**Анна Павловна АЛЕКСЕЕВА,**
доктор юридических наук, профессор, ORCID 0000-0002-4569-7564
Санкт-Петербургский университет МВД России (г. Калининград)
профессор кафедры уголовного права, криминологии
и уголовно-исполнительного права Калининградского филиала
Заслуженный юрист Российской Федерации
*alexeeva.klg-mvd@yandex.ru*

**Ольга Ивановна БЕЛОКОБЫЛЬСКАЯ,**
кандидат юридических наук, доцент, ORCID 0009-0007-9093-4761
Волгоградская академия МВД России (г. Волгоград)
доцент кафедры оперативно-разыскной
деятельности и специальной техники
*belokob-olga@yandex.ru*

Научная статья
УДК 343.85:[343.721:004]

# СОВРЕМЕННЫЕ СПОСОБЫ СОВЕРШЕНИЯ КИБЕРМОШЕННИЧЕСТВ И ОСНОВНЫЕ ПУТИ ПРОТИВОДЕЙСТВИЯ ИМ

**КЛЮЧЕВЫЕ СЛОВА. Кибермошенничество, способ совершения преступления, дистанционная форма совершения преступления, цифровизация, противодействие кибермошенничеству, кибербезопасность.**

**АННОТАЦИЯ.** ***Введение.*** *В России преступления против собственности традиционно совершаются чаще других. За последние десять лет в структуре корыстной преступности доля краж сократилась, в то время как доля мошенничеств существенно выросла. Это связано с развитием технологий и повышением уровня доступности информации в современном мире. Люди всё больше зависят от Интернета и мобильных устройств, что делает их уязвимыми для дистанционного обмана.* ***Методы.*** *В ходе исследования применялся общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Кроме того, были использованы метод описания, абстрагирование и обобщение, статистический метод.* ***Результаты.*** *За последний год в России увеличился объем незаконно выведенных из банков средств. Одним из наиболее распространенных сегодня способов кибермошенничества является хищение денег с виртуальных карт через сайты-двойники. Новым видом преступлений стало заражение компьютеров криптомайнером, которое приводило к снижению мощности устройства, его перегреву, перерасходу электроэнергии. Наряду с новыми способами для совершения кибермошенничеств используются и ранее известные, например, когда преступники пытаются убедить граждан в мнимом содействии правоохранительным органам, заставляя их передавать злоумышленникам наличные деньги. В 2024 году проявилась негативная тенденция, связанная с привлечением мошенниками несовершеннолетних к совершению незаконных операций с помощью мобильных устройств родителей. Противодействие кибермошенничеству представляет собой важное для страны и требующее постоянного к себе внимания направление работы. Ключевую роль в этом процессе играет государство, так как от его своевременного реагирования на возникающие угрозы зависит не только безопасность отдельных граждан и компаний, но и национальная безопасность в целом.*

**ВВЕДЕНИЕ**

Преступления против собственности в России традиционно занимают лидирующие позиции в статистике зарегистрированных противоправных деяний. Их доля, как правило, составляет более половины общего количества преступлений. Вместе с тем необходимо отметить, что в последнее время наблюдается тенденция к перераспределению долей внутри корыстной преступности. Так, если доля краж за прошедшие десять лет существенно сократилась (в 2015 году она составляла 42,4% в общем объеме преступности, в 2019 – 38,2%, в 2024 – 26,1%), то доля мошенничеств значительно выросла (в 2015 году – 8,4% в общем объеме преступности, в 2019 – 12,7%, в 2024 – 23,3%)[1].

По нашему мнению, вполне очевидно, что сокращение количества краж и увеличение числа зарегистрированных мошенничеств связано с развитием технологий и повышением уровня доступности информации в современном мире. В эпоху, когда люди активно пользуются Интернетом, различными мобильными устройствами и разработанными для них приложениями, они становятся всё более уязвимыми для дистанционного обмана. Кражи же, как правило, требуют прямого контакта с жертвой, поэтому такой способ совершения преступления постепенно теряет свою привлекательность для преступников. В условиях стремительной цифровизации общества предпринимаемые меры по обеспечению безопасности, в том числе улучшение систем видеонаблюдения, внедрение управляемых с помощью искусственного интеллекта комплексов и т.д., препятствуют сокрытию следов краж, способствуют установлению и изобличению виновных. Другое дело – мошенники, применяющие новые способы совершения хищений (фишинг, спуфинг, скам, трояны и т.д.): сведения об их личности и местонахождении остаются скрытыми благодаря анонимности их деятельности в Интернете, что осложняет процесс привлечения их к ответственности за содеянное.

По заявлению руководителя Центробанка России Э.С. Набиулиной, в 2024 году было зафиксировано увеличение на 15% объема средств, незаконно выведенных из кредитных организаций. У физических лиц злоумышленникам удалось похитить более 27 миллиардов рублей, что выше показателя 2023 года на 74,4%[2]. Э.С. Набиулина объяснила сложившуюся ситуацию ростом популярности безналичных операций, связанных с приобретением товаров, оплатой услуг и т.д. При этом нет уверенности в том, что все банки в полном объеме передавали в общую базу данных ставшую им известной информацию о противоправных деяниях в отношении их клиентов. Некоторые финансовые организации могли умышленно занижать уровень кибермошенничества, опасаясь репутационных потерь, обвинений в недостаточном внимании к обеспечению безопасности вкладчиков и т.д.

С мнением руководителя Центробанка России вполне согласуется вывод некоторых исследователей о том, что в 2024 году наиболее популярным способом кибермошенничества стало хищение денег с виртуальных карт, которыми пользуются покупатели маркетплейсов [1, с. 64; 2, с. 36]. Преступники для этого создают сайты-двойники, которые внешне практически неотличимы от оригиналов. При попытке совершения покупателем оплаты товаров (услуг) мошенник получает доступ к сведениям о банковской карте жертвы, после чего происходит незаконное списание всех имеющихся на ней средств. Аналогичная схема действует и при попытке оплаты покупки через двойники мобильных приложений.

Еще одним недавно выявленным способом получения незаконного дохода путем обмана граждан является заражение компьютеров физических лиц так называемым криптомайнером через установленную на устройство популярную игру. Вместе с игрой на компьютер без ведома его владельца устанавливается вредоносное программное обеспечение (троян), которое вместе с игрой запускает программу майнинга, используемую для получения криптовалюты. Сгенерированные доходы отправляются злоумышленникам[3]. Среди наиболее очевидных последствий такого заражения можно отметить снижение мощности устройства, его перегруженность, перегрев, перерасход электроэнергии и т.д.

Наряду с новыми видами кибермошенничества продолжают фиксироваться и известные ранее варианты его совершения, когда преступникам удается убедить граждан в том, что они содействуют правоохранительным органам [3, с. 110]. Так, например, мошенники убедили Н. в том, что ее квартира находится в опасности из-за действий мужа, и предложили ей сотрудничество с ФСБ, чтобы решить эту проблему. Н., не подозревая об истинных намерениях мошенников, согласилась помогать и стала курьером, передавая наличные деньги от обманутых жертв «инкассаторам»[4]. Отличие этого и других похожих случаев от ранее зафиксированных заключается в том, что в последнее время мошенники пытаются любыми способами получить именно наличные деньги. Из-за того, что службы безопасности банков стали всё чаще блокировать сомнительные транзакции, у мошенников перестало получаться доводить

[1] Статистика и аналитика // МВД России: сайт // URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 23.02.2025).
[2] ЦБ зафиксировал рекордную сумму хищений у банковских клиентов в 2024 году // РБК: сайт. 18.02.2025 // URL: https://www.rbc.ru/finances/18/02/2025/67b489749a794780d1527516.
[3] Злоумышленники заражали устройства российских пользователей криптомайнером под видом игр-симуляторов // Лаборатория Касперского: сайт. 25.02.2025 // URL: https://www.kaspersky.ru/about/press-releases/zloumyshlenniki-zarazhali-ustrojstva-rossijskih-polzovatelej-kriptomajnerom-pod-vidom-igr-simulyatorov.
[4] Российская учительница хотела поймать мошенников, но стала их соучастницей // Московский комсомолец: сайт. 20.02.2025 // URL: https://www.mk.ru/incident/2025/02/20/rossiyskaya-uchitelnica-khotela-poymat-moshennikov-no-stala-ikh-souchastnicey.html.

**Anna P. ALEKSEEVA,**
Doctor of Law, Professor, ORCID 0000-0002-4569-7564
Saint-Petersburg University of the Ministry
of the Interior of Russia (Kaliningrad, Russia)
Professor of the Department of Criminal Law, Criminology
and Criminal Executive Law of the Kaliningrad Branch
Honored Lawyer of the Russian Federation
*alexeeva.klg-mvd@yandex.ru*

**Olga I. BELOKOBYLSKAYA,**
Cand. Sci. (Jurisprudence), Associate Professor, ORCID 0009-0007-9093-4761
Volgograd Academy of the Ministry of the Interior of Russia (Volgograd, Russia)
Associate Professor of the Department of Operational
Investigative Activities and Special Equipment
*belokob-olga@yandex.ru*

# MODERN METHODS OF COMMITTING CYBERFRAUD AND THE MAIN WAYS TO COUNTER THEM

**KEYWORDS. Cyberfraud, method of committing a crime, remote form of committing a crime, digitalization, counteraction to cyberfraud, cybersecurity.**

**ANNOTATION.** ***Introduction.*** *In Russia, property crimes are traditionally committed more often than others. Over the past ten years, the share of thefts in the structure of acquisitive crime has decreased, while the share of fraud has increased significantly. This is due to the development of technology and the increasing availability of information in the modern world. People are increasingly dependent on the Internet and mobile devices, which makes them vulnerable to remote fraud.* ***Methods.*** *The study used the general scientific dialectical method of cognition of the surrounding reality, which involves a complete and comprehensive study of phenomena, consideration of the connections and contradictions between them. In addition, the description method, abstraction and generalization, and the statistical method were used.* ***Results.*** *Over the past year, the volume of funds illegally withdrawn from banks has increased in Russia. One of the most common methods of cyber fraud today is the theft of money from virtual cards through duplicate sites. A new type of crime has become the infection of computers with a cryptominer, which led to a decrease in the power of the device, its overheating, and excessive energy consumption. Along with new methods, previously known ones are also used to commit cyber fraud, for example, when criminals try to convince citizens of imaginary assistance to law enforcement agencies, forcing them to hand over cash to the attackers. In 2024, a negative trend emerged related to fraudsters attracting minors to commit illegal transactions using their parents' mobile devices. Counteracting cyber fraud is an important area of work for the country that requires constant attention. The state plays a key role in this process, since not only the safety of individuals and companies, but also national security as a whole depends on its timely response to emerging threats.*

свой умысел до конца и завладевать сбережениями жертв при помощи проведения электронных операций.

Среди негативных тенденций кибермошенничества, проявившихся в 2024 году, стоит выделить повышение интереса преступников к ранее не охваченной их вниманием аудитории. Теперь мошенники пытаются уговаривать детей и подростков совершать незаконные операции с помощью мобильных устройств их родителей [4, с. 360; 5, с. 83]. Злоумышленники связываются с несовершеннолетним посредством мессенджеров, в ходе разговора представляются сотрудниками банка или другой организации, убеждают ребенка в том, что его родители нуждаются в помощи. Затем просят продиктовать им информацию с банковской карты или сообщить пароль от мобильного приложения банка, якобы чтобы предотвратить хищение денег.

Значительную опасность кибермошенничество представляет не только для физических лиц, но и для организаций, для бизнеса. Так, в аналитическом отчете российской компании «F6», являющейся разработчиком технологий для борьбы с киберпреступлениями, отмечена повышенная опасность программ-вымогателей, с помощью которых преступники получают доступ к электронным устройствам фирм, затем зашифровывают хранящуюся на них информацию и требуют выкуп за возможность ее расшифровать [6, с. 124]. Запрашиваемые в таких случаях суммы в 2024 году варьировались для малого бизнеса от 100 тысяч до 5 миллионов рублей, а для крупных и средних компаний – от 5 миллионов рублей и выше. Вместе с тем было спрогнозировано, что в 2025 году программы-вымогатели продолжат оставаться основными киберугрозами для российских компаний. В условиях геополитического конфликта ожидается увеличение количества кибератак и осуществляющих их хакерских групп. В отчете указано, что если в 2023 году было зафиксировано 14 таких групп, то в 2024-м их было уже 27[1].

Между тем, по данным Роскомнадзора, произошло снижение числа случаев несанкциониро-

[1] Главные киберугрозы 2025 года назвали в F6 // Ведомости: сайт. 19.02.2025 // URL: https://www.vedomosti.ru/technology/articles/2025/02/19/1093056-glavnie-kiberugrozi (дата обращения: 23.02.2025).

ванного доступа к информации, содержащейся в базах данных компаний: со 168 в 2023 году до 135 в 2024-м. Эти базы данных включали в себя в прошлом году более 710 миллионов записей о гражданах Российской Федерации (годом ранее – 300 миллионов)[1]. Соответственно, объем сведений, к которым был получен незаконный доступ, стал больше, однако количество зафиксированных случаев утечки данных уменьшилось. С одной стороны, снижение числа эффективно реализованных эпизодов незаконного доступа к сведениям было обусловлено по большей части высокой степенью готовности финансовых организаций к внедрению инновационных технологий безопасности. Банки сегодня располагают значительными материальными и человеческими ресурсами для развития систем защиты информации, что и позволяет им сравнительно быстро адаптироваться к постоянно меняющимся угрозам. С другой стороны, само по себе сокращение количества случаев не всегда является гарантией существенного улучшения кибербезопасности. Поэтому важно не только констатировать снижение числа посягательств, но и постоянно принимать меры для предотвращения новых инцидентов, особенно, когда речь идет о конфиденциальных сведениях, охраняемых государством. Косвенным подтверждением нашего вывода является значительный рост доли незаконно раскрытой информации, относящейся к категории коммерческой тайны. Если в 2023 году этот показатель составил 8,9% от общего объема зафиксированных случаев несанкционированного доступа к информации, то в 2024 году он увеличился до 20%. В основном такие инциденты в российских финансовых организациях были связаны с кибератаками проукраинских активистов на небольшие банки и страховые компании – 88% случаев, причем за 2024 год их число выросло на 7%. Еще 8% – это результат незаконных действий сотрудников, предавших интересы своей организаций (эта доля, напротив, уменьшилась на 4,6%) [7, с. 216]. Злоумышленники сразу же публиковали незаконно полученные сведения. Например, в Интернет попали файлы из бухгалтерской базы данных одной из известных страховых фирм [8, с. 134].

Стоит отметить, что государственные организации, крупные компании и предприятия всё чаще привлекают к сотрудничеству независимых программистов (так называемых «белых хакеров»), которые целенаправленно ищут уязвимости в объектах информационной инфраструктуры. Несмотря на то, что цель их деятельности кардинально отличается от целей злоумышленников, внешне используемые ими способы поиска часто похожи на кибератаки. В связи с этим актуальным стал вопрос о юридической оценке подобной деятельности. Для того чтобы легализовать такого рода работу независимых программистов, законодателем был разработан законопроект[2], в котором предложено закрепить необходимость идентификации таких специалистов через портал «Госуслуги» и лицензирования их работы с помощью Федеральной службой по техническому и экспортному контролю. Реализация этих мер позволит исключить непрофессиональный подход к поиску уязвимостей электронных систем, а также снизить вероятность незаконного доступа к информации государственных организаций, крупных компаний и предприятий.

Таким образом, есть основания говорить о том, что уменьшение количества случаев несанкционированного доступа к информации происходит из-за развития технических средств ее защиты, особенно в части программного обеспечения. Впрочем, эти же обстоятельства создают предпосылки для обострения угрозы кибератак. Тем не менее компании научились эффективно противостоять наиболее распространенным формам противоправного воздействия, таким как вирусные и DDoS-атаки. Однако координирующая роль в противодействии совершаемым с использованием информационно-телекоммуникационных технологий посягательствам должна принадлежать государству [9, с. 550].

## МЕТОДЫ

В ходе исследования, результаты которого представлены в настоящей статье, применялся общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Для сбора фактического материала о способах совершения кибермошенничеств был использован метод описания; абстрагирование и обобщение были востребованы для систематизации установленных фактов и их толкования; статистический метод применен в целях изучения динамики показателей, характеризующих современное кибермошенничество, и сопутствующих данных, а также для извлечения полезной информации из полученных сведений, выявления тенденций, закономерностей и зависимостей, принятия обоснованных решений.

## РЕЗУЛЬТАТЫ

В целях реализации ключевой роли государства в противодействии посягательствам, совершаемым с использованием информационно-телекоммуникационных технологий, 15 февраля 2025 года в Государственную Думу Федерального Собрания Российской Федерации был представлен проект Федерального закона «О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации»[3] (далее – Законопроект).

[1] Эксперты зафиксировали снижение числа утечек данных в России // РБК: сайт. 20.02.2025 // URL: https://www.rbc.ru/finances/20/02/2025/67b5fb6a9a79472cf3f61553 (дата обращения: 23.02.2025).

[2] В России легализуют «белых хакеров». «Дыры» в ИТ-системах за деньги можно будет искать на законных основаниях // CNews: сайт. 27/12/2024 // URL: https://gov.cnews.ru/news/top/2024-12-27_rossijskih_belyh_hakerov?p=homecnewsmob (дата обращения: 23.02.2025).

[3] Законопроект № 842276-8 «О создании государственных информационных систем по противодействию

Данным документом предусматривается возможность онлайн-обмена информацией между органами государственной власти, банками и цифровыми платформами. Оператором системы такого онлайн-обмена должен выступать Минцифры России. В пояснительной записке к Законопроекту отмечается, что автоматический мониторинг позволит практически мгновенно выявлять подозрительные действия, блокировать их и оперативно информировать правоохранительные органы о возможных нарушениях. Кроме того, в рамках Законопроекта предусмотрены и другие инновации, направленные на защиту от противоправных действий, совершаемых с использованием информационно-телекоммуникационных технологий. Предлагается: ввести новые обязательные правила по идентификации и проверке личности пользователей услуг связи; закрепить обязательную маркировку звонков, при которой на экране устройства пользователя должно отображаться название организации, инициировавшей вызов, что поможет быстро понять, является ли звонок подлинным или исходит от злоумышленников; запретить сотрудникам органов государственной власти, финансовых организаций, операторов связи и иным специализированным субъектам общаться с гражданами посредством мессенджеров; установить запрет на передачу SIM-карт третьим лицам; ввести для граждан возможность самозапрета на заключение договоров об оказании услуг связи без личного присутствия (установить через «Госуслуги» или при обращении в МФЦ, а снять – только при личном посещении МФЦ). Предложено также запретить частным лицам и организациям использовать сервисы, которые маскируют российские телефонные номеров под иностранные.

В рамках общей политики противодействия совершаемым с использованием информационно-телекоммуникационных технологий посягательствам Центральный банк России намерен обязать все финансовые учреждения внедрить специальные инструменты («спецкнопки») для подачи жалоб от физических лиц на мошеннические действия. Кроме того, все финансовые организации должны будут предоставлять клиентам в случае обнаружения мошенничества возможность онлайн-обращения в банк и полицию посредством банковских приложений. В этих же приложениях граждане смогут отвечать на запросы банка о том, была ли какая-либо подозрительная, по мнению банка, операция мошеннической. Если запрос поступит в банк от МВД России, пользователь сможет дать ответ прямо в приложении.

Интересный опыт в сфере противодействия мошенникам накоплен не только финансовыми организациями, но и компаниями, работающими в сфере информационных технологий. Так, в 2024 году автоматический определитель номера от «Яндекс» обработал почти 1,5 миллиарда телефонных звонков, поступивших с неизвестных номеров. Из них 800 миллионов были классифицированы как нежелательные, включая мошеннические. По сравнению с 2023 годом их количество возросло на 16% [10, с. 20]. Среди наиболее распространенных предлогов для звонков, которые впоследствии были определены как нежелательные, можно выделить следующие:

1) продление договора с оператором связи (44% от общего числа зафиксированных мошеннических вызовов): злоумышленники, представляясь сотрудниками фирмы - оператора связи, сообщают о необходимости «продлить договор» и требуют предоставить код из СМС [11, с. 50];

2) двухэтапное давление на пользователя (20%): в первом звонке пользователю ясно дают понять, что с ним разговаривает мошенник, затем, во втором звонке, якобы от имени банка предлагают обезопасить счета от действий ранее звонившего злоумышленника [12, с. 53];

3) обещание оформить пособие или повысить его размер, увеличить размер пенсии или пересчитать выплаты с учетом ранее упущенного стажа или иных данных (16%) [13, с. 335];

4) предложение разблокировать аккаунт (11%), который якобы был заблокирован из-за подозрительной активности, например на портале «Госуслуги» или в программе, используемой банком [14, с. 49];

5) доставка письма из отделения почты или службы доставки (5%): в этом случае от жертвы также требуют назвать код из СМС [15, с. 459].

Специалисты компании «Яндекс», используя возможности искусственного интеллекта, разработали новые меры по противодействию мошенникам в рекламе. Компания значительно усилила защитные механизмы в этой сфере благодаря постоянно совершенствующимся ML-моделям и «YandexGPT». Теперь скорость обнаружения и блокировки нарушителей возросла в 12 раз. В 2024 году «Яндексом» было заблокировано около 300 тысяч аккаунтов, пытавшихся обойти правила рекламной политики, что на 40% больше, чем годом ранее. Ежедневно система анализирует более 230 миллионов рекламных объявлений, выявляя не только непосредственно нарушения установленных правил, но и случаи подмены контента после модерации. За попытки фишинга, включая массовые хищения данных через QR-коды, было заблокировано более трех тысяч рекламных доменов [10, с. 21].

Вопросам противодействия мошенникам как важной проблеме современности был посвящен прошедший в Екатеринбурге 19-21 февраля 2025 года Уральский форум кибербезопасности в финансах, в котором приняли участие Председатель Центрального банка России Э.С. Набиуллина и Министр цифрового развития России М.И. Шадаев. На мероприятии была представлена новая разработка российских ученых, которая, по мнению специалистов, может существенно снизить количество телефонных звонков мошенников, вплоть до полной блокировки данного вида преступной

правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // Система обеспечения законодательной деятельности: сайт // URL: https://sozd.duma.gov.ru/bill/842276-8 (дата обращения: 23.02.2025).

деятельности. Речь идет о так называемой «Фрод-рулетке» – системе, которая помогает выявлять новые методы, используемые мошенниками, отнимая у их колл-центров время, силы и ресурсы. Эта система распознает вызов от злоумышленника и автоматически перенаправляет его на специалиста, участвующего в проекте. При этом мошенник уверен в том, что общается с ни о чем не подозревающей жертвой, которую он намеревается обмануть. Для повышения эффективности этой технологии Правительство Российской Федерации планирует собирать векторы голосов людей, которые были замечены в совершении противоправных действий рассматриваемого нами вида. Полученные от органов государственной власти и участников интернет-рынка сведения будут аккумулироваться на единой антифрод-платформе. Такой разноплановый подход позволит не только противостоять современным киберугрозам, но и эффективно выявлять и раскрывать совершенные преступления, доказывать с помощью вышеназванных цифровых разработок вину мошенников для привлечения их к ответственности.

Представляется, что описанный нами комплекс организационно-управленческих, технических и правовых мер при условии его успешной реализации будет способствовать значительному повышению эффективности защиты физических и юридических лиц от кибермошенников.

**ЗАКЛЮЧЕНИЕ**

В целях противодействия кибермошенничествам, совершаемым с использованием информационно-телекоммуникационных технологий, законодателем, финансовыми организациями, коммерческими компаниями предлагается осуществление ряда эффективных мер, включая внедрение прогрессивных инноваций. Законодатель рассматривает возможность создания государственных информационных систем, онлайн-обмена сведениями между органами государственной власти, банками и цифровыми платформами, введения новых правил по идентификации и проверке личности пользователей услуг связи, маркировке звонков и др. Центральный банк России намерен обязать финансовые учреждения внедрять специализированные онлайн-инструменты для подачи физическими лицами жалоб на мошеннические действия. Кроме того, все финансовые организации, как предполагается, должны будут предоставлять клиентам возможность онлайн-обращения в банк и полицию через банковские приложения.

Компании, работающие в сфере информационных технологий, внедряют автоматические определители номеров телефонов, которые классифицируют входящие звонки как допустимые, нежелательные или мошеннические. На базе использования искусственного интеллекта и постоянно совершенствующихся ML-моделей разработаны новые меры по противодействию мошенникам в рекламе. Особого внимания заслуживает «Фрод-рулетка» – система, которая должна помогать выявлению новых способов совершения мошеннических действий, распознавать вызовы, поступающие от злоумышленников, и автоматически перенаправлять их на специалиста по кибербезопасности.

Таким образом, очевидно, что противодействие кибермошенничеству представляет собой важное для страны и требующее постоянного к себе внимания направление работы. Ключевую роль в этом процессе играет государство, так как от его своевременного реагирования на возникающие угрозы зависит не только безопасность отдельных граждан и компаний, но и национальная безопасность в целом. ■

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Милованова М.М., Шурухнов В.А. Кибермошенничество: взаимосвязь способа совершения преступления и личности преступника // Расследование преступлений: проблемы и пути их решения. 2024. № 2 (44). С. 63-71.

2. Кузнецов В.В. Управление рисками в современной платежной системе // Банковское дело. 2024. № 7. С. 34-39.

3. Москальков А.В. Виктимологическая характеристика кибермошенничества // Известия Юго-Западного государственного университета. Серия: История и право. 2024. Т. 14. № 2. С. 107-118.

4. Кабанов П.А. Криминальная виктимность несовершеннолетних от имущественной киберпреступности: анализ статистических показателей и перспективы формирования ювенальной кибервиктимологии // Виктимология. 2024. Т. 11. № 3. С. 359-366.

5. Карпасюк И.В., Карпасюк А.И., Давидюк Н.В., Чертина Е.В. Формализация процедуры выявления личностных характеристик потенциальной жертвы кибермошенничества // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2024. № 2. С. 77-84.

6. Орлова Л.В., Саламон В.Ю. Кибермошенничество как сдерживающий фактор развития безналичных платежей // Тенденции развития науки и образования. 2024. № 115-5. С. 122-127.

7. Долотова Н.П. Киберпреступность в банковской сфере в Российской Федерации // Гуманитарные, социально-экономические и общественные науки. 2024. № 12. С. 215-219.

8. Мамаева Д.Ч., Рудакова О.С. Кибермошенничество: угрозы и защита в цифровом мире // Финансовые рынки и банки. 2024. № 12. С. 132-135.

9. Алексеева А.П. Профилактика правонарушений в России: законодательные основы и перспективы реализации // Преступность, уголовная политика, уголовный закон. Сборник научных трудов. Саратов: Саратовская государственная юридическая академия, 2013. С. 549-551.

10. Яджин Н.В. Некоторые способы совершения мошеннических действий с использованием сети «Интернет» // Вестник Тюменского института повышения квалификации сотрудников МВД России. 2024. № 1 (22). С. 18-22.
11. Соколов А. Кибермошенничество. Актуальные схемы и меры противодействия // Наука и Техника. 2024. № 3. С. 50-51.
12. Евтушенко И.И. Предупреждение виктимизации дистанционных хищений и сферы его воздействия // Виктимология. 2024. Т. 11. № 1. С. 43-56.
13. Каширин К.Д., Куровский С.В., Мишин Д.А., Блащинский С.А., Чумакова А.А. Разработка и внедрение антифродовых систем в банках // Финансовые рынки и банки. 2024. № 6. С. 333-336.
14. Таков А.З. Некоторые вопросы противодействия совершению киберпреступлений // Юридическая наука и практика. 2025. № 1. С. 48-50.
15. Лукошкин А.А. Цифровая безопасность личности в условиях развития цифрового права // Образование и право. 2024. № 2. С. 459-466.

**REFERENCES**

1. Milovanova M.M., Shurukhnov V.A. Kibermoshennichestvo: vzaimosvyaz' sposoba soversheniya prestupleniya i lichnosti prestupnika // Rassledovaniye prestupleniy: problemy i puti ikh resheniya. 2024. № 2 (44). S. 63-71.
2. Kuznetsov V.V. Upravleniye riskami v sovremennoy platezhnoy sisteme // Bankovskoye delo. 2024. № 7. S. 34-39.
3. Moskal'kov A.V. Viktimologicheskaya kharakteristika kibermoshennichestva // Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo. 2024. T. 14. № 2. S. 107-118.
4. Kabanov P.A. Kriminal'naya viktimnost' nesovershennoletnikh ot imushchestvennoy kiberprestupnosti: analiz statisticheskikh pokazateley i perspektivy formirovaniya yuvenal'noy kiberviktimologii // Viktimologiya. 2024. T. 11. № 3. S. 359-366.
5. Karpasyuk I.V., Karpasyuk A.I., Davidyuk N.V., Chertina Ye.V. Formalizatsiya protsedury vyyavleniya lichnostnykh kharakteristik potentsial'noy zhertvy kibermoshennichestva // Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravleniye, vychislitel'naya tekhnika i informatika. 2024. № 2. S. 77-84.
6. Orlova L.V., Salamon V.Yu. Kibermoshennichestvo kak sderzhivayushchiy faktor razvitiya beznalichnykh platezhey // Tendentsii razvitiya nauki i obrazovaniya. 2024. № 115-5. S. 122-127.
7. Dolotova N.P. Kiberprestupnost' v bankovskoy sfere v Rossiyskoy Federatsii // Gumanitarnyye, sotsial'no-ekonomicheskiye i obshchestvennyye nauki. 2024. № 12. S. 215-219.
8. Mamayeva D.Ch., Rudakova O.S. Kibermoshennichestvo: ugrozy i zashchita v tsifrovom mire // Finansovyye rynki i banki. 2024. № 12. S. 132-135.
9. Alekseyeva A.P. Profilaktika pravonarusheniy v Rossii: zakonodatel'nyye osnovy i perspektivy realizatsii // Prestupnost', ugolovnaya politika, ugolovnyy zakon. Sbornik nauchnykh trudov. Saratov: Saratovskaya gosudarstvennaya yuridicheskaya akademiya, 2013. S. 549-551.
10. Yadzhin N.V. Nekotoryye sposoby soversheniya moshennicheskikh deystviy s ispol'zovaniyem seti «Internet» // Vestnik Tyumenskogo instituta povysheniya kvalifikatsii sotrudnikov MVD Rossii. 2024. № 1 (22). S. 18-22.
11. Sokolov A. Kibermoshennichestvo. Aktual'nyye skhemy i mery protivodeystviya // Nauka i Tekhnika. 2024. № 3. S. 50-51.
12. Yevtushenko I.I. Preduprezhdeniye viktimizatsii distantsionnykh khishcheniy i sfery yego vozdeystviya // Viktimologiya. 2024. T. 11. № 1. S. 43-56.
13. Kashirin K.D., Kurovskiy S.V., Mishin D.A., Blashchinskiy S.A., Chumakova A.A. Razrabotka i vnedreniye antifrodovykh sistem v bankakh // Finansovyye rynki i banki. 2024. № 6. S. 333-336.
14. Takov A.Z. Nekotoryye voprosy protivodeystviya soversheniyu kiberprestupleniy // Yuridicheskaya nauka i praktika. 2025. № 1. S. 48-50.
15. Lukoshkin A.A. Tsifrovaya bezopasnost' lichnosti v usloviyakh razvitiya tsifrovogo prava // Obrazovaniye i pravo. 2024. № 2. S. 459-466.

*Авторы заявляют об отсутствии конфликта интересов.*
*Авторами внесён равный вклад в написание статьи.*
*The authors declare no conflicts of interests.*
*The authors have made an equal contribution to the writing of the article.*


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