УДК 338

***В.Ю. Циклаури, Л.В. Афанасьева***
Юго-Западный государственный университет, г. Курск,
email: vika-ts@mail.ru, lv_af@mail.ru

# КИБЕРПРЕСТУПНОСТЬ В РОССИИ: НОВЫЙ ВЫЗОВ ДЛЯ ОБЩЕСТВА И ГОСУДАРСТВА

**Ключевые слова:** киберпреступность, новая угроза современного мира, экономическая безопасность; противодействие киберпреступной деятельности.

Сегодня современный мир можно охарактеризовать стремительным развитием информационных отношений, информационно-коммуникационных и робототехнических технологий, глобального киберпространства, социальных информационных сетей и когнитивных технологий, а также тотальной компьютеризацией человеческого общества. Однако высокие технологии несут обществу не только блага, но и различные проблемы социально-негативного характера. Одной из таких проблем для современного российского общества выступает компьютерная преступность или киберпреступность. Киберпреступность – новая угроза современного мира, причем стоит признать, что этот вид преступности представляет реальную угрозу не только отдельным организациям, физическим лицам, но и государствам, их национальной безопасности и суверенитету. Цель исследования заключается в изучении стремительного роста киберпреступной деятельности в Российской Федерации, и разработка, с учетом изученных научных позиций, организационно-управленческих и технических мер противодействия компьютерной преступности. Задачи исследования: сформулировать характерные черты, способы совершения и проблемные вопросы при исследовании киберпреступлений; определить ключевые факторы, способствовавшие возникновению негативной ситуации: к числу которых автором были отнесены: низкий уровень цифровой грамотности населения; недостаточно эффективное противодействие киберпреступной деятельности (несовершенство антифрод-инфраструктуры – комплекса технологий и программного обеспечения, разработанного для противодействия киберпреступной деятельности). Киберпреступность становится одной из наиболее серьезных проблем современного российского общества, наносящей огромный урон российской экономике и благосостоянию граждан. Проблема киберпреступности – сложная проблема, которая требует комплексного решения с активным участием различных заинтересованных сторон: государственных органов, коммерческих и некоммерческих организаций, научного сообщества. В исследовании применен обширный комплекс научных подходов (абстрактно-логический, дедуктивный, комплексный и системный). При помощи диалектического метода познания, предопределяющего изучение экономических явлений в их взаимосвязи и развитии осуществлялась реализация процесса исследования. Для решения отдельных задач применялись экономико-статистические методы, методы сравнения, абсолютных, относительных и средних величин, графического и табличного представления данных.

***V.Y. Tsiklauri, L.V. Afanasyeva***
South-Western State University, Kursk, email: vika-ts@mail.ru, lv_af@mail.ru

# CYBERCRIME IN RUSSIA: A NEW CHALLENGE FOR SOCIETY AND THE STATE

**Keywords:** cybercrime, a new threat to the modern world, economic security; countering cybercrime.

The modern world is characterized by the rapid development of information relations, information and communication and robotic technologies, global cyberspace, social information networks and cognitive technologies, as well as the total computerization of human society. However, high technologies bring not only benefits to society, but also various problems of a socially negative nature. One of such problems for the world community and modern Russian society is computer crime. Cybercrime is a new threat to the modern world, and it is worth recognizing that this type of crime poses a real threat not only to individual organizations, individuals, but also to states, their national security and sovereignty. The purpose of the study is to study the current state of cybercrime activity, the rapid growth of which is noted in the Russian Federation, and to develop, taking into account the studied scientific positions, organizational, managerial and technical measures to counter computer crime. The key factors that significantly contributed to the emergence of a negative situation are also formulated: the low level of digital literacy of the population against the background of the digitalization process, accelerated and deepened during the COVID-19 pandemic; insufficiently effective counteraction to cybercrime activities (insufficient level of competence on the part of law enforcement agencies, imperfection of the anti-fraud infrastructure – a complex of technologies and software developed by to counter cybercrime). Cybercrime is becoming one of the most serious problems of modern Russian society, causing huge damage to the Russian economy and the welfare of citizens. The problem of cybercrime is a complex problem that requires a comprehensive solution with the active participation of various stakeholders: government agencies, commercial and non—profit organizations, and the scientific community. The study uses an extensive set of scientific approaches (abstract-logical, deductive, complex and systematic). With the help of the dialectical method of cognition, which determines the study of economic phenomena in their interrelation and development, the implementation of the research process was carried out. To solve individual problems, economic and statistical methods, methods of comparison, absolute, relative and average values, graphical and tabular representation of data were used.

Цифровизация – один из основополагающих процессов современности. Пандемия COVID-19 существенным образом повлияла на поведение и привычки людей, на то, как люди используют технологии. Прямо сейчас мы можем наблюдать оформление глобального цифрового мира, в который инвестируется все больше ресурсов в виде инфраструктуры, денег, технологий, идей и человеческого времени, и который обособляется от мира физического. В выборе между физическим и цифровым миром современный человек все чаще отдает предпочтение последнему: удаленная работа и онлайн-конференции, использование соцсетей для общения и получения информации, рост электронной коммерции.

Вместе с тем по мере становления нового цифрового мира одной из главных его характеристик становятся хрупкость и неустойчивость. Сюда можно отнести как глобальные сбои, которые затрагивают миллиарды людей по всей планете , так и феномен киберпреступности.

## Цель исследования

Главной целью работы является изучение киберпреступной деятельности в Российской Федерации, и разработка, с учетом изученных научных позиций, организационно-управленческих и технических мер противодействия компьютерной преступности.

## Материалы и методы

Информационную базу исследования составили статистические данные Российской Федерации.

В исследовании применен комплекс общенаучных подходов (абстрактно-логический, дедуктивный, комплексный и системный). Реализация процесса исследования осуществлялась при помощи диалектического метода познания, предопределяющего изучение экономических явлений в их взаимосвязи и развитии. Для решения отдельных задач применялись экономико-статистические методы, методы сравнения, абсолютных, относительных и средних величин, графического и табличного представления данных, корреляционно-регрессионный анализ.

## Результаты и их обсуждение

«Киберпреступление» – термин иностранного происхождения. Как отмечается, в Оксфордском словаре кибер (cyber) определяется как: «относящийся к компьютерам, информационным технологиям, виртуальной реальности» [1, с. 35]. Наряду с термином «киберпреступления», ученые используют такие категории как: «преступления в сфере информационных технологий», «информационные преступления», сетевые компьютерные преступления, интернет-преступления.

Стоит признать, что этот вид преступности представляет реальную угрозу не только отдельным организациям, физическим лицам, но и государствам, их национальной безопасности и суверенитету. Киберпреступники становятся все более профессиональными и изощренными, они получают огромные доходы. Только за 2020 г. россияне перевели мошенникам около 150 млрд рублей [2]. По заявлениям зампреда Сбербанка, ущерб российской экономике от киберпреступлений может достичь 6 трлн рублей к началу 2022 г. [3], это около 5,6% от ВВП страны за 2020 г. [4].

Прогнозы экспертов по мировой экономике также неутешительны: согласно отчету Cybersecurity Ventures, в ближайшие несколько лет глобальный урон от киберпреступности будет расти на 15% ежегодно и составит 10,5 триллионов долларов США к 2025 г. [5]. Эксперты компании подчеркивают, что киберпреступность – один из главных вызовов, с которым человечество столкнется в ближайшие десятилетия.

Рассматривая признаки киберпреступлений исследователями называется несколько характерных ее черт (рисунок 1).

Представляется необходимым дополнить данный перечень указанием на умышленный характер действий, так как при совершении киберпреступления лицо осознает общественную опасность деяния, предвидит наступления вредных для общества или отдельного лица последствий и желает наступления этих последствий, либо относится к ним безразлично. Киберпреступления исключают совершение их по небрежности или легкомыслию.

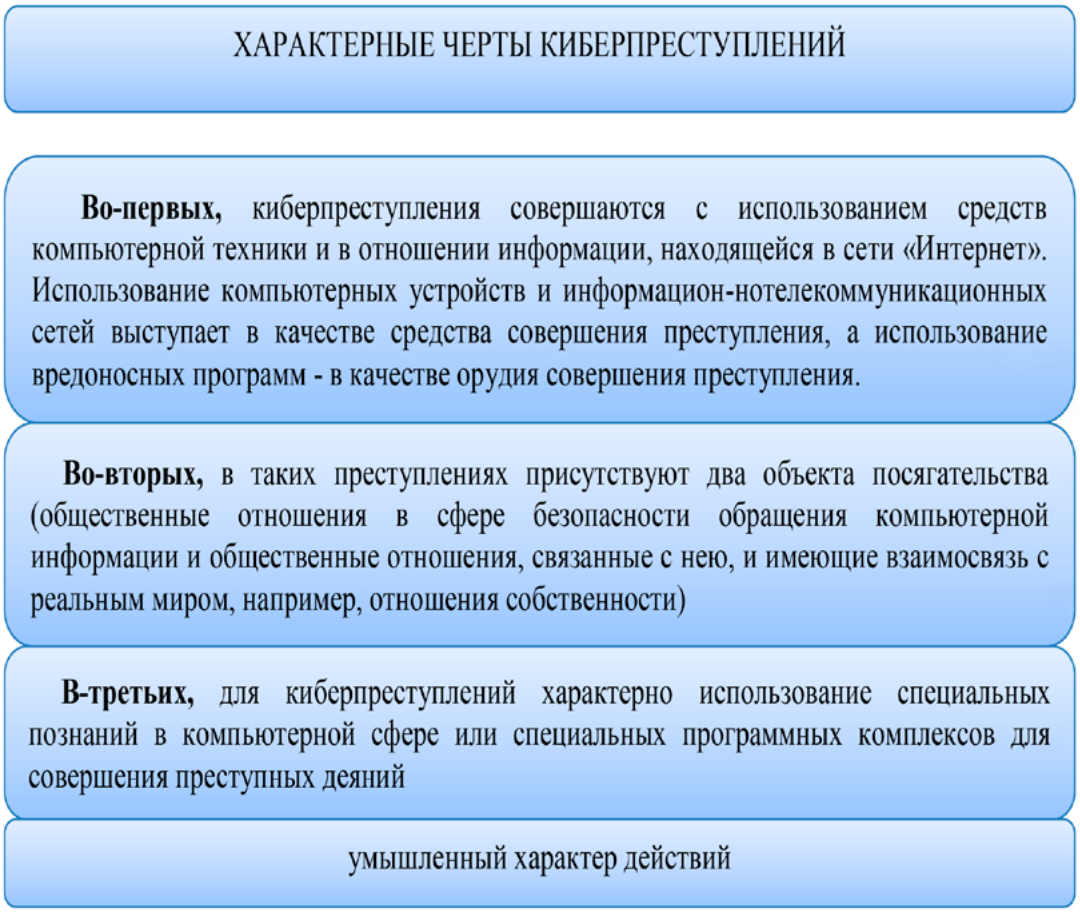


*Рис. 1. Характерные черты киберпреступлений*

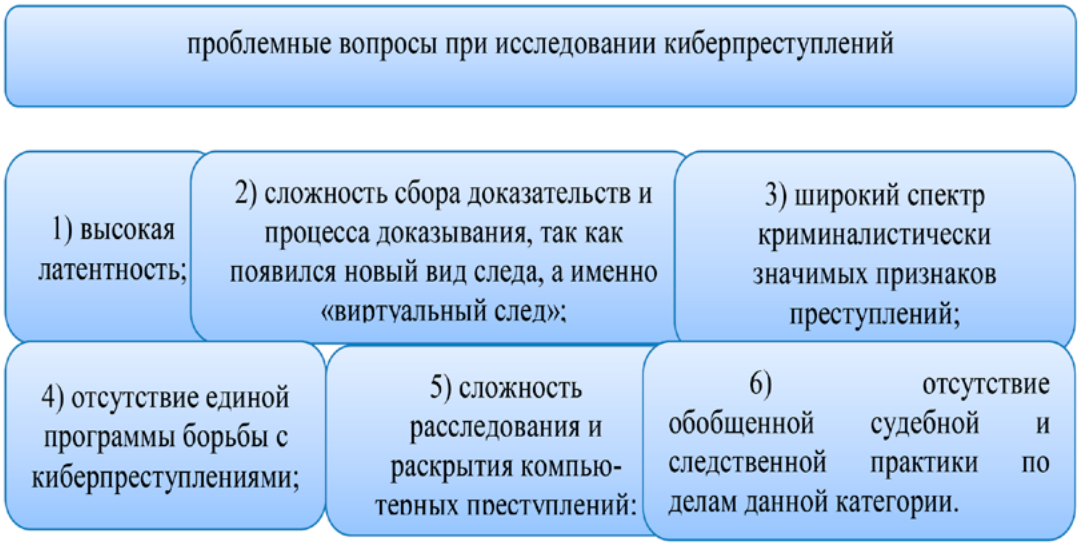


*Рис. 2. Проблемные вопросы при исследовании киберпреступлений*

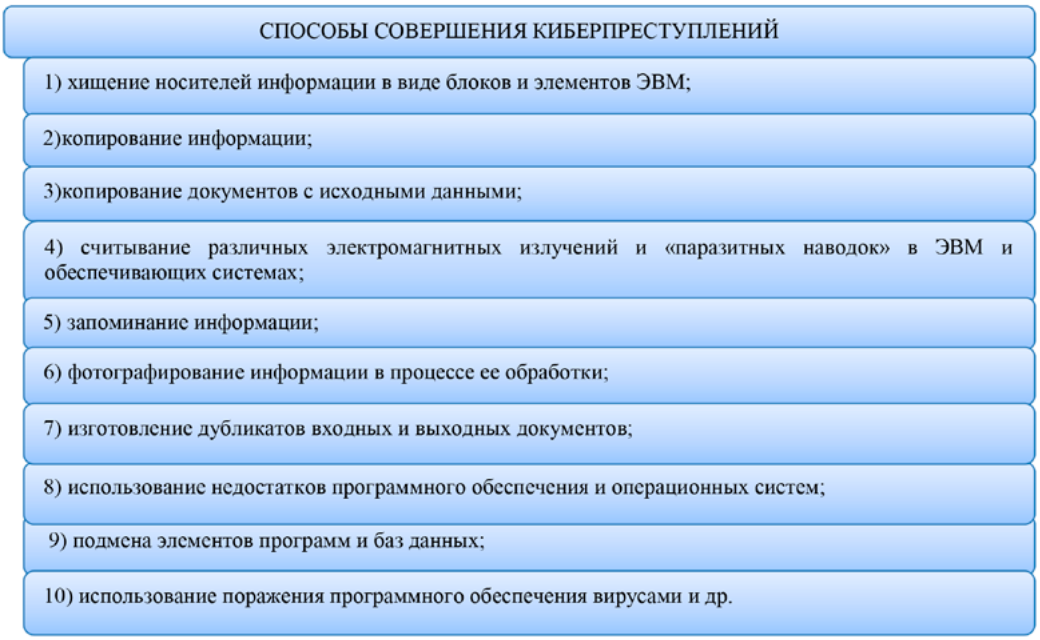


*Рис. 3. Способы совершения киберпреступлений*

**Таблица 1**

Кодификатор компьютерных преступлений, разработанный зарубежными учеными

| Код группы | Расшифровка |
|---|---|
| QA | Несанкционированный доступ и перехват |
| QD | Изменение компьютерных данных |
| QF | Компьютерное мошенничество |
| QR | Незаконное копирование |
| QS | Компьютерный саботаж |
| QZ | Прочие компьютерные преступления |

**Таблица 2**

Полномочия отдела «К»

| Преступление | Статья |
|---|---|
| борьба с нарушением авторских и смежных прав | ст. 146 УК РФ, ст. 7.12 КоАП РФ |
| выявление незаконного проникновения в компьютерную сеть | ст. 272 УК РФ |
| борьба с распространителями вредоносных программ | ст. 273 УК РФ |
| выявление нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети | ст. 274 УК РФ |
| выявление использования подложных кредитных карт | ст. 159.3 УК РФ |
| кража с банковского счета | ст. 158 УК РФ |
| неправомерный оборот электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств | ст. 187 УК РФ |
| борьба с распространением порнографии посредством сети Интернет | ст. 242 УК РФ |
| выявление незаконного подключения к телефонным линиям | ст. 165 УК РФ, ст. 13.2 КоАП РФ |
| борьба с незаконным оборотом радиоэлектронных и специальных технических средств | ст. 138 УК РФ, ст. 171 УК РФ, ст. 14.1, 14.42 КоАП |

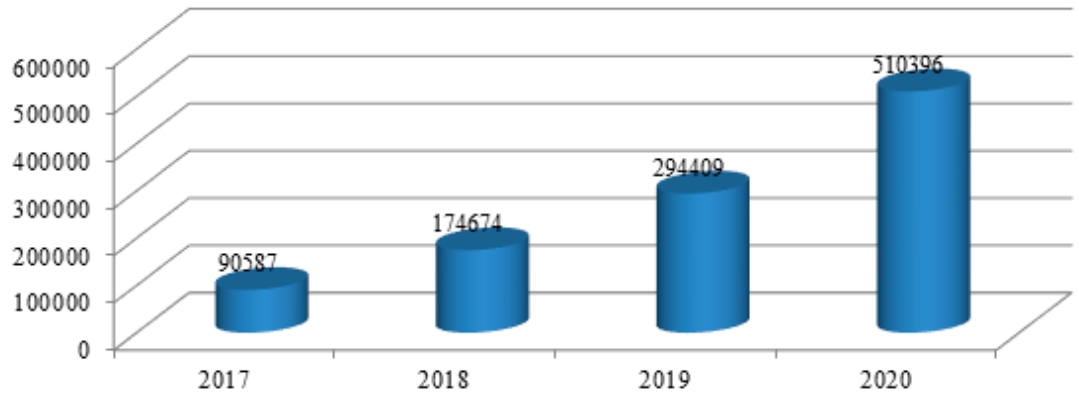


*Рис. 4. Количество официально зарегистрированных преступлений в 2017–2020 гг., совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации*

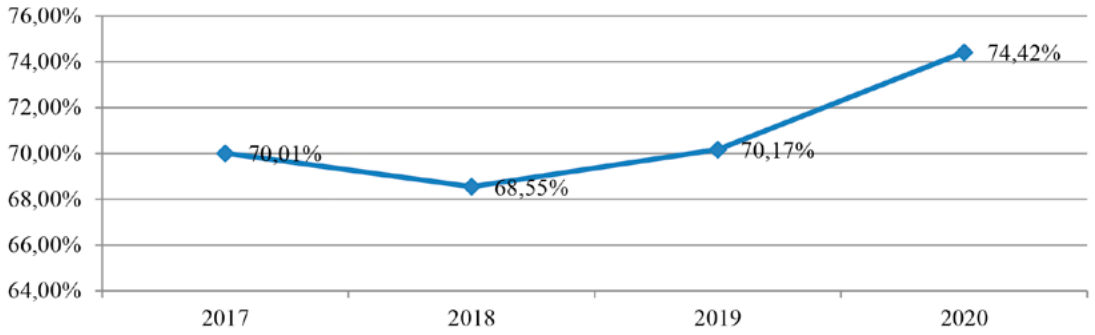


*Рис. 5. Доля нераскрытых киберпреступлений относительно всех зарегистрированных преступлений в 2017–2020 гг.*

Основная особенность, отличающая киберпреступления от иных противоправных деяний, заключается в использовании компьютерных технологий и сети Интернет при совершении преступления. Компьютер или компьютерная сеть играют в данном случае ведущую роль [6].

Актуальность борьбы с данным видом преступности, а также расследование и раскрытие, имеют приоритетное значение для государства, но ввиду его специфичности возникают проблемы исследования особенностей киберпреступлений.

При исследовании особенностей преступлений в сфере информационных технологий можно выделить ряд проблемных вопросов.

Для решения обозначенных проблем необходимо выделить криминалистически значимые элементы характеристики киберпреступлений: способ совершения преступления; особенности следовой информации; особенности обстановки совершения преступления (место совершения преступления, время совершения преступления и др.); личностная характеристика преступника; особенности непосредственного предмета преступного посягательства.

Отметим, что мы живем в непростое время. Пандемия COVID-19 изменила весь мир, а также изменила и киберпреступления, кибербезопасность и все киберпространство. До COVID-19 фиксировалось порядка 350 000 новых массовых кибератак в день, но сейчас выявляется порядка 400 000. Активность киберпреступников возросла примерно на 20–25%. По нашему мнению, пандемия открыла киберпреступникам новые возможности.

В криминалистической литературе можно встретить множество классификаций способов совершения компью-

терных преступлений, вот некоторые их них. Крылов В.В. приводит описание возможных способов нарушения конфиденциальности и целостности компьютерной информации без их классификации.

Разработкой классификации способов совершения компьютерных преступлений занимаются и зарубежные ученые. Так рабочей группой Интерпола разработана и встроена в автоматизированную поисковую информационную систему запросов следующий кодификатор компьютерных преступлений (таблица 1).

Далее по каждому коду, дается обширный перечень способов совершения компьютерных преступлений.

В Российской Федерации существует специальный отдел «К», который занимается противодействием киберпреступности и преступлениям, связанным с нелегальным оборотом РЭС (радиотехнических средств) – см. табл. 2.

Чтобы проиллюстрировать общие тенденции развития киберпреступности в России, построим график, показывающий количество официально зарегистрированных преступлений в 2017–2020 гг. (Рисунок 4)

Представленные данные свидетельствуют о стабильно высоком росте количества регистрируемых киберпреступлений в последние годы в России. Данные МВД пока не предоставляет, но по всей видимости, в 2021 г. повышательный тренд сохранится.

Одна из самых важных характеристик киберпреступности в России – это низкий процент раскрываемости (Рисунок 5).

Доля нераскрытых киберпреступлений не только остается на стабильно высоком уровне – в районе 70%, но и демонстрирует рост в последние три года, несмотря на активную деятельность российских государственных органов и организаций.

Прямо сейчас мы наблюдаем мощную волну цифровизации преступной деятельности, активное использование технологий при совершении противоправных действий. При совершении преступления посредством киберпространства можно говорить, что применена новая совокупность приемов, методов, последовательность действий, которая придает преступлению уникальные свойства, не характерные для преступлений без использования сети. Представляется, что в такой трактовке совершение преступления посредством Интернет, сама сеть является и способом преступления, и в то же время информационное пространство является средством как совокупность предметов и процессов материального мира. Такое двойственное значение информационного пространства при совершении преступления возможно благодаря его природе, которое является одновременно набором принципов, алгоритмов, правил взаимодействий и в то же время оно реализовано в материальном мире в виде совокупности соединенных компьютеров.

Перечислим ключевые факторы, которые, по нашему мнению, способствовали возникновению негативной ситуации с состоянием киберпреступности в стране. Во-первых, дисбаланс между темпами цифровизации в России и ростом уровня цифровых компетенций граждан страны. Масштабы цифровизации в России велики: например, на 2020 г. пришелся рекорд по количеству выданных банковских карт, активное использование безналичных способов оплаты, рост аудитории соцсетей и их активности.

Наряду с этим сохраняется низкий уровень компетенций россиян в сфере цифровых технологий: согласно исследованию остается неизменным количество россиян с продвинутым уровнем цифровых компетенций – 27%. Авторы подчеркивают, что многие граждане до сих пор обладают недостаточными знаниями и навыками в сфере информационных технологий, необходимыми для безопасного использования цифровых продуктов.

Во-вторых, недостаточный уровень эффективности противодействия киберпреступной деятельности: недостаточный уровень компетенций со стороны правоохранительных органов, несовершенство антифрод-инфраструктуры. Проблема подчеркивается в том числе и высшим руководством правоохранительных органов. Так, начальник Главного управления международноправового сотрудничества Генпрокуратуры РФ сообщил, что правоохранительные органы отстают от киберпреступников в техническом обеспечении и инструментах связи.

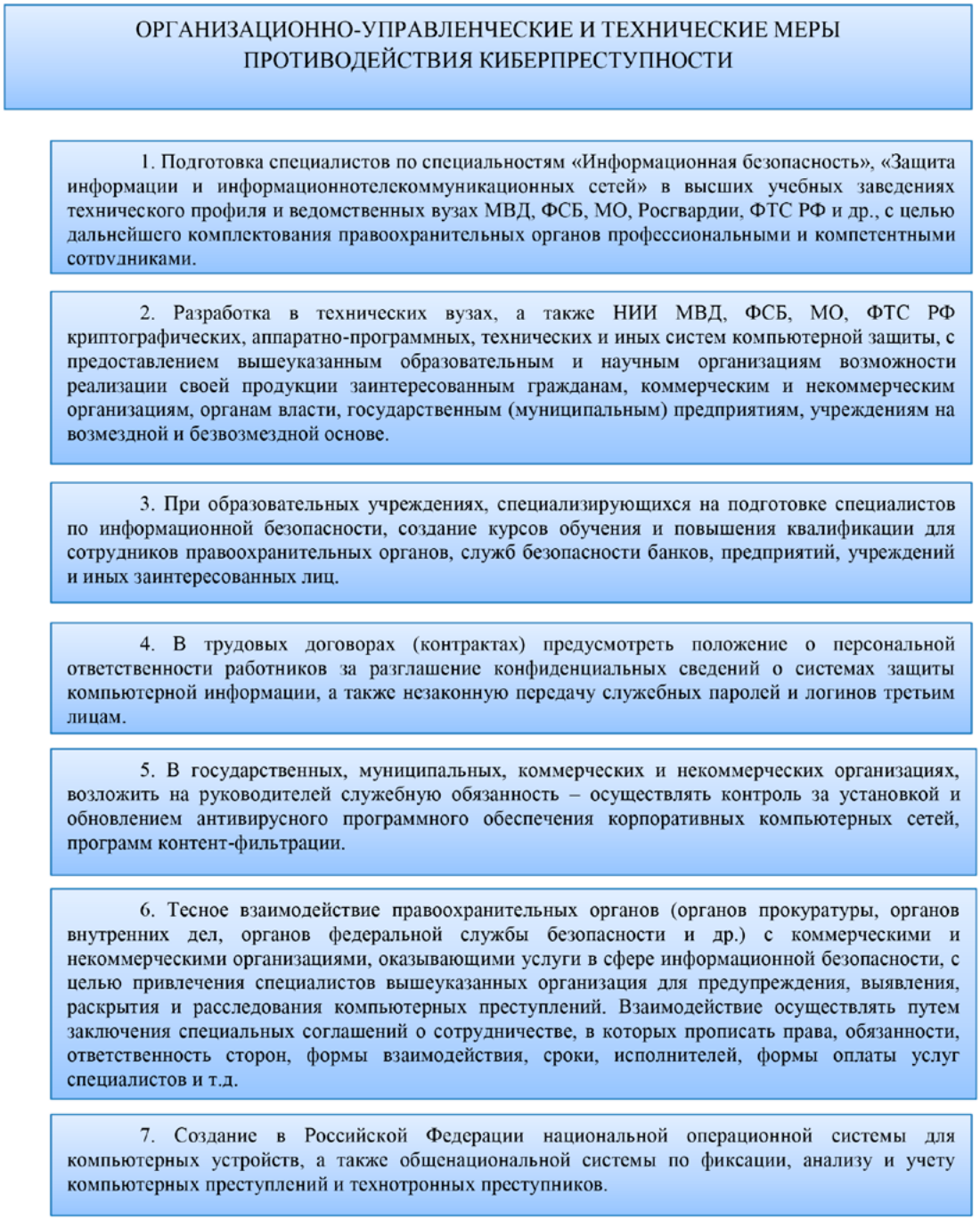


*Рис. 6. Организационно-управленческие и технические меры противодействия киберпреступности*

Источник: составлено автором на основании источника [8]

Следствием недостаточного уровня компетенций правоохранительных органов становится достаточно низкий процент раскрываемости киберпреступлений.

С учетом изученных научных позиций, автор предлагает следующие организационно-управленческие и технические меры противодействия компьютерной преступности.

Анализ проблемных вопросов противодействия компьютерной преступности позволяет автору предложить следующие специальные криминалистические меры.

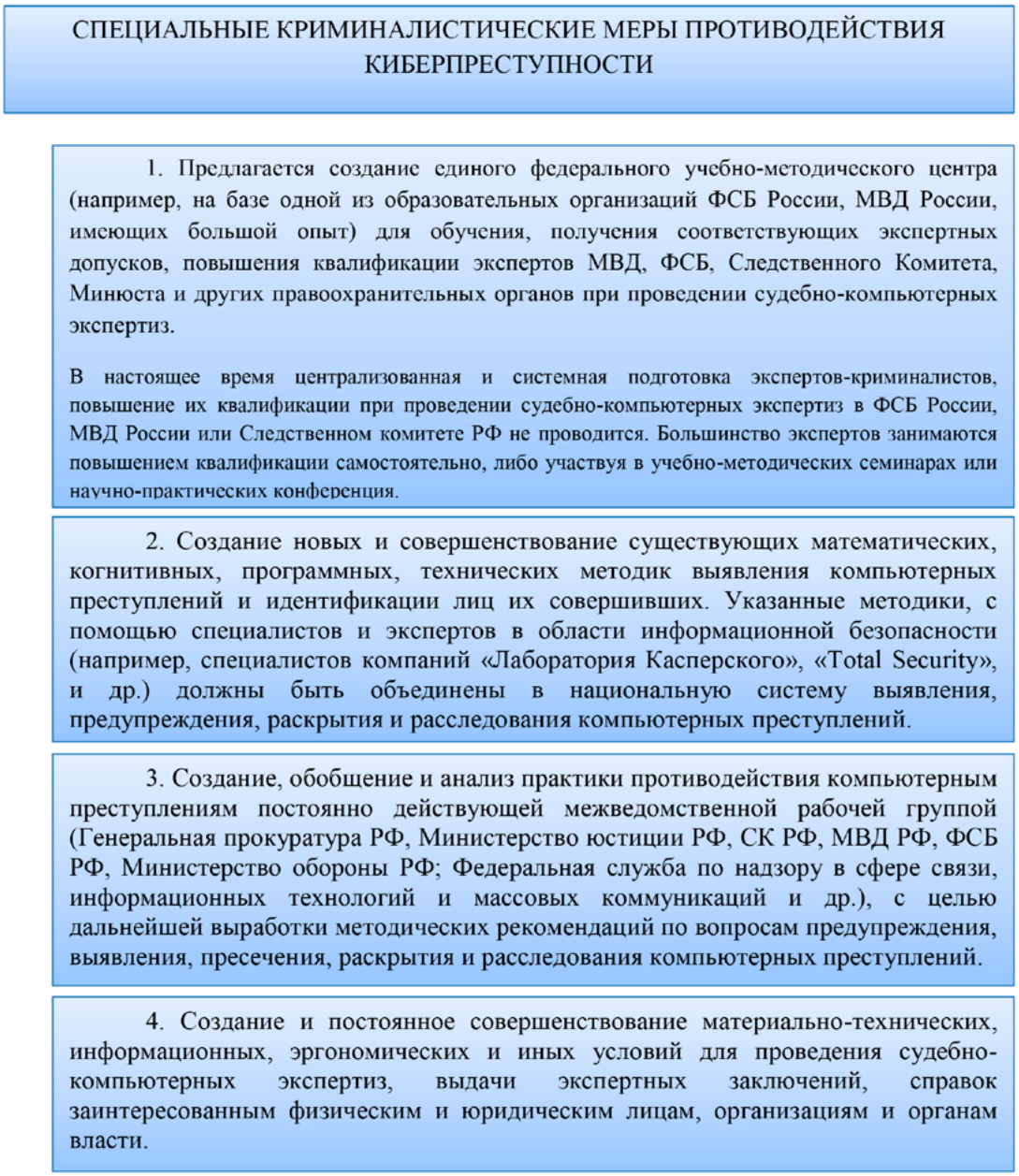


*Рис. 7. Специальные криминалистические меры противодействия киберпреступности*

Источник: составлено автором на основании источника [8]

Система специальных мер по противодействию компьютерной преступности, предложенная автором, не является полной и исчерпывающей. Она может быть дополнена с учетом различных объективных и субъективных факторов, влияющих на развитие российского технотронного общества (применение «облачных» и «туманных» технологий, искусственного интеллекта, создание «цифровой» экономики, использование электронного документооборота в органах власти, коммерческих и некоммерческих организациях; предоставление «цифровых» государственных и муниципальных услуг, распространение робототехники в производственной и бытовой сферах; кардинальное изменение информационного законодательства и т.д.), должна носить комплексный, разносторонний и многоуровневый характер.

Пандемия COVID-19 и вынужденная форсированная цифровизация в России в связи с самоизоляцией послужили лишь катализаторами тех проблем, которые формировались на протяжении нескольких лет до начала «коронакризиса». Сегодня, когда о проблеме кибермошенничества говорят уже повсюду, важно сначала замедлить, а впоследствии остановить высокие на текущий момент темпы прироста новых случаев киберпреступлений. По нашему мнению, для решения этой комплексной, сложной и многогранной проблемы требуется масштабная и долгосрочная кооперативная работа государственных и правоохранительных органов, коммерческих и некоммерческих организаций, научного сообщества, активное взаимодействие с международными партнерами. Для эффективного противодействия виртуальным преступникам необходима многоуровневая институциональная система кибербезопасности, которая защищала бы и простых граждан, и государственные институты. Сейчас становится очевидным, что киберпреступность – это не просто проблема, а вызов всему российскому обществу, который требует незамедлительного и жесткого ответа.

*Библиографический список*

1 Ефремова М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Право и кибербезопасность. 2014. № 2. С. 33-38.

2 Не пойман – не разговор // Коммерсантъ. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4627498 (дата обращения: 26.04.2022).

3 Потери экономики РФ от кибератак оценили в 6 трлн руб. // Вести.ру [Электронный ресурс]. URL: https://www.vesti.ru/finance/article/2585133 (дата обращения: 26.04.2022).

4 Федеральная служба государственной статистики. [Электронный ресурс]. URL: https://rosstat.gov.ru (дата обращения: 01.05.2022).

5 Cybercrime To Cost The World $10.5 Trillion Annually By 2025. [Электронный ресурс]. URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (дата обращения: 26.04.2022).

6 Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25-33.

7 Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4 (13). С. 58-61.

8 Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. … докт. юрид. наук. Москва, 2021.