Оригинальная статья
УДК 316.35.023.6
https://doi.org//1999-9836_2023_19_4_11_616_629
EDN ZICJKA

Проблема киберпреступности в России: актуальное состояние и перспективы решения

Швыряев Павел Сергеевич
аспирант, факультет государственного управления, Московский государственный университет им. М.В. Ломоносова, Москва, Россия
(ShvyryaevPS@spa.msu.ru)

Аннотация
Статья посвящена исследованию актуального состояния проблемы киберпреступности в России. Проведено качественное социологическое исследование: опрос экспертов, занимающихся изучением проблемы киберпреступности. Исследование было направлено на то, чтобы получить экспертную оценку актуального состояния киберпреступности в России: выявление причин ухудшения ситуации в стране с проблемой киберпреступности; определение наиболее эффективных стратегий решения данной проблемы. Среди наиболее опасных особенностей киберпреступности экспертами были отмечены её латентный характер; нарастание масштаба и актуальности проблемы, её переход в угрозу национального масштаба; низкая эффективность расследования киберпреступлений правоохранительными органами; усиление экономического и социального ущерба от киберпреступлений; снижение порога входа и приобщения к киберпреступному сообществу; оформление киберпреступности как полноценной индустрии. Предложенные экспертами меры для решения проблемы можно объединить в следующие ключевые направления: более масштабная, глубокая и системная работа с населением по повышению осведомлённости, цифровой грамотности и образованности; модернизация правоохранительных органов, которые оказались не готовы к быстрому переходу преступности в цифровой сектор; более тесное международное сотрудничество, необходимость которого вытекает из трансграничной природы киберпреступности; решение проблемы дефицита высококвалифицированных кадров для всей российской ИТ-отрасли; выделение дополнительного финансирования на проекты по борьбе с киберпреступностью; эффективное и оперативное взаимодействие правоохранительных органов, банков и операторов связи для блокировки мошеннических ресурсов и номеров; совершенствование российского законодательства в сфере информационных технологий; более глубокая поддержка российских стартапов и инициатив в области информационной безопасности и просвещения населения.

Ключевые слова: цифровизация, киберпреступность, экспертный опрос, цифровая грамотность, правоохранительные органы

Для цитирования: *Швыряев П.С.* Проблема киберпреступности в России: актуальное состояние и перспективы решения // Уровень жизни населения регионов России. 2023. Том 19. № 4. С. 616–629. https://doi.org/10.52180/1999-9836_2023_19_4_11_616_629; EDN ZICJKA

RAR (Research Article Report)
https://doi.org//1999-9836_2023_19_4_11_616_629
EDN ZICJKA

The Problem of Cybercrime in Russia: Current State and Prospects for Solution

Pavel S. Shvyryaev
Postgraduate student, School of Public Administration, Lomonosov Moscow State University, Moscow, Russia
(ShvyryaevPS@spa.msu.ru)

Abstract
The article is devoted to the study of the current state of the problem of cybercrime in Russia. A qualitative sociological study was conducted: a survey of experts involved in the study of the problem of cybercrime. The study was aimed at obtaining an expert assessment of the current state of cybercrime in Russia; identifying the reasons for the deterioration of the situation in the country with the problem of cybercrime; determining the most effective strategies for solving this problem. Among the most dangerous features of cybercrime, experts noted its latent nature; increasing scale and relevance of the problem, its transition to a threat on a national scale; low efficiency of investigation of cybercrimes by law enforcement agencies; increased economic and social damage from cybercrime; lowering the threshold for entry and joining the cybercriminal community; establishing cybercrime as a full-fledged industry. The measures proposed by experts to solve the problem can be combined into the following key areas: larger, deeper and more systematic work with the population to increase awareness, digital literacy and education; modernization of law enforcement agencies, which were not ready for the rapid transition of crime to the digital sector; closer international cooperation, the need for which arises from the cross-border nature of cybercrime; solving the problem of shortage of highly qualified personnel for the entire Russian IT industry; providing additional funding for projects to combat cybercrime; effective and prompt interaction between law enforcement agencies, banks and telecom operators to block fraudulent resources and numbers; improvement of Russian legislation in the field of information technology; deeper support for Russian startups and initiatives in the field of information security and public education.

Keywords: digitalization, cybercrime, expert survey, digital literacy, law enforcement agencies

For citation: Shvyryaev PS. The Problem of Cybercrime in Russia: Current State and Prospects for Solution. *Uroven' zhizni naseleniya regionov Rossii=Living Standards of the Population in the Regions of Russia.* 2023;19(4):616–629. (in Russ.) https://doi.org/10.52180/1999-9836_2023_19_4_11_616_629

Введение

Киберпреступность – одна из главных угроз для человечества в XXI веке. Киберпреступность и киберпреступления становятся актуальными угрозами в сфере безопасности человека, общества и государства [1, с. 141], одним из самых распространённых экономических преступлений во всём мире [2, с. 90]. Это неотъемлемый спутник цифровизации, негативная и крайне опасная сторона технологического развития. По мере нарастания масштабов технологической трансформации, проблема киберпреступности вставала всё более остро и в конечном итоге приобрела черты глобальной угрозы для всего человечества, наносящей ущерб мировой экономике, национальной безопасности, социальной стабильности и личным интересам [3, с. 2]. Киберпреступность становится одной из наиболее серьёзных проблем современного российского общества, наносящей огромный урон российской экономике и благосостоянию граждан [4, с. 553].

События во время пандемии показали, что глобальная система безопасности оказалась не готова к серьёзным трансформационным изменениям. Кибербезопасность стала серьёзной проблемой во время пандемии [5, с. 220]. Оказалась не готова и социальная система: резкий переход в онлайн привычной общественной жизни стал вызовом для значительной части населения планеты, чем оперативно воспользовались кибермошенники. Рост числа киберпреступлений в масштабах всей планеты – яркое проявление назревших проблем. Волна киберпреступности захлестнула и нашу страну [6, с. 145]. Потребность в аудите системы безопасности назрела и в России, которая столкнулась с беспрецедентным давлением в период пандемии и геополитической нестабильности 2022–2023 годов. Как в новых реалиях обеспечить цифровую стабильность и устойчивое развитие российской экономики и общества в целом?

В настоящий момент это один из ключевых вопросов, которым задаются российские управленцы, исследователи и лица, принимающие решения. Интерес к данной проблематике находит своё отражение и в научной литературе. Исследованием проблемы киберпреступности занимаются криминологи, юристы, виктимологи, психологи, экономисты, философы, специалисты в области международных отношений и представители других дисциплин. Исследование киберпреступности как социального феномена представителями социологической науки – только зарождающееся направление. В рамках этого направления можно выделить труды Комлева Ю.Ю. [7], Карповой Д.Н. [8], Сергеева А. Ю. и Широковой О. В. [9], Тимофеева А.В. и Комолова А.А. [10], Старостенко О.А. [11] и ряда других авторов.

Цель исследования: на основании результатов экспертного опроса выявить ключевые факторы, которые, по мнению опрошенных экспертов, оказывают влияние на состояние киберпреступности в России.

Достижение поставленной цели потребовало решения следующих задач:

1. Выявить оценку опрошенными экспертами актуального состояния киберпреступности в России.

2. Выявить ключевые факторы, которые, по мнению опрошенных экспертов, оказывают влияние на состояние киберпреступности в России.

3. Выявить оценку опрошенными экспертами эффективности реализуемой стратегии в области борьбы с киберпреступностью.

Объект исследования – киберпреступность в России.

Предмет исследования – факторы, оказывающие влияние на состояние киберпреступности в России.

Гипотеза исследования: актуальные стратегии борьбы с киберпреступностью требуют пересмотра и корректировки с учётом и глубоким пониманием социальной природы киберпреступности.

Существующие стратегии противодействия киберпреступности показали ограниченность своего применения и низкую степень эффективности. Эти стратегии в большинстве своём – ответная реакция на сложившуюся ситуацию, попытки минимизировать последствия, а не понять и ликвидировать причину. В последние годы, с ростом проблемы киберпреступности, сформировался отчётливый тренд на ужесточение законодательства за совершения преступных деяний в цифровой среде. Об этом заявляли эксперты[1], данная политика реализуется через принятие соответствующих законопроектов[2]. Но какова эффективность таких законотворческих мер в условиях, когда правоохранительные органы отстают от киберпреступников в техническом обеспечении и инструментах связи[3], а источник атак нередко находится за пределами государства[4]? Более того, законодательство не успевает за стремитель-

[1] Необходимо ужесточить ответственность за киберпреступления – эксперты // Российская газета: [сайт]. URL: https://rg.ru/2021/08/05/neobhodimo-uzhestochit-otvetstvennost-za-kiberprestupleniia-eksperty.html (дата обращения: 16.07.2023).

[2] Президент подписал закон о конфискации имущества у киберпреступников // Interfax: [сайт]. URL: https://www.interfax.ru/russia/906019 (дата обращения: 16.07.2023).

[3] ГП: правоохранительные органы отстают в технических возможностях от киберпреступников // ТАСС: [сайт]. URL: https://tass.ru/politika/8915711 (дата обращения: 16.07.2023).

[4] ФСБ сообщила об участии Пентагона в кибератаках против России // Известия: [сайт] URL: https://iz.ru/1497823/2023-04-13/fsb-soobshchilo-ob-uchastii-pentagona-v-kiberatakakh-protiv-rossii (дата обращения: 16.07.2023).

ным развитием информационных технологий [12, с. 98]. О каком эффективном противодействии с помощью законодательных инициатив можно говорить, когда правовая система не регламентирует актуальное состояние взаимоотношений в цифровой среде? Насколько целесообразно в таком случае ужесточение законодательства, если процент раскрываемости киберпреступлений сохраняется в России на низком уровне? Или же ситуация не столь линейна и требует иных, более глубоких и проработанных мер?

Таким образом, события пандемии и ускоренной цифровизации продемонстрировали высокую степень актуальности проблемы киберпреступности по двум основным причинам. Во-первых, существует потребность в том, чтобы углубить понимание социальной природы киберпреступности. Во-вторых, существующие методы и стратегии противодействия киберпреступности всё ещё ограничены по эффективности, что ставит вопрос о разработке комплексного подхода к борьбе с киберпреступностью.

Основные теоретические и методологические положения. Актуальное состояние киберпреступности в России и перспективы решения проблемы. Экспертный опрос

Для углубления анализа сложившейся в России и мире ситуации с киберпреступностью, а также оценки возможностей и ограничений различных стратегий противодействия данной проблеме обратимся к опыту исследователей и практиков. Важно подчеркнуть, что заявленные в рамках опроса мнения экспертов – это субъективные оценки конкретных исследователей. Однако это не отменяет важности и ценности общения с экспертами и исследователями киберпреступности.

Обратимся к результатам экспертного опроса, который был проведён в формате дистанционного интервью в июле-августе 2023 года. В рамках данного исследования было проведено 17 экспертных интервью с представителями следующих организаций (в скобках указаны должности экспертов):

1. МИРЭА – Российский технологический университет (доцент кафедры государственного и административного права).

2. Институт государства и права Российской академии наук (старший научный сотрудник сектора уголовного права, уголовного процесса и криминологии).

3. Финансовый университет при Правительстве РФ (младший научный сотрудник Департамента информационной безопасности).

4. Уральский юридический институт МВД России (кандидат юридических наук, сотрудник института).

5. Московский государственный технический университет им. Н.Э. Баумана (Доктор юридических наук, профессор, академик РАЕ, профессор кафедры юриспруденции, интеллектуальной собственности и судебной экспертизы).

6. Байкальский государственный университет (кандидат юридических наук, доцент кафедры уголовного права и криминологии).

7. Санкт-Петербургский юридический институт (аспирант кафедры уголовного права, криминологии и уголовно-исполнительного права).

8. Краснодарский университет МВД России (первый эксперт – доцент кафедры уголовного права и криминологии, кандидат юридических наук; второй эксперт – адъюнкт, лейтенант полиции РФ).

9. Московский финансово-промышленный университет «Синергия» (кандидат философских наук, доцент).

10. Иркутский юридический институт Академии Генеральной прокуратуры РФ (доцент кафедры государственно-правовых дисциплин Иркутского юридического института (филиала) Академии Генеральной прокуратуры РФ, кандидат юридических наук).

11. Институт социально-экономических проблем народонаселения Федерального научно-исследовательского социологического центра Российской академии наук (кандидат экономических наук, старший научный сотрудник).

12. Юридический институт Вятского государственного университета (доцент кафедры уголовного права, процесса и национальной безопасности, кандидат юридических наук).

13. Казанский инновационный университет им. В.Г. Тимирясова (директор НИИ противодействия коррупции, доцент, доктор юридических наук).

14. Московский Государственный Университет им. М.В. Ломоносова (аспирант кафедры социологии управления).

15. Омский государственный технический университет (доцент кафедры государственного и муниципального управления и таможенного дела, кандидат юридических наук).

16. Челябинский государственный университет (доцент кафедры уголовно-правовых дисциплин, кандидат юридических наук).

Экспертная выборка включает как исследователей-теоретиков проблемы киберпреступности, так и практиков: бывших следователей, которые непосредственно работали в сфере расследования киберпреступлений, а также в образовательных учреждениях по подготовке специалистов для расследова-

ния в том числе и преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Была разработана дорожная карта глубинного интервью (Приложение А), которое включает 4 блока вопросов по следующим темам:

1. Состояние киберпреступности в России.
2. Причины сложившейся ситуации.
3. Стратегии решения проблемы.
4. Заключительный блок.

Первый блок вопросов направлен на то, чтобы определить позицию эксперта по поводу актуального состояния киберпреступности в России: ключевые тренды, степень внимания со стороны государства, главный объект воздействия, возможные прогнозы на ближайшие 2–3 года.

Вопросы второго блока направлены на определение позиции эксперта по поводу причин сложившейся ситуации: ключевые факторы усугубления проблемы, эффективность государственной политики и правоохранительных органов, оценка влияния санкционного давления с 2022 года и прочих факторов.

Вопросы третьего блока направлены на то, чтобы выяснить отношения экспертов к реальным и потенциальным стратегиям решения проблемы, их возможностям и ограничениям.

Четвёртый блок предоставляет возможность эксперту в свободной форме изложить своё мнение по тем вопросам, которые не прозвучали ранее в ходе интервью.

Результаты исследования: экспертный опрос

Оценивая актуальное состояние киберпреступности в России, практически все эксперты отмечают актуальность данной проблемы, её рост в последние годы и фиксацию показателей на высоких уровнях по состоянию на 2023 год. Один из экспертов отметил, что в России фактически упустили нарастающую проблему, которая активно формировалась в течение последних нескольких лет. Другой эксперт на основании большого опыта работы в правоохранительных органах заявил, что, по его мнению, официальная статистика лишь отчасти отражает действительность, но не передаёт фактического масштаба проблемы. Это объясняется как особенностями классификации преступлений внутри российской правоохранительной системы, так и латентностью как характерной чертой такого рода преступлений. Жертва далеко не всегда может осознавать факт совершённого в отношении неё преступления, либо не заявлять об этом в полицию[5]. Тем не менее, даже с учётом некоторых сложностей с систематизацией и классификацией преступлений, эксперты отмечают отчётливый тренд на стабильное увеличение количества киберпреступлений в России. Отмечается и возросшее количество кибератак, в том числе и на критическую инфраструктуру России, которые совершаются из-за рубежа. Стоит отметить, что повышение защищённости критической информационной инфраструктуры и устойчивости её функционирования – одно из основных направлений обеспечения информационной безопасности страны, провозглашённое в Доктрине информационной безопасности Российской Федерации[6].

Резкое усугубление проблемы киберпреступности в России в последние годы всё чаще поднимает вопрос о том, является ли в настоящий момент киберпреступность угрозой национальной безопасности. Этот вопрос обсуждается в научных и общественных кругах, средствах массовой информации. О важности данной проблемы заявляют высшие государственные лица страны. Вопрос о том, является ли в настоящий момент проблема киберпреступности угрозой национальной безопасности России, был задан экспертам. И больше 70% процентов опрошенных (12 из 17 экспертов) дали утвердительный ответ. Эксперты подчёркивают, что в данном вопросе важно больше не состояние в моменте, а ухудшающийся тренд: правоохранительные органы не успевают за злоумышленниками, не успевает и законодательство, масштабы угрозы постоянно растут, а процент раскрываемости всё ещё остаётся низким. Ряд экспертов высказали важную мысль о том, что в глобальном смысле проблема заключается в том, что российская громоздкая и инертная система принятия и исполнения решений не отвечает вызовам со стороны киберпреступности – очень быстрого и адаптивного врага, который быстро находит уязвимости этой системы и активно их эксплуатирует.

Далее экспертам был задан вопрос о том, в чём они видят главную опасность киберпреступности. Наиболее популярный ответ – это латентный характер киберпреступности. Проблема обнаружения и пресечения несанкционированного доступа в цифровую систему – одна из главных и наиболее актуальных в сфере компьютерной безопасности. Результаты расследований инцидентов показывают, что уязвимость в цифровой системе может довольно продолжительное время находиться в «спящем» режиме и совсем не эксплуатироваться до определённого момента. Резкий всплеск количества утечек в России

[5] Киберпреступность в домашних тапочках // Ведомости: [сайт]. URL: https://www.vedomosti.ru/opinion/articles/2018/10/17/783976-kiberprestupnost (дата обращения: 24.07.2023).

[6] Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

в 2022 году на фоне усиления международной конфронтации – характерный пример влияния внешних событий на состояние цифровой безопасности в целом государстве. Латентный характер киберпреступлений неразрывно связан с проблемой эффективности расследования киберпреступлений, на что особое внимание обращали бывшие следователи и преподаватели академий МВД России.

Неподконтрольность закономерностей развития технологий в общем и киберпреступности в частности – ещё одна важная опасность для человечества, которая делает затруднённым прогнозирование процесса цифровизации и попытки его урегулирования. Развитие технологий – сложный процесс, который включает в себя огромное количество факторов. В таких условиях высока вероятность появления трудно прогнозируемых событий, так называемых «чёрных лебедей», которые могут иметь разрушительные последствия для всей системы. В качестве серьёзной опасности киберпреступности эксперты отмечают и всё более заметный экономический и социальный ущерб, который за последние 4 года вырос более чем втрое[7]. Снижающийся порог входа в преступную индустрию – ещё одна важная проблема, которую отметили эксперты. Если ещё 30 лет назад киберпреступность была занятием наиболее талантливых и продвинутых знатоков в области информационных технологий (так называемых «хакеров»), то в настоящее время, в век высокой доступности интернета и устройств связи, порог входа в преступную индустрию сильно снижен. Например, для совершения преступных деяний в социальных сетях или звонков потенциальным жертвам не требуется каких-либо специальных знаний или умений: это, по сути, классические мошеннические операции одних людей в отношении других, совершаемые с использованием цифровых инструментов коммуникации. Низкий порог входа приводит к формированию полноценной индустрии киберпреступности, на что обратил внимание один из экспертов. Существуют полноценные нелегальные компании со своими офисами, оборудованием, системами найма и мотивации, которые занимаются незаконной киберпреступной деятельностью. Развитие данной индустрии – повод обратить на неё пристальное внимание как со стороны правоохранителей, так и общественности.

Ещё одна серьёзная опасность киберпреступности, о которой рассказали эксперты, – это низкая эффективность расследования киберпреступлений. И если в расследовании относительно простых преступлений, не требующих высокой технической и исследовательской подготовки, эксперты отмечают положительную динамику, то в расследовании преступлений, совершённых злоумышленниками среднего и высокого уровня, ситуация складывается негативно. В процессе интервью эксперты, которые имеют непосредственный опыт работы в правоохранительных органах, перечислили целый ряд проблем, которые не позволяют российским правоохранительным органам эффективно бороться с новыми вызовами со стороны киберпреступного сообщества и оставляют их в отстающей позиции. К ключевым причинам низкой эффективности российской правоохранительной системы эксперты отнесли низкую мотивацию сотрудников, прежде всего материальную; низкий уровень подготовки слушателей академий, проблемы с повышением квалификации действующих сотрудников; отсутствие стандартизированного формата коммуникации правоохранительных органов с операторами мобильной связи и банками по обмену информацией; административно-территориальные барьеры при обмене информацией между регионами; проблемы в материально-техническом обеспечении; недоукомплектованность профильными ИТ-специалистами, которые должны работать в тесной связке со следователями. Все эти проблемы имеют системный характер и требуют системного решения, исходящего прежде всего от лиц, принимающих решения. Однако, как отметили некоторые эксперты, серьёзных подвижек в данном направлении до сих пор нет, несмотря на опыт пандемии. В 2022–2023 годах Россия столкнулась с новой, опасной волной киберпреступности, исходящей уже преимущественно из-за границы, которая направлена не только на граждан, но и на объекты критической инфраструктуры. С учётом как российской специфики, так и общемирового тренда роста киберпреступности, вопрос модернизации российской правоохранительной системы встаёт всё острее, по мнению экспертов. На примере последних нескольких лет можно было убедиться, что правоохранительная система с методами и подходами прошлого века малоэффективна против вызовов XXI века, в том числе и киберпреступности.

Наряду с низкой эффективностью правоохранительной системы эксперты отметили быстроту реакции и принятия решений со стороны преступного сообщества: происходит постоянный процесс тестирования новых преступных схем и их масштабирование на большое количество потенциальных жертв. В таких условиях как правоохранительные органы, так и законодательная

[7] Интернет несёт потери // Ведомости: [сайт] URL: https://www.vedomosti.ru/importsubstitution/new_technologies/articles/2023/03/14/966290-internet-neset-poteri (дата обращения: 06.08.2023).

база и инструменты информирования населения не всегда успевают за появлением новых способов мошенничества. Данная проблема вновь поднимает вопрос о выработке комплексного подхода к непрерывной, эффективной профилактике совершения киберпреступлений, что отмечалось некоторыми экспертами.

Принципиально не изменит ситуацию и ужесточение законодательства в отношении правонарушителей, считают эксперты. Один из экспертов ёмко сформулировала бесперспективность данного направления. «*На мой взгляд, важно не ужесточение наказания в законодательстве, а неотвратимость ответственности. Тогда, когда за киберпреступления неизбежно будет следовать наказание, даже не самое жестокое, это будет более эффективной мерой, чем повышение санкций за него.*» Такую позицию нельзя не поддержать. Какой эффект будет иметь закон[8] о конфискации имущества киберпреступника, если он будет уверен в том, что его не смогут обнаружить? А в плане эффективности расследования киберпреступлений у российских правоохранительных органов остаются серьёзные проблемы, которые, в отличие от принятия нового закона, может потребовать фундаментального переустройства всей правоохранительной системы.

Среди ключевых трендов последних лет в области киберпреступлений наиболее популярный ответ – рост доли социальной инженерии. Действительно, в последние годы отмечается глобальный «поворот» от технологии к человеку – самому слабому звену системы. И эффективное средство решения данной проблемы до сих пор не найдено, поскольку для абсолютно любого человека свойственны ошибки, когнитивные искажения или проявления эмоций. Использование социальной инженерии здесь можно охарактеризовать как эксплуатацию природных человеческих уязвимостей.

Практически половина экспертов (7 из 17) отметили неготовность системы безопасности России к росту киберпреступности в России на фоне пандемии и после её окончания. Однако даже те эксперты, которые считают, что ситуация остаётся под контролем, отмечают тенденции к её ухудшению. По мнению экспертов, полной гарантии защиты от киберугроз сегодня не может дать ни одна структура в стране. На фоне усиления защиты государственной системы эксперты отмечают незащищённость рядовых граждан, что привело к значительному росту совершения киберпреступлений и атак в отношении них как в период пандемии, так и на фоне обострения геополитической обстановки в 2022–2023 годах. Один из экспертов отметил, что проблемы безопасности в настоящий момент зачастую решаются государством «по остаточному принципу». Другой эксперт высказал позицию о том, что система безопасности России не могла быть готова к росту киберпреступности. А сам скачок киберпреступлений – это «*вспышка преступности в резко изменившихся социальных условиях*».

На вопрос о том, уделяется ли проблеме киберпреступности достаточное внимание со стороны органов государственной власти, ряд экспертов отметили низкую способность системы работать на опережение и предупреждать потенциальные киберугрозы. Эксперты подчёркивают, что несмотря на довольно широкую законодательную базу, которая включает в себя Доктрину информационной безопасности Российской Федерации[9], федеральные законы «Об информации, информационных технологиях и о защите информации»[10], «О персональных данных»[11], Федеральный закон «О техническом регулировании»[12] и другие, заявления официальных лиц различного уровня о важности проблемы, реализуемая в настоящий момент политика борьбы с киберпреступностью имеет значительный потенциал к росту, что отметили несколько экспертов. И реализовать этот потенциал можно через повышение эффективности раскрытия киберпреступлений правоохранительными органами, а также через повышение профилактики киберпреступлений: в ряде случаев киберпреступление целесообразнее предупредить, чем ликвидировать последствия. Сотрудники академий МВД подчеркнули, что несмотря на то, что проблему низкой раскрываемости киберпреступлений констатировали ещё в 2020 году, более трёх лет назад, каких-либо фундаментальных изменений в данном вопросе до сих пор нет: проблема обучения следователей и привлечения квалифицированных ИТ-специалистов в правоохранительные органы остаётся острой.

Оценивая эффективность российских правоохранительных органов в борьбе с киберпреступностью, 11 экспертов отметили её неэффективность или низкую степень эффективности. Один из экспертов прямо отметил, что сегодня «*правоохранительные органы практически ничем не могут помочь гражданам*». Другой эксперт выразил

[8] У киберпреступников будут конфисковывать незаконно полученное имущество // ТАСС: [сайт]. URL: https://tass.ru/obschestvo/17995469 (дата обращения: 08.08.2023).

[9] Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

[10] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

[11] Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».

[12] Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».

слабую надежду на сформированное в сентябре 2022 года управление по борьбе с киберпреступностью[13]. Несколько экспертов также подчеркнули, что при анализе эффективности правоохранительных органов важно ранжировать киберпреступников по уровню и степени их профессионализма: если в вопросе расследования условно простых преступлений, совершённых не профессиональными злоумышленниками без специальных средств связи и программного обеспечения, можно отметить положительную динамику, то в вопросах расследования киберпреступлений, совершённых профессионалами высокого уровня, сохраняются серьёзные сложности.

Каким образом могут повлиять отмеченные экспертами проблемы на дальнейший характер развития киберпреступности в стране на горизонте 2–3 лет? 11 из 17 экспертов прогнозируют дальнейшее усугубление проблемы: рост числа киберпреступлений на фоне сохраняющейся низкой раскрываемости. Один из экспертов прогнозирует ежегодный рост числа совершаемых киберпреступлений на 15–20 процентов; рост количества приостанавливаемых производством дел по причине неустановления лиц, подлежащих привлечению к уголовной ответственности; снижение количества преступников, привлекаемых к уголовной ответственности; использование технологий DeepFake для совершения преступлений. Другой эксперт также отмечает, что ситуация с проблемой киберпреступности будет усугубляться на фоне сохраняющейся замедленной реакции со стороны органов безопасности, которые и дальше не будут успевать за новыми трендами и схемами совершения преступлений в цифровой среде. Третий эксперт отметил, что в ближайшие 2–3 года общее количество кибератак увеличится минимум на 30 процентов, при этом атаки всё чаще будут хорошо организованы группировками или отдельными хакерами. Один из экспертов при ответе на этот вопрос отметил важность характера развития технологий, в том числе искусственного интеллекта: *всё более активное внедрение ИИ в преступную деятельность, в частности, Chat GPT уже сейчас позволяет маскировать безграмотность некоторых «компьютерных преступников»*. Внимание на проблему искусственного интеллекта обратил и другой эксперт, подчеркнув, что преступники уже сейчас активно осваивают ИИ и продолжат это делать для совершения противозаконных деяний. Учитывая, что предугадать развитие искусственного интеллекта и последствия этого развития сложно, проблеме использования искусственного интеллекта в преступных целях должно быть уделено важное внимание со стороны исследователей, практиков-разработчиков, лиц, принимающих решения. Таким образом, киберпреступления с использованием искусственного интеллекта – ещё одно важное направления для исследования в рамках общей проблемы киберпреступности.

Второй блок вопросов направлен на раскрытие тех причин, которые, по мнению экспертов, лежат в основе становления и развития проблемы киберпреступности в стране. Общий тезис можно свести к тому, что рост киберпреступности в последние годы – это общемировой тренд и связан с ускоренной цифровизацией и легкодоступностью технологий, однако это не отменяет причин, которые усугубили ситуацию в стране. К таким причинам эксперты относят низкую цифровую грамотность населения, отток квалифицированных ИТ-кадров, отсутствие стандартов безопасности компьютерных программ, несовершенство правоохранительной системы, влияние недружественных стран и иных внешних факторов, изменения на программном и аппаратном рынке на фоне санкционного давления и курс на импортозамещение. Один из экспертов отметил ряд правовых причин, которые представляют собой несовершенства российского уголовного, гражданского и административного законодательства. В качестве иллюстрации эксперт привёл следующие примеры: «*не урегулирован вопрос оценки ущерба, причиненного компьютерными правонарушениями и преступлениями, а также то, какими критериями должен руководствоваться суд при определении размера ущерба и его возмещения виновными лицами*». Отмечается и недостаточная проработанность концепции информационной безопасности: «*отсутствие правовой регламентации ответственности должностных лиц за определённые сферы экономической, в том числе хозяйственной, а также общественной жизни конкретных государственных и общественных институтов*».

Экспертам был предложен вопрос о том, какие ключевые решения могли быть предприняты для недопущения столь стремительного ухудшения ситуации в последние несколько лет. Предлагаемые экспертами решения можно разбить на несколько ключевых блоков.

1. Более масштабная, глубокая и системная работа с населением по повышению осведомлённости, цифровой грамотности и образованности. Цифровая грамотность – важный элемент достижения состояния информационной безопасности [13, с. 123]. В России важной задачей в рамках данного направления является устранение дисбаланса между темпами цифровизации в стране и

[13] В МВД создано управление по борьбе с киберпреступностью // Коммерсантъ: [сайт]. URL: https://www.kommersant.ru/doc/5592758 (дата обращения: 30.07.2023).

ростом уровня цифровых компетенций граждан [14, с. 191]. Один из экспертов предложил введение специальных курсов по информационной гигиене на уровне общего, специального и высшего образования. Другие эксперты отметили важность постоянной работы с населением как одной из базовых составляющих профилактики предупреждения киберпреступлений. Ещё один эксперт описал высокую грамотность населения как «прививку от киберпосягательств». «*Сформированная на необходимом уровне цифровая грамотность станет не только одним из столпов эффективного противодействия, но и особой «вакциной», не позволяющей развиваться вирусу. Когда сам организм борется с вирусом. Я бы назвала это «прививкой от киберпосягательств».*

2. Модернизация правоохранительных органов, которые оказались не готовы к быстрому переходу преступности в цифровой сектор. Один из экспертов отметил ряд шагов, которые могли бы повысить эффективность правоохранителей в расследовании киберпреступлений: «*увеличение штатной численности подразделений Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России, введение специализации в следственных подразделениях и районных судах по данному направлению, установление данным сотрудникам дополнительных надбавок к должностным окладам «за сложность и напряжённость», повышение квалификации сотрудников органов предварительного расследования по данному направлению на системной основе*». Отсутствие централизованного процесса обучения и повышения квалификации сотрудников правоохранительных органов отметил и другой эксперт, непосредственно работающий в академии МВД. Также эксперты отметили и сохраняющиеся проблемы с кадрами: российская правоохранительная система испытывает кадровый голод, особенно в области высококвалифицированных ИТ-специалистов, ключевой задачей которых и должна быть борьба с киберпреступностью на стороне государственной власти. С учётом вышесказанного, важно особое внимание уделять совершенствованию обучения сотрудников, формированию компетенций у каждого выпускника ведомственных образовательных организаций [15, с. 67]. Актуальной остаётся задача развития киберполиции, которая обусловлена складывающимися на современном этапе правоотношениями и отвечает потребностям информационного общества [16, с. 78].

3. Более тесное международное сотрудничество, необходимость которого вытекает из трансграничной сущности киберпреступности. При этом при рассмотрении вопросов взаимодействия государств в целях противодействия киберпреступности можно выделить два важных аспекта: 1) официальное международное сотрудничество, в том числе выдача (экстрадиция) и оказание взаимной правовой помощи; 2) неофициальное сотрудничество [17, с. 678]. Один из экспертов, имеющий опыт работы в правоохранительных органах, отметил, что тесное взаимодействие российских правоохранителей с их коллегами из других стран по линии Интерпола для расследования киберпреступлений так и не было установлено. Если в вопросах традиционных преступлений, совершаемых в физическом мире, обмен информацией активно происходил, то в вопросах расследования киберпреступлений взаимодействие было минимально. Несмотря на то, что в 2022 году Россия не была исключена из Интерпола, наложенные ограничения могут ещё сильнее затруднить взаимодействие между спецслужбами, в том числе и по расследованию киберпреступлений. Санкционное давление и накладываемые ограничения со стороны «недружественных» стран характеризуются экспертами как неблагоприятные в вопросе решения проблемы киберпреступности в стране. Один из экспертов подчеркнул, что «*международное сотрудничество играет важную роль не только для обмена опытом противодействия киберпреступлениям, но и для принятия совместных мер, в том числе правовых, преследующих указанные цели. Тем более, как уже отмечалось, такие преступления выходят за пределы границ отдельного государства, а значит и вопрос юрисдикции может быть не решён или вызывать проблемы при отсутствии договорённостей между странами, отражённых в международных документах*».

4. Решение проблемы дефицита высококвалифицированных кадров как для всей российской ИТ-отрасли для построения надёжных и устойчивых к проникновению цифровых систем, так и в правоохранительных органах для эффективного расследования совершённых преступлений и проведения профилактических мероприятий. В 2022 году российское государство столкнулось с масштабной, серьёзной волной отъезда квалифицированных кадров, в том числе и ИТ-специалистов [18, с. 238]. Несколько экспертов подчеркнули, что в решении проблемы киберпреступности кадры имеют ключевое, основополагающее значение, и в этом вопросе у России сохраняются серьёзные проблемы. Один из экспертов подчеркнул серьёзность проблемы оттока квалифицированных ИТ-кадров не только в моменте, но и на долгосрочную перспективу, что может внести свой негативный вклад

в перспективные технические разработки в области кибербезопасности.

5. Выделение дополнительного финансирования на проекты по борьбе с киберпреступностью. Особо эксперты подчёркивали проблему в правоохранительных органах, где система материального поощрения не позволяет привлекать и удерживать перспективных, квалифицированных специалистов. Эксперты отметили и недостаточное финансирование в рамках федеральных проектов и инициатив, направленных на борьбу с киберпреступностью в России.

6. Эффективное и оперативное взаимодействие правоохранительных органов, банков и операторов связи для блокировки мошеннических ресурсов и номеров. Эксперты подчёркивают, что положительные решения в данном вопросе были приняты с сильным запозданием: лишь в 2021 году на эту проблему обратил внимание президент страны[14]. Тем не менее, один из экспертов в ходе интервью отметил сохранение проблемы по состоянию на середину 2023 года: в регионах формат взаимодействия между правоохранительными органами и операторами связи может строиться не на формальных предписаниях, а на основании личных знакомств и предпочтений, что имеет свои негативные последствия, которые приобретают системный характер.

7. Совершенствование российского законодательства в сфере информационных технологий. Один из экспертов отметил необходимость *«полного обновления норм, регулирующих сеть «Интернет»*. Уголовно-правовые составы действующего российского законодательства, предусматривающие ответственность за рассматриваемые преступления, не адаптированы к новым видам преступных посягательств, совершаемых в области информационно-коммуникационных технологий [19, с. 101]. Существует необходимость детально проработать национальное законодательство и международные акты, предусматривающие ответственность за совершение киберпреступлений [20, с. 320].

8. Более глубокая поддержка российских стартапов и инициатив в области информационной безопасности и просвещения населения. Активная интеграция российской коммерческой экспертизы в государственные органы, правоохранительные институты.

Но были ли решения, подобные предлагаемым экспертами, предприняты и эффективно реализованы государством? Эксперты отметили, что в некоторых вопросах можно выделить отдельные эффективные решения, которые могут иметь положительный, но ограниченный эффект, и такие, которые не способствуют изменению ситуации в целом. Такие меры, по мнению экспертов, имеют запоздалый характер и не способны в корне переломить ситуацию. Один из экспертов отметил, что киберпреступность, в отличие от государственной машины, хаотична: она не имеет чётких процедур и регламентов, распространяется молниеносно и может принимать самые разные формы, зачастую сложно прогнозируемые. Для государства, которое более инертно и функционирует по своим законам и нормам, такой противник является весьма проблематичным.

На прямой вопрос «Является ли реализуемая в России в настоящий момент политика в области борьбы с киберпреступностью результативной и эффективной?» ни один из опрошенных 17 экспертов не дал чёткого утвердительного ответа. 9 экспертов отметили некоторые положительные решения, которых, однако, недостаточно для принципиального изменения ситуации. 2 эксперта отметили, что российская политика в области противодействия киберпреступности в настоящий момент полностью неэффективна. Остальные эксперты чёткую позицию по данному вопросу не высказали.

Какие положительные решения за последние несколько лет в области противодействия киберпреступности в России отметили эксперты? По мнению экспертов, положительный эффект имели профилактические мероприятия и информирование населения; широкое освещение данной проблемы в СМИ; деятельность российских компаний Антивирус Касперского и InfoWatch; стандарты Банка России; подготовка и введение в действие комплекса законов о защите критической инфраструктуры; внедрение Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак; создание Центра мониторинга и реагирования на компьютерные атаки («ФнЦЕРТ»); деятельность Национального координационного центра по компьютерным инцидентам (НКЦКИ); деятельность банков по возврату украденных средств; постепенное налаживание процесса взаимодействия правоохранителей с банками и операторами связи; финансирование проектов в области информационной безопасности и противодействия киберпреступности; некоторые законодательные инициативы в области противодействия киберпреступности. Однако, как уже ранее отметили эксперты, данного набора ограниченных, зачастую запоздалых, несистемных и непоследовательных мер недостаточно для стабилизации ситу-

[14] Путин поручил МВД наладить взаимодействие с банками для борьбы с мошенничеством // Ведомости: [сайт]. URL: https://www.vedomosti.ru/finance/news/2021/03/03/860016-putin-poruchil-mvd-naladit-vzaimodeistvie-s-bankami-dlya-borbi-s-moshennichestvom (дата обращения: 01.08.2023).

ации в моменте, а тем более решения проблемы в перспективе.

Какие препятствия в настоящий момент встают перед Россией в борьбе с киберпреступностью? Эксперты отметили следующие:

1. Негативные последствия на фоне внешнего давления, вызванного как санкциями, так и кибератаками на российскую инфраструктуру и граждан страны.

2. Отсутствие единого, централизованного подхода к повышению цифровой грамотности и образованности населения, оперативного информирования о новых угрозах.

3. Ограничения и проблемы правоохранительной системы: уровень подготовки кадров, административно-территориальные барьеры, сложности обмена информацией с банками и операторами связи, низкая скорость реакции и чрезмерная забюрократизированность.

4. Коррупция.

5. Недостаточное финансирование в сфере противодействия киберпреступности.

6. Недостаточное внимание к проблеме со стороны лиц, принимающих решения. Латентность всей государственной системы.

Описанные выше проблемы один из экспертов суммировала таким образом. «*Отсутствие комплексного реагирования на проблему. В одном направлении работа ведётся, в других нет. Но только комплексное противодействие будет высоко эффективно. Это и право, и профилактика, и кадры, и наука. Ещё и международный аспект, и отток кадров*». Можно дополнить, что при таком подходе в системе безопасности неизбежно создаются пробелы и уязвимости, которыми очень быстро начинают пользоваться киберпреступники.

Есть ли решения у данных проблем? Здесь ряд экспертов снова обратили внимание на отсутствие системного подхода к решению проблемы киберпреступности. Усугубление проблемы киберпреступности в мире и России приходится на экстраординарные события планетарного масштаба: пандемию COVID-19 в 2020–2021 годах и усиление геополитического напряжённости начиная с 2022 года. В таких условиях фокус внимания ключевых лиц может смещаться на более приоритетные, как им кажется, проблемы. Однако это ошибочная позиция. Очевидно, что информационные технологии и цифровой мир – это новая реальность, неотъемлемая черта образа человечества настоящего и будущего. А киберпреступность – неразрывный спутник этой новой реальности. Не замечать эту проблему или занижать её значимость, не предпринимать решительные действия по борьбе с киберпреступностью – стратегия не только проигрышная, но и опасная для благополучия населения и развития страны. В такой ситуации принципиальное значение приобретает вопрос, который всё ещё остается открытым: готово ли государство перестраиваться под новые условия для конкурентной борьбы с новым серьёзным противником либо намерено продолжать сохранять отстающую, проигрышную позицию?

Выводы по результатам исследования

Общение с экспертами и исследователями киберпреступности подтвердило гипотезу о том, что в России не были предприняты необходимые меры для недопущения ухудшения ситуации. Было бы наивно надеяться, что с массовым распространением электронной коммерции, онлайн-банкинга, удалённой работы и прочего широкого круга активностей в цифровой среде и с использованием информационных технологий этим новым трендом не воспользуются преступники. А возможности технологий по сохранению анонимности, сокрытию следов преступлений или подделке голоса или изображений лишь способствуют повышению вероятности совершения деяния без последствий для злоумышленника.

Рост киберпреступности в России – это проявление неэффективности российской государственной системы перед деятельностью очень неудобного и эффективного противника. В большинстве своем пассивная, забюрократизированная и инертная система столкнулась с крайне гибким, адаптивным и умным врагом, влияние которого долгое время недооценивалось и который представляет колоссальную угрозу для самой системы сегодня.

Эффективная борьба с этим врагом требует иного подхода, который принципиально отличается от тех стратегий, которые использовались в отношении реальных преступлений и которые привычны для системы. Эксперты подчеркнули, что меры по борьбе с киберпреступностью имеют запоздалый характер и являются ответной реакцией на уже совершённые события. В борьбе с таким быстрым и адаптивным врагом это уже по умолчанию проигрышная стратегия: когда законодатели обсуждают законопроекты по пресечению одной преступной схемы, преступники активно тестируют уже другие.

Список литературы

1. *Плотникова Т.В., Котельникова О.В.* Феномен киберпреступности в условиях XXI века // Право: история и современность. 2020. № 3(12). С. 141–150. https://doi.org/. 10.17277/pravo.2020.03.pp.141-150; EDN XERGDJ
2. *Султыганова А.А., Кунцман М.В.* Киберпреступность как следствие цифровизации экономики // Экономика и бизнес: теория и практика. 2021. № 9-2(79). С. 88–91. https://doi.org/10.24412/2411-0450-2021-9-2-88-91; EDN YDKKZC
3. Exploring the global geography of cybercrime and its driving forces / S. Chen, M. Hao, F. Ding, D. Jiang, J. Dong, S. Zhang, Q. Guo, C. Gao // Palgrave Communications. 2023. Vol. 1. No. 10. P. 1–10. https://doi.org/10.1057/s41599-023-01560-x
4. *Циклаури В.Ю., Афанасьева Л.В.* Киберпреступность в России: новый вызов для общества и государства // Управленческий учет. 2022. № 6–3. С. 553–561. https://doi.org/10.25806/uu6-32022553-561; EDN BZOTQH
5. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities / H. Saleous, M. Ismail, S.H. AlDaajeh [et al.] // Digital communications and networks. 2022. № 9. P. 211–222. https://doi.org/10.1016/j.dcan.2022.06.005
6. *Прокофьева Т.В.* О мерах по совершенствованию борьбы с киберпреступностью в Российской Федерации // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2022. № 1(842). С. 142–146. https://doi.org/10.52070/2500-3488_2022_1_842_142; EDN ODPGSG
7. *Комлев Ю.Ю.* От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии // Российский девиантологический журнал. 2022. № 2(1). С. 17–26. https://doi.org/10.35750/ 2713-0622-2022-1-17-26; EDN CLLGON
8. *Карпова Д.Н.* Киберпреступность: глобальная проблема и её решение // Власть. 2014. № 8. С. 46–50.
9. *Сергеев А.Ю., Широкова О.В.* Мошенничество в цифровом обществе в условиях социальных изменений // Цифровая социология. 2023. Т. 6. № 1. С. 59–71. https://doi.org/10.26425/2658-347X-2023-6-1-59-71
10. *Тимофеев А.В., Комолов А.А.* Киберпреступность как социальная угроза и объект правового регулирования // Вестник МГОУ. Серия: Философские науки. 2021. № 1. С. 95–101. https://doi.org/10.18384/2310-7227-2021-1-95-101
11. *Старостенко О.А.* Закономерности становления и развития кибермошенничества в России и за рубежом // Вестник Уральского юридического института МВД России. 2021. № 1. С. 138–143. EDN UCURDF
12. *Никульченкова Е.В.* О необходимости введения дефиниции "киберпреступление" в уголовный закон Российской Федерации // Вестник Омского университета. Серия. Право. 2022. Т. 19. № 3. С. 98–107. https://doi.org/10.24147/1990-5173.2022.19(3).98-107; EDN NGKTBX
13. Цифровая грамотность населения как средство обеспечения информационной безопасности в Республике Беларусь и Российской Федерации / Н.Н. Ковалева, А.С. Анисимова, И.В. Шахновская, П.В. Соловьев // Вестник Полоцкого государственного университета. 2023. Серия D. Экономические и юридические науки. № 1. С. 118–124. https://doi.org/10.52928/2070-1632-2023-63-1-118-124; EDN MCOHJG
14. *Швыряев П.С.* Киберпреступность в России: новый вызов для общества и государства // Государственное управление. Электронный вестник. 2021. № 89. С. 184–196. https://doi.org/10.24412/2070-1381-2021-89-184-196; EDN KFWYZW
15. *Осипенко А.Л., Луговик В.Ф.* Проблемы доступа правоохранительных органов к скрываемой компьютерной информации при раскрытии преступлений // Общество и право. 2021. № 2(76). С. 60–68. EDN NGIAPT
16. *Михайлюк В.А.* Киберполиция – современный правоохранительный орган в борьбе с интернет-преступностью // Вестник Уфимского юридического института МВД России. 2023. № 1(99). С. 74–79.
17. *Клевцов К.К.* Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам // Вестник Санкт-Петербургского университета. Право. 2022. Том 13. № 3. С. 678–695. https://doi.org/10.21638/spbu14.2022.306; EDN BGHNMV
18. *Швыряев П.С.* Кадровая обеспеченность в сфере информационных технологий в России: проблемы и перспективы // Государственное управление. Электронный вестник. 2023. № 97. С. 231–240. https://doi.org/10.24412/2070-1381-2023-97-231-240
19. *Кобец П.Н.* Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт // Научный вестник Омской академии МВД России. 2022. № 2. С. 101–105. https://doi.org/10.24412/1999-625X-2022-285-101-105
20. *Долженко Н.И., Хмелевская И.Г.* К вопросу о содержательных аспектах киберпреступности // NOMOTHETIKA: Философия. Социология. Право. 2020. Том 45. № 2. С. 315–322. https://doi.org/10.18413/2712-746X-2020-44-2-315-322; EDN WKUGYD

Информация об авторе:
Павел Сергеевич Швыряев – аспирант, факультет государственного управления, Московский государственный университет им. М.В. Ломоносова, Москва, Россия
(e-mail: ShvyryaevPS@spa.msu.ru)
Автор заявляет об отсутствии конфликта интересов.

Статья поступила в редакцию 12.09.2023; одобрена после рецензирования 15.11.2023; принята к публикации 01.12.2023.

References

1. Plotnikova T.V., Kotel'nikova O.V. Fenomen kiberprestupnosti v usloviyakh XXI veka. *Pravo: istoriya i sovremennost'*. 2020;(3(12));141–150. (In Russ.) https://doi.org/. 10.17277/pravo.2020.03.pp.141–150
2. Sultyganova A.A., Kuntsman M.V. Cybercrime as a consequence digitalization of the economy. E*hkonomika i biznes: teoriya i praktika=Journal of Economy and Business.* 2021;(9-2(79)):88-91. (In Russ.) https://doi.org/10.24412/2411-0450-2021-9-2-88-91
3. Chen S., Hao M., Ding F., et al. Exploring the global geography of cybercrime and its driving forces. *Palgrave Communications.* 2023;1(10):1-10. https://doi.org/10.1057/s41599-023-01560-x
4. Tsiklauri V.Y., Afanasyeva L.V. Cybercrime in Russia: a new challenge to society and the state. *Upravlencheskiy uchet=Management Accounting.* 2022;(6-3):553-561. (In Russ.) https://doi.org/10.25806/uu6-32022553-561
5. Saleous H., Ismail M., Aldaajeh S.H., et al. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital communications and networks.* 2022;(9):211-222. https://doi.org/10.1016/j.dcan.2022.06.005
6. Prokofieva T.V. On Measures to Improve the Fight Against Cybercrimes in the Russian Federation. *Vestnik Moskovskogo gosudarstvennogo lingvisticheskogo universiteta. Obrazovanie i pedagogicheskie nauki=Vestnik of Moscow State Linguistic University. Education and Teaching.* 2022;842(1):142–146. (In Russ.) https://doi.org/10.52070/2500-3488_2022_1_842_142
7. Komlev Yu.Yu. From digitalization of society to cybercrime, cyber deviance and the development of digital deviantology. *Russian Journal of Deviant Behavior=Russian Journal of Deviant Behavior.* 2022;1(2);17–26. (In Russ.) https://doi.org/10.35750/ 2713-0622-2022-1-17-26
8. Karpova D.N. Kiberprestupnost': global'naja problema i ee reshenie. *Vlast'*. 2014;8;46-50. (In Russ.)
9. Sergeyev A.Yu., Shirokova O.V. Fraud in a digital society in the context of social change. *Tsifrovaya sotsiologiya=Digital Sociology.* 2022;6(1):59–71. (In Russ.) https://doi.org/10.26425/2658-347X-2023-6-1-59-71
10. Timofeev A.V., Komolov A.A. Cybercrime as a Social Threat and an Object of Legal Regulation. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskie Nauki=Bulletin of Moscow Region State University. Series: Philosophy.* 2021;1:95–101. (In Russ.) https://doi.org/10.18384/2310-7227-2021-1-95-101
11. Starostenko O.A. Regularities of the Formation and Development of Cyber Fraud in Russia and Abroad. *Vestnik Ural'skogo yuridicheskogo instituta Ministerstva vnutrennikh del Rossii=Bulletin of the Ural Law Institute of the Ministry of the of the Interior of the Russian Federation.* 2021;(1):138-143. (In Russ.)
12. Nikulchenkova E.V. On the Need to Introduce the Definition of "Cybercrime" into the Criminal Law of the Russian Federation. *Vestnik Omskogo universiteta. Seriya "Pravo"=Herald of Omsk University. Series "Law".* 2022;19(3):98-107. (In Russ.) https://doi.org/10.24147/1990-5173.2022.19(3).98-107
13. Kovaleva NN., Anisimova AS., Shakhnovskaya IV., et al. Digital literacy of the population as a means of information security in the Republic of Belarus and the Russian Federation. *Vestnik Polotskogo gosudarstvennogo universiteta. 2023. Seriya D. Ehkonomicheskie i yuridicheskie nauki=Vestnik of Polotsk State University. Part D. Economic and legal sciences.* 2023;(1):118-124. (In Russ.) https://doi.org/10.52928/2070-1632-2023-63-1-118-124
14. Shvyriaev P. Cybercrime in Russia as a new challenge for society and the state. *Gosudarstvennoe upravlenie. Ehlektronnyi vestnik=Public Administration. E-journal (Russia).* 2021;(89):184-196. (In Russ.) https://doi.org/10.24412/2070-1381-2021-89-184-196
15. Osipenko A.L., Lugovik V.F. Problems of access of law enforcement agencies to concealed computer information when solving crimes. *Obshchestvo i parvo=Society and law.* 2021;(2(76)):60-68. (In Russ.)
16. Mikhailyuk V.A. Cyber police is a modern law enforcement agency in the fight against internet crime. *Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii=Bulletin of Ufa Law Institute of the Ministry of Internal Afairs of Russia.* 2023;(1(99)):74-79. (In Russ.)
17. Klevtsov K.K. International cooperation in the fight against cyberpression in the context of response to new challenges and threats. *Vestnik Sankt-Peterburgskogo universiteta. Pravo=Vestnik of Saint Petersburg University. Law.* 2022;13(3):678-695. (In Russ.) https://doi.org/10.21638/spbu14.2022.306
18. Shvyriaev P. Staffing in the Field of Information Technology in Russia: Problems and Prospects. *Gosudarstvennoe upravlenie. Ehlektronnyi vestnik=Public Administration. E-journal (Russia).* 2023;(97):231-240. (In Russ.) https://doi.org/10.24412/2070-1381-2023-97-231-240
19. Kobets P.N. Legal Basis for Cybercrime Prevention: Domestic and Foreign Experience. *Nauchnyi vestnik Omskoi akademii MVD Rossii=Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia.* 2022;(2):101-105. (In Russ.) https://doi.org/10.24412/1999-625X-2022-285-101-105
20. Dolzhenko N.I., Khmelevskaya I.G. To the question of the content aspects of cyber crime. *NOMOTHETIKA: Filosofiya. Sotsiologiya. Pravo=NOMOTHETIKA: Philosophy. Sociology. Law series.* 2020;45(2):315-322 (in Rus.) https://doi.org/10.18413/2712-746X-2020-44-2-315-322

Information about the author:
Pavel S. Shvyriaev – Postgraduate student, School of Public Administration, Lomonosov Moscow State University, Moscow, Russia (e-mail: ShvyryaevPS@spa.msu.ru)

The author declare no conflict of interest.

The article was submitted 12.09.2023; approved after reviewing 15.11.2023; accepted for publication 01.12.2023.

Приложение А
Дорожная карта глубинного интервью с экспертами
(государственными служащими, специалистами в области информационной безопасности, исследователями киберпреступности)

Appendices A
Roadmap for In-depth Interviews with Experts
(Government Officials, Information Security Specialists, Cybercrime Researchers)

№	Тема	№	Вопрос	Ответ
1.	Состояние киберпреступности в России	1	Как бы Вы охарактеризовали актуальное состояние киберпреступности в России в 2023 году?	
		2	Можно ли говорить о том, что сегодня проблема киберпреступности – угроза национальной безопасности России?	
		3	В чем, на Ваш взгляд, главная опасность киберпреступности?	
		4	Какие ключевые тренды за последние несколько лет в сфере киберпреступлений в России Вы бы отметили?	
		5	Как Вы считаете, оказалась ли система безопасности России готова к росту количества киберпреступлений в период пандемии и после её окончания? Или же ситуация вышла из-под контроля?	
		6	Как Вы считаете, в настоящий момент проблеме киберпреступности в России уделяется достаточное внимание со стороны государственной власти?	
		7	В какой степени, на Ваш взгляд, эффективны российские правоохранительные органы в борьбе с киберпреступностью?	
		8	Как Вы считаете, кто сегодня в России главный объект киберпреступного воздействия: общество, государство, бизнес?	
		9	А кто в России в настоящее время несёт наиболее серьёзные потери от киберпреступной деятельности: бизнес, государство, общество?	
		10	А кто сейчас в России наименее защищён перед угрозой киберпреступности: общество, бизнес, государство?	
		11	Можно ли спрогнозировать дальнейшее развитие проблемы киберпреступности в России? Если да, каким Вам представляется состояние киберпреступности в России на горизонте ближайших 2–3 лет?	
2.	Причины сложившейся ситуации	1	Как Вы считаете, каковы ключевые причины роста количества киберпреступлений в России в последние годы?	
		2	Какие ключевые факторы влияют на состояние киберпреступности в России, на Ваш взгляд?	
		3	На Ваш взгляд, какие ключевые решения должны были быть предприняты для недопущения ухудшения ситуации с киберпреступностью в России в последние годы?	
		4	Были ли они предприняты? Если нет, то по какой причине, на Ваш взгляд?	
		5	Как Вы считаете, в какой степени российская законодательная база отвечает вызовам со стороны киберпреступной угрозы? Актуальна ли она и эффективна в борьбе с киберпреступностью?	
		6	Как Вы считаете, в России реализуемая сегодня политика по борьбе с киберпреступностью является результативной и эффективной?	

Окончание Приложения А

№	Тема	№	Вопрос	Ответ
		7	Какие эффективные решения в борьбе с киберпреступностью в России Вы бы отметили? Если таковые имели место быть, на Ваш взгляд.	
		8	Как Вы считаете, влияет ли уровень цифровой грамотности населения на состояние киберпреступности в государстве? Как бы вы оценили уровень цифровой грамотности населения в России?	
		9	Как Вы считаете, каким образом мог повлиять отток высококвалифицированных ИТ-кадров в 2022 году на состояние киберпреступности в стране? А влияет ли "утечка мозгов", которая наблюдается в течение многих лет в России?	
		10	Как Вы считаете, каким образом санкционное давление и курс на импортозамещение могли повлиять и повлияют на состояние киберпреступности в России?	
3.	Стратегии решения проблемы	1	Какие, на Ваш взгляд, препятствия встают перед Россией на пути решения проблемы киберпреступности?	
		2	Есть ли решения у этих проблем? Если да, какими Вы видите эти решения?	
		3	В последние несколько лет набирает популярность киберимунный подход к разработке и внедрению цифровых систем, где первостепенный приоритет отдаётся безопасности и отказоустойчивости системы. Как Вы считаете, сегодня уже назрел пересмотр сложившегося подхода к разработке цифровых систем? Должен ли принцип безопасности лежать в основе цифровых систем будущего?	
		4	На ваш взгляд, ужесточение законодательства за киберпреступную деятельность и халатность в отношении конфиденциальных данных эффективно в борьбе с киберпреступностью?	
		5	Эффективна ли работа с населением в рамках борьбы с киберпреступностью? Сегодня в России проводятся массовые кампании по информированию граждан, повышению их цифровой грамотности. На Ваш взгляд, есть ли смысл в такой деятельности? И если да, как можно повысить эффективность и результативность таких кампаний?	
		6	Как Вы считаете, какое место занимает международное сотрудничество в решении проблемы киберпреступности? Какое влияние в данном контексте может оказать курс России на разрыв отношений с "недружественными" странами?	
4	Заключительный блок	1	Если Вы хотели бы что-то добавить по проблеме киберпреступности и стратегиям борьбы с ней, это можно сделать в рамках данного блока.	