новаторских разработках и, как результат, на общем экономическом прогрессе.

Аналитики CSIS охарактеризовали киберпреступность как своего рода «сбор за инновации». Очевидно, что чем более развита экономическая система государства, тем значительнее становятся потери от киберпреступлений в соотношении с ее валовым внутренним продуктом.

По оценке CSIS, доля ущерба от киберпреступности в мире приближается уже к показателям наркоторговли и распространению контрафакта (табл. 1).

Таблица 1

Экономический ущерб от незаконных видов деятельности [5]

№	Вид деятельности	Ущерб, % от ВВП
1	Международная преступность	1,2
2	Наркотики	0,9
3	Подделка/пиратство	0,89
4	Киберпреступность	0,8
5	Морское пиратство	0,02

В 2024 году наблюдалась четкая тенденция: люди старше 60 лет оказались наиболее уязвимыми к мошенничеству, о чем свидетельствуют 147 127 жалоб и колоссальные 4,8 млрд долларов потерь [6]. Следующие по величине убытки понесли возрастные группы: 50–59 лет (84,5 тыс. жалоб, 2,5 млрд долларов потерь) и 40–49 лет (112,8 тыс. жалоб и 2,2 млрд долларов потерь). Примечательно, что молодежь до 20 лет пострадала значительно меньше (18 тысяч обращений и 22,5 млн долларов убытков). Среди наиболее распространенных видов мошенничества доминировали фишинг (193 тыс. случаев), вымогательство (86 тыс.), утечки личных данных (65 тыс.), схемы «запла-

[1] Ущерб от киберпреступлений в 2024 году составил порядка 200 млрд рублей // Комерсант. 05 марта 2025. [Сайт] URL: https://www.kommersant.ru/doc/7552645] (дата обращения: 20.09.2025).

тил — не получил» (50 тыс.) и фальшивые инвестиции (48 тыс.). Важно отметить, что криптовалюта использовалась в качестве платежного средства в 150 тыс. жалоб, что указывает на ее значительную роль в мошеннических схемах[2].

Исследование 2024 года выявило тревожную тенденцию: Россия признана лидером среди стран с самым высоким индексом киберпреступности[3]. С показателем WCI 58,39 Россия выступает как основной источник большинства киберугроз. За ней следуют Украина (36,44) и Китай (27,84), что подчеркивает глобальный характер проблемы. В число стран с наибольшим риском киберпреступности входят США (25,01) и Нигерия (21,28), а также Румыния, Северная Корея, Великобритания, Бразилия и Индия, что требует комплексного подхода к обеспечению кибербезопасности на международном уровне [7].

Согласно данным Всемирного индекса киберпреступности, наблюдается тенденция специализации отдельных государств на конкретных видах кибернетических угроз. Иными словами, страны концентрируют свои усилия и ресурсы на определенных типах преступлений в киберпространстве, что отражается в структуре мирового киберкриминала. Лидирующую позицию в сфере интернет-мошенничества занимает Нигерия. Установлено, что российские, украинские и китайские киберпреступники преимущественно занимаются разработкой и распространением вредоносного программного обеспечения, в то время как в Великобритании основное направление деятельности — незаконный вывод средств и отмывание полученных преступным путем денег. В Соединенных Штатах Америки наиболее распространенным видом киберпреступлений является похищение конфиденциальной информации.

Киберпреступность в России проявляется в следующих формах: финансовое мошенничество; фишинг; атаки на банковские системы (например, хищения через мобильные приложения). Целевые атаки на предприятия: *ransomware*-атаки на промышленность. Продажа персональных данных на *darknet*, компрометация государственных структур.

Нанесенный россиянами ущерб от телефонного мошенничества за 2024 год составил не менее 295 млрд руб. Если динамика сохранится, то по итогам 2025 года ущерб может достичь 350 млрд руб.[4] По данным Центрального банка России, в 2024 году мошенники похитили со счетов россиян на 74,4% больше средств, чем годом ранее, что оценивается на сумму в 27,5 млрд руб. В начале 2025 года общий рост мошеннических операций впервые за три года пошел на спад: за январь таких инцидентов стало меньше на 4,6% относительно января прошлого года [8]. По данным МВД, за 10 месяцев 2025 года удалось предотвратить более 27 млн случаев телефонного мошенничества[5]. Снижение количества таких преступлений по итогам января-октября составило 9,5%[6]. В октябре 2025 года количество телефонных мошенничеств уменьшилось на 25%.

Киберпреступность оказывает существенное влияние на экономическую безопасность, прямые потери, ущерб бизнесу, затраты на восстановление систем. Косвенные эффекты обоснованы снижением доверия к цифровым услугам, оттоком иностранных инвестиций (по данным РАЭК, 30% хозяйствующих субъектов избегают выхода на российский рынок из-за киберрисков). Атаки на объекты ТЭК могут вызвать остановку производств (пример: атака на нефтепровод «Транснефть» в 2020 г.).

Согласно данным «Лаборатории Касперского», в 2024 году 41,6% инцидентов, зафиксированных среди организаций, которые обращаются за помощью к команде экстренного реагирования на киберинциденты (GERT), были связаны с действиями шифровальщиков.

По сведениям от *Solar JSOC*, центра противодействия кибератакам ГК «Солар», 60% всех кибератак в промышленном секторе с начала 2024 года было вызвано попытками заражения систем вредоносным программного обеспечения.

Не вызывает сомнений, что в эпоху цифровизации финансовые киберпреступления стали одной из наиболее распространенных угроз, подрывающей стабильность бизнеса. Злоумышленники, чтобы получить доступ к учетным данным и проникнуть в банковские счета организаций, широко применяют такие методы, как фишинг, вредоносные программы и техники социальной инженерии[7]. Взлом онлайн-банкинга и корпоративных платежных систем дает преступникам возможность совершать незаконные операции и присваивать денежные средства. Также серьезную угрозу представляют подделки электронных платежных

---

[2] Отчет ФБР по киберпреступности в 2024 году. URL: https://cpa. rip/news/ic3-report-2024/ (дата обращения: 29.09.2025).

[3] Высокотехнологичный хакинг: Россия вошла в топ индекса киберпреступности // РБК 01 ноября 2024. URL: https://trends.rbc.ru/trends/industry/672471259a794794c6b77e87? from=copy (дата обращения: 12.10.2025).

[4] Сбербанк: официальный сайт. URL: https://www.sberbank.ru/ (дата обращения: 12.12.2025).

[5] В России снизилось количество телефонных мошенничеств и ущерб от них в 2025 году. URL: https://www.kommersant.ru/doc/8312024? (дата обращения: 22.12.2025).

[6] Там же.

[7] Сбербанк назвал сумму ущерба россиянам от телефонного мошенничества за 2024 год // Коммерсант. 04 марта 2025. URL: https://www.kommersant.ru/doc/7551712/7551712 (дата обращения: 22.12.2025).

документов, что может привести к значительным финансовым потерям и правовым сложностям для компаний [9, 10, 11].

В 2024 году на киберпреступления пришлось 40% всех преступлений, зарегистрированных в России[8], данный показатель является наивысшим начиная с 2020 года. За 11 месяцев 2025 года данный показатель составил 43%[9], что позволяет заключить о замедлении темпов прироста данного вида преступлений за последние 5 лет.

Отмывание денежных средств, осуществляемое посредством цифровых платформ, является одним из ключевых видов преступной деятельности. Оно стало проще благодаря активному использованию криптовалют и анонимных платежных систем, что ставит в тупик финансовых регуляторов. Одним из наиболее частых приемов является многократное перемещение средств через онлайн-казино, невозможно отследить их происхождение. Также мошенники используют автоматизированные торговые системы для размывания финансовых потоков. В условиях цифровой трансформации наблюдается всплеск активности финансовых пирамид и инвестиционного мошенничества [12]. Люди становятся жертвами, доверяя несуществующим инвестиционным платформам, торговым ботам и обещаниям легкого и быстрого обогащения. Путем искусственного завышения стоимости цифровых активов (криптовалют, токенов) перед их продажей мошенники лишают инвесторов их вложений. Организаторы этих схем успешно избегают правосудия, оставляя пострадавших без компенсации [13].

Статистические данные субъектов финансовых пирамид, собранные Банком России, представлены в таблице 2[10].

Таблица 2

Субъекты с признаками финансовой пирамиды [13]

	2023 год	2024 год	2025 год (1 полугодие)
Интернет-проекты	2886	5457	2288
Общества с ограниченной ответственностью	15	16	12
Потребительские кооперативы	16	4	5
Иные формы *	27	33	23
Всего выявлено	2944	5510	2328

Таким образом, в первом полугодии 2025 года удельный вес субъектов с признаками финансовой пирамиды составляет 42,3%, что 7,7% меньше относительно 2024 года. При этом прирост числа интернет-проектов показывает отрицательный прирост в –8,07%. В то время как число обществ с ограниченной ответственностью, проявляющих признаки финансовой пирамиды, увеличилось в 1,5 раза, потребительских кооперативов — в 2,5 раза, иных форм — в 1,4 раза.

Примечательно, что классические пирамиды до сих пор существуют и одновременно с этим возродилась практика проведения презентаций, активного обзвона потенциальных клиентов и приглашения их в офис для личного общения. Вместе с тем нами установлены на основании первоисточников [3, 5–10, 13–16] самые популярные схемы финансовых пирамид, в настоящее время представленных обязательным упоминанием криптовалют. Организаторы таких пирамид действуют не только в Интернете, но и оффлайн [17].

В настоящее время заметно сократилось количество мошеннических схем в форме экономических игр, симулирующих инвестиционную деятельность и гарантирующих пользователям доходность. Этот факт обусловлен в том числе с охлаждением интереса к играм-кликерам, вероятно, из-за разочарования потенциальной аудитории после обесценивания токенов одной из наиболее популярных игр.

Для вовлечения в мошеннические проекты субъекты с признаками финансовых пирамид или нелегальные кредиторы, выявленные в первом полугодии 2025 года, использовали более 170 телеграм-каналов и свыше 110 страниц в соцсетях, в то время как в 2024 и 2023 годах их было в разы больше.

В 2025 году по результатам рассмотрения материалов были приняты следующие меры:

1) возбуждены административные дела (по различным статьям КоАП РФ);
2) приняты иные меры реагирования (принудительно закрываются телеграм-каналы, страницы и пр.);
3) заблокирован доступ к онлайн-ресурсам, связанным с незаконными финансовыми

[8] В России в 2024 году IT-преступления достигли пика за последние 5 лет. URL: https://tass.ru/proisshestviya/ (дата обращения: 30.12.2025).

[9] В России снизилось количество телефонных мошенничеств и ущерб от них в 2025 году. URL: https://www.kommersant.ru/doc/8312024? (дата обращения: 22.12.2025).

[10] Сайт Банка России. URL: https://cbr.ru/analytics/inside/ (дата обращения: 15.12.2025).

организациями и структурами, имеющими признаки финансовых пирамид [18].

В ответ на растущую угрозу перехода пользователей на вредоносные ресурсы разработчики антивирусного программного обеспечения в сотрудничестве с Банком России активно пополняют свои базы данных информацией о подозрительных сайтах. Наряду с этим растет угроза налоговых преступлений, совершаемых с помощью цифровых технологий. Особенно тревожит тот факт, что современные офшорные схемы активно используют криптовалюты для сокрытия прибыли и обхода налоговых законов [14]. Современные офшорные стратегии зачастую задействуют криптовалюты для маскировки финансовых потоков и уклонения от налоговых обязательств. Некоторые хозяйствующие субъекты прибегают к искусственным способам снижения налогооблагаемой базы, включая применение цифровых бухгалтерских платформ, фальсификацию финансовой отчетности и проведение сложных финансовых манипуляций. В последние годы автоматизация процессов с внедрением искусственного интеллекта приобретает особое значение в механизмах уклонения от налогов. Количество выявленных налоговых преступлений неуклонно растет (табл. 3).

Таблица 3

Динамика налоговых преступлений с применением цифровых технологий [11]

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025[11]
Количество преступлений	1655	1831	2022	3111	2428	2894	2798	2675	2896	3458	4117	5230	5450

Анализ данных таблицы 2 позволяет заключить, что в период с 2013 по 2025 год наблюдался существенный скачок (более чем втрое) в количестве налоговых преступлений, совершаемых с использованием цифровых технологий. Это связано с бурным развитием цифровых инструментов (таких как электронные деньги, онлайн-торговля, блокчейн, одноранговые сети и др.), а также с увеличением налогового бремени, сокращением оборота наличных, упрощением вывода прибыли через трансфертное ценообразование, размещением нематериальных активов в офшорах и другими схемами, включая перераспределение долга и фиктивные сделки.

Несмотря на то, что Москва (1,7 тыс.), Санкт-Петербург (1,5 тыс.) и Краснодарский край (0,9 тыс.)[12] являются лидерами по абсолютному числу зарегистрированных налоговых преступлений с применением цифровых технологий, общая картина с их раскрываемостью вызывает серьезные опасения. В 2024 году лишь около 20% таких преступлений были раскрыты, причем в отдельных регионах, таких как Ленинградская область (менее 11%), Севастополь и Смоленская область (менее 12%)[13] этот показатель критически низок.

Цифровое пространство стало ареной для серьезных угроз в виде корпоративного шпионажа и утечек данных. Преступные группы активно ищут уязвимости в корпоративных базах данных, чтобы получить доступ к ценной информации, такой как коммерческие тайны и персональные данные клиентов. Помимо прямого хищения, инсайдерская информация используется для манипуляций на фондовых рынках, что позволяет нечистоплотным участникам извлекать выгоду из предсказуемых движений котировок. Появление передовых технологий (например, *Deepfake* [15]) значительно повышает уровень опасности, поскольку они могут быть применены для фальсификации цифровых документов и дискредитации влиятельных лиц в бизнесе, создавая риски для финансовых активов и деловой репутации современных хозяйствующих субъектов.

Правовые и институциональные механизмы противодействия. Основным законодательным инструментом является Федеральный закон № 187 «О безопасности критической информационной инфраструктуры», дополненный Концепцией кибербезопасности РФ, где акцент сделан на импортозамещение программного обеспечения[14]. Среди институтов выделяются Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и Роскомнадзор, который занимается блокировкой противоправного контента. Важную роль играет международное сотрудничество, в частности, участие России в Шанхайской организации сотрудничества (ШОС) по вопросам кибербезопасности. Технологические решения

[11] Динамика налоговых преступлений с применением цифровых технологий представлена за 11 месяцев 2025 года.

[12] Генеральная прокуратура. URL: https://d-russia.ru/rossii-udalos-prelomit-tendenciju-rosta-onlajn-prestupnosti-genprokuratura (дата обращения: 05.01.2026).

[13] Там же.

[14] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ. URL: http://www.kremlin.ru/acts/bank/42128 (дата обращения: 27.12.2025).

включают внедрение искусственного интеллекта для анализа угроз и использование блокчейна в банковской сфере. В рамках государственно-частного партнерства создаются киберполигоны для тестирования решений, например, совместные проекты Сбербанка и Ростеха.

Образовательные программы подготовки специалистов в организациях высшего образования, таких как МФТИ и ИТМО, также являются важным элементом стратегии. Ключевые проблемы включают дефицит кадров: по оценкам RAEC, к 2025 году нехватка специалистов достигнет 300 тыс. человек. Геополитические ограничения, такие как сокращение сотрудничества с западными странами, усложняют обмен опытом. Кроме того, злоумышленники активно используют искусственный интеллект для создания адаптивных атак, что требует постоянного обновления защитных механизмов. Для укрепления законодательной базы предлагается расширить положения ФЗ № 187, включив в перечень к искусственному интеллекту объекты сельского хозяйства и малый бизнес, а также ввести уголовную ответственность за использование искусственного интеллекта в кибератаках, включая генерацию *deepfake*-контента.

Указ Президента РФ от 9 мая 2017 года № 203 утвердил Стратегию развития информационного общества в Российской Федерации на 2017–2030 годы. Согласно данной стратегии развития информационного общества [9], определены цели, задачи и меры по реализации внутренней и внешней политики РФ в сфере применения информационных и коммуникационных технологий. При этом центральное место отведено формированию технологической основы для развития экономики и социальной сферы, которая должна базироваться на реализации потребностей личности и общества, обеспечение национальных интересов.

Стандартизация требований должна предусматривать разработку обязательных норм кибербезопасности для компаний, работающих с персональными данными, и сертификацию отечественных IT-решений. Введение обязательного киберстрахования для стратегических отраслей и создание государственного фонда компенсаций для малого бизнеса помогут минимизировать риски. Технологическая модернизация требует увеличения финансирования R&D в области кибербезопасности через гранты и налоговые льготы для стартапов. Создание национальной платформы для тестирования уязвимостей (киберполигонов) с участием компаний, таких как Яндекс и «Касперский», ускорит разработку защитных решений. Внедрение блокчейна для защиты финансовых транзакций и предиктивной аналитики на базе искусственного интеллекта повысит устойчивость систем. Для критической инфраструктуры актуальны проекты «цифровых двойников» и квантовой криптограф искусственный интеллект.

В сфере кадровой политики необходимо расширить программы магистратуры и аспирантуры по кибербезопасности в ведущих вузах, таких как МГУ и ИТМО, с упором на практические навыки. Федеральная программа *CyberSkills* позволит переобучить IT-специалистов из смежных областей, а ежегодные киберучения для сотрудников МВД и ФСБ повысят их готовность к инцидентам.

Популяризация профессий, связанных с применением искусственного интеллекта через олимпиады, хакатоны и медиакампании, такие как «Кибергерои России», привлечет молодежь в отрасль. Усиление международного сотрудничества предполагает разработку единых протоколов расследования киберпреступлений в рамках БРИКС и создание совместного киберцентра ШОС для обмена данными об угрозах. Партнерство с ОАЭ, Сингапуром и Индией в борьбе с криптовалютным отмыванием денег, а также проведение конференций с участием стран Глобального Юга расширит возможности взаимодействия. Оперативное реагирование и мониторинг требуют развертывания региональных центров CERT в каждом федеральном округе и налаживания автоматизированного обмена данными между ними, банками и правоохранительными органами. Мониторинг же *darknet* с использованием искусственного интеллекта алгоритмов для выявления утечек данных и введение ответственности для хостинг-провайдеров за размещение противоправного контента усилят контроль.

Создание резервных «цифровых убежищ» для критически важных данных, в свою очередь, ускорит восстановление после атак. Стимулирование публично-частного партнерства включает организацию акселераторов для стартапов при поддержке Сбербанка и ВЭБ. РФ, а также запуск программы госзакупок «Киберщит» для внедрения отечественных решений. Платформа для анонимного обмена данными об угрозах между компаниями и система бонусов за сообщения о кибератаках повысят уровень коллективной безопасности. Рекомендации по противодействию киберпреступности в России: расширить положения ФЗ № 187 «О безопасности критической информационной инфраструктуры (искусственный интеллект)», ввести уголовную ответственность за использование искусственного интеллекта в кибератаках, включая генерацию *deepfake*-контента для мошенниче-

ства[15] [16]. Также необходимо разработать обязательные стандарты кибербезопасности для всех предприятий, работающих с персональными данными (по аналогии с искусственным интеллектом с GDPR в ЕС), внедрить сертификацию отечественных IT-решений для госсектора, исключив использование непроверенного иностранного программного обеспечения, установить обязательное страхование киберрисков для компаний из стратегических отраслей (ТЭК, финансы, транспорт), создать государственный фонд компенсаций для малого и среднего бизнеса, пострадавшего от *ransomware*-атак увеличить финансирование R&D в области кибербезопасности через гранты и налоговые льготы для стартапов (например, по аналогии с Фондом развития интернет-инициатив), создать национальную платформу для тестирования уязвимостей в программном обеспечении (киберполигоны) с участием компаний (Яндекс, Касперский, Ростех).

Внедрение передовых технологий: использовать блокчейн для защиты цепочек поставок и финансовых транзакций. Следующим не менее важным аспектом является оперативное реагирование и мониторинг, для наиболее эффективного обеспечения экономической безопасности России. Для этого необходимо наладить автоматизированный обмен данными между CERT, банками и правоохранительными органами, ввести ответственность хостинг-провайдеров за размещение ресурсов, связанных с киберпреступностью, создать резервные «цифровые убежища» для хранения критически важных данных.

Организовать акселераторы для стартапов в области кибербезопасности при поддержке Сбербанка, Газпромбанка и ВЭБ. РФ. Запустить программу госзакупок «Киберщит», направленную на внедрение отечественных решений в госсекторе, а также обмен информацией, для чего необходимо создать платформу для анонимного обмена данными об угрозах между компаниями. Внедрить систему бонусов для организаций, сообщающих о кибератаках. Реализация предложенных мер требует консолидации усилий государства, бизнеса, науки и гражданского общества.

Ключевыми приоритетами должны стать: импортозамещение технологий, подготовка кадров, адаптивное законодательство и формирование культуры кибербезопасности. Только системный подход позволит России минимизировать экономические потери от киберпреступности и укрепить в глобальном цифровом пространстве.

Выводы. Проблема киберпреступности является одной из ключевых вызовов современности, требующей незамедлительного и системного реагирования. Для ее эффективного преодоления необходимо реализовать комплекс мер, включающий:

1) интеграцию международных усилий и совершенствование нормативно-правовой базы Российской Федерации в части регулирования интернет-среды;
2) внедрение перманентного мониторинга онлайн-ресурсов, осуществляющих коммерческую деятельность и предоставление сервисов;
3) оперативное пресечение деятельности подозрительных веб-сайтов посредством их блокировки;
4) формирование кадрового резерва высококвалифицированных специалистов в области информационных технологий;
5) повышение уровня цифровой компетенции и культуры населения.

По нашему мнению, противодействие киберпреступности требует комплексного подхода, объединяющего технологические инновации, правовое регулирование и международную кооперацию. Успешная реализация стратегий позволит минимизировать риски для экономической безопасности России в условиях цифровизации и обеспечить дальнейшее всестороннее социально-экономического развитие России.

Таким образом, рассмотренные в статье направления и пути противодействия современным киберпреступлениям при правильном и всестороннем их применении будут способствовать социально-экономическому развитию страны на долгие годы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Евдокимов К. Н. К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации // Российский следователь. 2021. № 10. С. 69–72.

2. Джафарли В. Ф. Криминология кибербезопасности: в 5 т. Т. 2: Уголовно-правовое обеспечение криминологической кибербезопасности / под ред. С. Я. Лебедева. М., 2021. 280 с.

[15] Доктрина информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646; в ред. от 21.07.2022. URL: https://base.garant.ru/71556224/ (дата обращения: 02.12.2025).

3. Темирбеков К. А. Противодействие киберпреступлениям в России и зарубежных странах: сравнительно-правовой анализ // Евразийский юридический журнал. 2024. № 11 (198). С. 327–329.

4. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология. Вчера, сегодня, завтра. 2012. № 1 (24). С. 45–54.

5. Кунц Е. В. Противодействие современным киберпреступлениям // Российско-азиатский правовой журнал. 2025. № 1. С. 97–104.

6. Лопатин С. В. Криминологическая характеристика киберпреступности на современном этапе развития общества // Международный журнал гуманитарных и естественных наук. 2025. № 8 (107). С. 349–353.

7. Копылов В. В., Прокофьев О. М., Субботин А. А., Истомин А. А. Анализ факторов, способствующих росту мобильного мошенничества в России // Человек: преступление и наказание. 2024. Т. 32. № 2. С. 247–257.

8. Голубовский В. Ю. Межотраслевые проблемы в сфере противодействия киберпреступлениям // Уголовно-исполнительная система: история и современность: сборник материалов Межвузовской научно-практической конференции с международным участием, Псков, 18–19 апреля 2024 года. Псков, 2024. С. 51–59.

9. Минаев В. А., Бондарь К. М. Противодействие киберпреступности на основе технологий искусственного интеллекта // Информация и безопасность. 2025. Т. 28, № 2. С. 181–190.

10. Иванов П. И. Оперативно-розыскное противодействие киберпреступлениям (проблемы и пути их решения) // Труды Академии управления МВД России. 2022. № 4 (64). С. 83–92.

11. Логинова Н. А., Головинский М. А. Предпосылки исследования криминальной деятельности участников онлайн-бизнеса // Экономическая политика и национальная безопасность. 2025. № 1 (1). С. 41–52.

12. Варакса Н. Г., Бехбудова Ф. Ф. Финансовые пирамиды как угроза финансовой безопасности граждан // Тренды и перспективы цифровой экономики: финансовые технологии и безопасность: материалы II Всероссийской научно-практической конференции, Орёл, 20–21 июня 2023 года. Орёл, 2023. С. 177–185.

13. Андреев Е. В., Токолов А. В. Противодействие киберпреступлениям в сфере национальной безопасности // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий: сборник научных статей. М., 2023. С. 21–24.

14. Демьянович А. А. Противодействие киберпреступлениям // Актуальные проблемы развития российского законодательства и практика его применения: сборник научных статей по результатам Всероссийской научно-практической конференции с международным участием, Ижевск, 15–16 ноября 2022 года. Ижевск, 2022. С. 389–393.

15. Хамидуллин С. А., Кибатов М. С., Лебедева А. В. Расследование хищений денежных средств, совершенных с использованием информационно-телекоммуникационной сети Интернет // Вопросы взаимодействия правоохранительных органов и их подразделений при раскрытии и расследовании преступлений: сборник трудов межведомственного круглого стола, Тверь, 06 апреля 2022 года. Тверь, 2022. С. 142–148.

16. Семенова И. С., Молодых М. Е. Некоторые вопросы совершенствования противодействия киберпреступлениям // Государство, право и общество: вопросы теории и практики: сборник материалов III Всероссийской с международным участием научно-практической конференции, Сочи, 27–28 октября 2022 года. Киров, 2022. С. 44–48.

17. Воротникова А. С. Отдельные закономерности совершения современных экономических преступлений в киберпространстве // Гуманитарные, социально-экономические и общественные науки. 2024. № 12. С. 150–154.

18. Арженовский С. В., Бахтеев А. В., Синявская Т. Г. Комплекс мер по противодействию угрозам национальной безопасности России в сфере аудита // Финансовые исследования. 2021. № 3 (72). С. 22–29.

REFERENCES

1. Evdokimov K. N. On Improving the System of Combating Technetronic Crime in the Russian Federation. Russian Investigator. 2021. No. 10. Pp. 69–72.

2. Jafarli V. F. Criminology of Cybersecurity: in 5 volumes. Vol. 2: Criminal-Legal Support for Criminological Cybersecurity / edited by S. Ya. Lebedev. Moscow, 2021. 280 p.

3. Temirbekov K. A. Counteracting Cybercrime in Russia and Foreign Countries: A Comparative Legal Analysis. Eurasian Law Journal. 2024. No. 11 (198). Pp. 327–329.

4. Nomokonov V. A., Tropina T. L. Cybercrime as a New Criminal Threat. Criminology. Yesterday, Today, Tomorrow. 2012. No. 1 (24). Pp. 45–54.

5. Kunz E. V. Counteracting Modern Cybercrimes. Russian-Asian Legal Journal. 2025. No. 1. Pp. 97–104.

6. Lopatin S. V. Criminological Characteristics of Cybercrime at the Current Stage of Society Development. International Journal of Humanities and Natural Sciences. 2025. No. 8 (107). Pp. 349–353.

7. Kopylov V. V., Prokofiev O. M., Subbotin A. A., Istomin A. A. Analysis of factors contributing to the growth of mobile fraud in Russia. Man: Crime and Punishment. 2024. Vol. 32. No. 2. Pp. 247–257.

8. Golubovsky V. Yu. Intersectoral Problems in Combating Cybercrime. The Penitentiary System: History and Modernity: Collection of Materials of the Interuniversity Scientific and Practical Conference with International Participation, Pskov, April 18–19, 2024. Pskov, 2024. Pp. 51–59.

9. Minaev V. A., Bondar K. M. Combating Cybercrime Based on Artificial Intelligence Technologies // Information and Security. 2025. Vol. 28. No. 2. Pp. 181–190.

10. Ivanov P. I. Operational-search counteraction to cybercrime (problems and solutions). Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2022. No. 4 (64). Pp. 83–92.

11. Loginova N. A., Golovinsky M. A. Prerequisites for the study of criminal activities of online business participants. Economic Policy and National Security. 2025. No. 1 (1). Pp. 41–52.

12. Varaksa N. G., Bekhbudova F. F. Financial pyramids as a threat to the financial security of citizens. Trends and prospects of the digital economy: financial technologies and security: Proceedings of the II All-Russian scientific and practical conference, Orel, June 20–21, 2023. Orel, 2023. Pp. 177–185.

13. Andreev E. V., Tokolov A. V. Counteracting cybercrimes in the sphere of national security. Counteracting crimes in the sphere of information and telecommunication technologies: Collection of scientific articles. Moscow, 2023. Pp. 21–24.

14. Dem'yanovich A. A. Counteracting cybercrime. Current issues in the development of Russian legislation and the practice of its application: Collection of scientific articles based on the results of the All-Russian scientific and practical conference with international participation, Izhevsk, November 15–16, 2022. Izhevsk, 2022. Pp. 389–393.

15. Khamidullin S. A., Kibatov M. S., Lebedeva A. V. Investigation of thefts of funds committed using the information and telecommunications network Internet. Issues of interaction between law enforcement agencies and their units in solving and investigating crimes: Collection of works of the interdepartmental round table, Tver, April 6, 2022. Tver, 2022. Pp. 142–148.

16. Semenova I. S., Molodykh M. E. Some issues of improving counteraction to cybercrime. State, law and society: issues of theory and practice: Collection of materials of the III All-Russian scientific and practical conference with international participation, Sochi, October 27–28, 2022. Kirov, 2022. Pp. 44–48.

17. Vorotnikova A. S. Certain patterns of modern economic crimes in cyberspace. Humanitarian, socio-economic and social sciences. 2024. No. 12. Pp. 150–154.

18. Arzhenovsky S. V., Bakhteyev A. V., Sinyavskaya T. G. A set of measures to counter threats to Russia's national security in the field of audit. Financial research. 2021. No. 3 (72). Pp. 22–29.

Поступила в редакцию: 16.01.2026.
Принята к печати: 16.03.2026.