РИСКИ СОЦИАЛЬНЫХ МЕТАМОРФОЗ

DOI: 10.19181/vis.2024.15.4.12
EDN: HOJENA

Развитие информационно-сетевой среды и девиантное поведение: киберпреступность как новая социальная угроза

Ссылка для цитирования: *Позднякова М. Е., Брюно В. В.* Развитие информационно-сетевой среды и девиантное поведение: киберпреступность как новая социальная угроза // Вестник Института социологии. 2024. Том 15. № 4. С. 235–254. DOI: 10.19181/vis.2024.15.4.12; EDN: HOJENA.
For citation: Pozdnyakova M. E., Bruno V. V. Development of the Information and Network Environment and Deviant Behaviour: Cybercrime as a New Social Threat. *Vestnik instituta sotziologii.* 2024. Vol. 15. No. 4. P. 235–254. DOI: 10.19181/vis.2024.15.4.12; EDN: HOJENA.

SPIN-код: 6236-8782

Позднякова Маргарита Ефимовна[1]

[1]Институт социологии ФНИСЦ РАН, Москва, Россия

margo417@mail.ru

SPIN-код: 3191-0120

Брюно Виктория Владимировна[1]

[1]Институт социологии ФНИСЦ РАН, Москва, Россия

victoria.bruno@mail.ru

Аннотация. В представленной статье рассматривается проблема новых цифровых угроз. В фокусе исследования основные тенденции развития киберпреступности в России и ее специфические страновые особенности. Проведенный авторами анализ статистических данных различных ведомств (МВД, Генпрокуратуры, Роскомнадзора) по состоянию и структуре преступности показал, что киберпреступность в России за последние годы значительно возросла, особенно в сфере телекоммуникаций и компьютерной информации. Выявлены и проанализированы наиболее распространенные виды киберпреступлений в российском обществе – различные виды мошенничеств и кражи, совершенные с использованием информационно-коммуникационных технологий.

Эмпирическую основу исследования составляют данные онлайн-опроса городского трудоспособного населения (18–60 лет), проведенного сотрудниками сектора социологии девиантного поведения ИС ФНИСЦ РАН по многоступенчатой квотной выборке (март-май 2024 г.). Было оценено отношение горожан к различным видам цифровой преступности.

Установлено, что многие респонденты считают вероятность стать жертвой кибермошенничества высокой, особенно в отношении незаконного использования персональных данных и взлома электронной почты.

Выявлено, что количество респондентов, опасающихся стать жертвой киберпреступления, увеличивается с возрастом. В то же время в самых старших возрастных группах эти опасения снижаются. Уровень образования также является важным дифференцирующим фактором в отношении столкновения с киберугрозами – чем выше его уровень, тем чаще респонденты имеют опыт столкновения с киберпреступлениями.

Для выявления ключевых особенностей киберпреступности в России был проведен опрос экспертов. К экспертизе были привлечены специалисты различных направлений – от исследователей-девиантологов до практических работников, занимающихся информационной безопасностью и имеющих опыт работы с киберпреступностью. Их прогноз на ближайшие годы неутешителен – ожидается дальнейший рост киберпреступности, усложнение применяемых техник, включая использование искусственного интеллекта, в связи с чем необходима разработка специализированных защитных решений.

Показано, что основными факторами роста киберпреступности в России является ее двойственная природа, проявляющаяся в одновременной организационной сложности и структурированности, с одной стороны, и гибкости, и адаптивности, – с другой. Кроме того, киберпреступность обостряет важную социальную проблему – растущее цифровое неравенство. Таким образом, киберпреступность в России представляет серьезную угрозу, требующую комплексного подхода и скоординированных усилий на всех уровнях общества для ее эффективного пресечения.

Ключевые слова: девиантное поведение, киберпреступность, информационно-коммуникационные технологии, кибермошенничество, социальная инженерия, компьютерная преступность, трудоспособное городское население

Введение

Появление и развитие цифровых технологий стали катализатором значительных метаморфоз в различных сферах общества, изменив не только способ общения людей, но и механизмы инициирования и распространения девиантного поведения [4; 7]. Цифровая эволюция привела к расширению технической инфраструктуры, а повсеместное распространение Интернета в российском обществе спровоцировало заметный сдвиг в сторону цифровых форм девиантности, охватывающих широкий спектр моделей поведения, большинство из которых противоречат социальным нормам, правовым стандартам или тому и другому. Наиболее распространенные формы отклонений в цифровой сфере в России и в мире, характерные для всех слов населения: киберагрессия и кибербуллинг, несанкционированное распространение информации, онлайн-мошенничество, кибератаки (злонамеренное вмешательство в компьютерную систему или сеть), распространение вредоносных компьютерных программ, рассылка спама, киберхарассмент (сексуализированные домогательства в Сети), кража личных данных, хакерство, распространение откровенных изображений или видео

людей без их ведома и/или согласия (так называемая «порноместь») и другие. Иными словами, в России отмечается переход от традиционных форм девиаций к цифровым, что отражает глобальные тенденции.

Специалисты в области компьютерных технологий по всему миру отмечают, что киберпреступность сегодня вышла на новый уровень, демонстрируя все более сложные формы и охватывая бо̀льшие масштабы [4]. В условиях цифрового неравенства и усложнения преступных схем киберугрозы становятся не просто технической или правовой, но и глубокой социальной проблемой, трансформируя повседневную жизнь и изменяя восприятие безопасности и доверие к цифровой среде. Важно понять, какие аспекты киберугроз воспринимаются обществом наиболее остро, какие группы населения чувствуют себя наиболее уязвимыми и как страх перед этими угрозами влияет на поведение в цифровом пространстве. Это позволит выявить не только точки наибольшей уязвимости, но и социальные механизмы, которые способствуют развитию киберпреступности.

Основная цель настоящей работы заключается в изучении киберпреступности в России как новой формы девиантного поведения. Исследование направлено на анализ ее структурных особенностей, масштабов распространения и восприятия в обществе. В задачи исследования входило проанализировать структуру компьютерных преступлений и выявить наиболее распространенные виды киберпреступлений в российском обществе; изучить отношение городского трудоспособного населения к различным видам цифровой преступности; проанализировать мнения экспертов относительно особенностей российской киберпреступности, причин ее роста и эффективных методов борьбы с ней, а также сформулировать ряд рекомендаций по борьбе с киберпреступностью.

Проблема киберпреступности вызывает все больший интерес в научном сообществе, что обусловлено ее нарастающей значимостью в условиях цифровизации общества. Наибольший интерес к этому явлению проявляют специалисты в области права и криминологии. Юристы и криминологи анализируют определения и классификации киберпреступлений в контексте российского и международного законодательства [12], изучают особенности правового регулирования, принципы предотвращения киберпреступлений и текущее состояние правовой среды в данной области [2; 3; 9]. Проблемам контроля компьютерной преступности в России и на международном уровне, особенно в условиях ее трансформации в высокотехнологическую преступность, посвящены исследования К. Н. Евдокимова [4].

Социологи рассматривают киберпреступность как часть более обширного явления кибердевиантности. Значительная часть работ содержит социологическую рефлексию о природе цифровой социальной реальности. Так, О. В. Крыштановская, М. В. Кибакин, В. Ф. Ницевич акцентируют внимание на социальных эффектах и проблемах, возникающих в результате влияния Интернета, социальных медиа и популярных онлайн-платформ на российское общество [15; 6; 11]. Вопросы влияния цифровизации на социальное развитие и рост киберпреступности изучаются в исследованиях А. Ю. Сергеева и О. В. Широковой [13].

Несмотря на активные дискуссии, комплексный подход к изучению киберпреступности остается на стадии формирования. В этой связи особый интерес представляют работы криминолога и социолога Ю. Ю. Комлева, посвященные анализу цифровизации и разработке и развитию цифровой девиантологии. Обобщая результаты российских и международных исследований, автор показывает, что с момента своего возникновения кибердевиантность проявляется в различных формах, обусловленных цифровизацией и сетевизацией; и они значительно эволюционировали, став более сложными и разнообразными. Комлев указывает на недостаточность традиционных криминологических теорий для объяснения данных процессов и обосновывает необходимость интегративного подхода, включающего знания из девиантологии, криминологии, социологии, юриспруденции, семиотики, теории масс-медиа и других дисциплин, в том числе математических наук [7; 8].

Из современных интересных социологических работ отметим диссертацию П. С. Швыряева, рассматривающего киберпреступность как социальную проблему. Автор отмечает, что существенный крен в сторону технократического подхода к киберпреступности упускает из фокуса внимания социальную природу этого явления, что делает борьбу с киберпреступностью неэффективной [14].

Несмотря на значительное количество исследований в области кибердевиантности и киберпреступности, социологических работ, посвященных этим явлениям, по-прежнему недостаточно. Особенно ограничено количество исследований, касающихся отношения населения к различным видам киберпреступности, а также изучения опыта «столкновения» с ними в повседневной жизни, что представляется важным для разработки эффективных стратегий профилактики и борьбы с данными угрозами.

Методологические и эмпирические основания исследования

Эмпирической основой нашего исследования являются материалы онлайн-опроса городского трудоспособного населения в возрасте от 18 до 60 лет, проведенного сотрудниками сектора социологии девиантного поведения ИС ФНИСЦ РАН по многоступенчатой квотной выборке (март-май 2024 г.). Выборка представлена 13 крупными городами России: Москва, Санкт-Петербург, Калининград, Омск, Челябинск, Воронеж, Сыктывкар, Архангельск, Краснодар, Казань, Екатеринбург, Тюмень и Пермь (n = 1300)[1].

Для исследования особенностей киберпреступности в России авторами был проведен опрос экспертов. Критерии отбора экспертов включали в себя: компетентность в теме цифровых девиаций и киберпреступности, знание о распространенности различных форм киберпреступлений, практический опыт работы с киберпреступностью, знания в сфере информа-

[1] Онлайн опрос осуществлен совместно с компанией OMI (Online Market Intelligence) – российской IT-компанией, предоставляющей комплексные решения для онлайн исследований.

ционной безопасности. Важным этапом отбора экспертов была проверка на компетентность, для чего на первичных консультациях собирались данные о кандидатах (документы, подтверждающие квалификацию специалиста, публикационная активность, участие в конференциях, участие в исследовательских проектах, связанных с темой киберпреступности). В результате отбора были опрошены: социологи и криминологи, владеющие темой преступности, включая цифровую; представители правоохранительных органов (участковые инспекторы Москвы Южного и Северного округа); специалисты по информационной безопасности. Помимо заявленных целей, авторы поставили перед экспертами задачу попытаться дать оценку будущему состоянию киберпреступности в России и сформулировать рекомендации для улучшения стратегии противодействия киберпреступности. Для этого был применен метод деструктивной отнесенной оценки[1], а сам опрос проходил в очном групповом формате, что позволило экспертам дискутировать по вопросам, представленным в сценарии. Всего было опрошено 10 человек.

В работе также использованы статистические материалы различных ведомств (Росстата, МВД, Генпрокуратуры, Роскомнадзора) по состоянию и структуре преступности (по некоторым видам преступлений).

Распространенность киберпреступности в России

С 2005 г. общее число зарегистрированных преступлений в России, включая тяжкие и особо тяжкие, снизилось более, чем на 45%, с 3 554 738 случаев в 2005 г. до 1 947 161 в 2023 г. (тяжкие и особо тяжкие – с 1 076 988 до 589 079 случаев)[2]. Во многом благодаря улучшению систем безопасности в городах, включая системы видеонаблюдения, значительно сократились традиционные виды преступлений: грабежи, разбои и убийства[3]. В то же время заметно увеличилось число «бесконтактных» преступлений, которые в первую очередь связаны с незаконными действиями в области информационных технологий, то есть киберпреступность[4].

В широком смысле, киберпреступность – это преступная деятельность, осуществляемая с помощью компьютеров или Интернета. В России в структуре рассматриваемого вида преступности принято выделять три вида преступлений: 1) преступления в сфере компьютерной информа-

[1] Метод деструктивной отнесенной оценки направлен на выявление наиболее значимых факторов или элементов из множества альтернатив через процесс последовательного исключения наименее важных с помощью деструирования (опровержения).

[2] Состояние преступности в России за январь-декабрь 2005: стат. сб. // МВД РФ ФКУ «Главный информационно-аналитический центр». М., 2005. 32 с.; Состояние преступности в России за январь-декабрь 2023: стат. сб. // МВД РФ ФКУ «Главный информационно-аналитический центр». М., 2023. 64 с.

[3] В МВД заявили об историческом максимуме показателя раскрываемости убийств в РФ // Известия. 2023. 20 июля. URL: https://iz.ru/1546971/2023-07-20/v-mvd-zaiavili-ob-istoricheskom-maksimume-pokazatelia-raskryvaemosti-ubiistv-v-rf (дата обращения: 15.04.2024).

[4] Петров И. Числа по беспределу: как изменилась криминальная картина в стране // Известия. 2023. 23 сентября. URL: https://iz.ru/1579157/ivan-petrov/chisla-po-bespredelu-kak-izmenilas-kriminalnaia-kartina-v-strane (дата обращения: 01.06.2024).

ции[1], 2) преступления, *совершаемые с использованием* информационно–телекоммуникационных технологий (ИТТ) и 3) преступления, *совершаемые в* информационно-телекоммуникационных сетях (ИТС), включая сеть Интернет[2] [5]. В статистических данных МВД количество зарегистрированных преступлений по этим трем показателям суммируется (приказ Генпрокуратуры РФ № 589 от 12.10.2022), что некоторыми криминологами считается некорректным, поскольку безосновательно расширяет категорию данного типа преступлений и искажает динамику их роста. Так, известный специалист в области информационных технологий, кандидат юридических наук, К. А. Каримов считает, что к истинной киберпреступности следует относить лишь первый тип преступлений, совершаемых лицами, обладающими высокой квалификацией и глубокими знаниями в сфере информационных технологий. Второй и третий типы, как правило, совершаются менее квалифицированными преступниками, которые используют интернет как инструмент, для чего не нужно глубоких знаний [5]. В целом соглашаясь с К. А. Каримовым, по мнению авторов этих строк, анализ второго и третьего типов преступлений все же имеет значение в контексте киберпреступности, поскольку они происходят в рамках цифровой среды и используют онлайн-платформы. В условиях, когда личная и коммерческая жизнь все больше переходит в онлайн, возможности для совершения преступлений второго и третьего типов возрастают, что может создавать благоприятную почву и для более серьезных киберугроз и требует соответствующих мер реагирования.

Отметим, что количество россиян, имеющих доступ в интернет, выросло с 15% в 2005 г. до 83% в 2023 г., при этом российские пользователи в среднем проводят в интернете около четырех часов в день, а в младших возрастных группах этот показатель превышает шесть часов в день[3]. С ростом проникновения Интернета увеличивается как количество киберпреступлений, так и круг потенциальных жертв. Преступники используют анонимность и масштабы Интернета для совершения различных преступлений: от кражи личных данных до изощренных мошенничеств.

В России статистика компьютерных преступлений ведется с 1997 г., когда была введена уголовная ответственность за преступления в сфере компьютерной информации[4]. За период 1999–2003 гг. среднегодовые темпы

---

[1] Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»; ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации»; ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

[2] Ст. ст.: 138, 138.1, 146, 158, 159, 159.3, 159.6, 163,165, 171.2, 183, 228.1, 230, 242, 242.1, 242.2, 280, 282 УК РФ и др.

[3] Давыдов С. Г., Казарян К. Р., Сайкина М. В. Интернет в России в 2022–2023 годах. Состояние, тенденции, перспективы развития. Отраслевой доклад // Минцифры. М.: Дизайн-студия RE-FORM, 2023. 207 с. URL: https://digital.gov.ru/uploaded/files/internet-v-rossii-v-2022-2023-godah.pdf (дата обращения: 15.04.2024).

[4] В 1998 г. было создано специализированное подразделение «Р» МВД РФ по борьбе с преступностью в сфере высоких технологий. В настоящее время его функции выполняет управление «К» МВД РФ по борьбе с компьютерными преступлениями. Кроме того, с 2022 года в структуре МВД России указом президента Владимира Путина создано управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК).

роста компьютерной преступности в России составляли уже 88% [10]. С тех пор количество киберпреступлений в России показывает неуклонный и интенсивный рост. Так, по данным МВД РФ, за последние 10 лет количество преступлений в сфере телекоммуникаций и компьютерной информации увеличилось в России в 62 раза, с 11 тыс. в 2013 г. до 676951 в 2023 г., а удельный вес с 0,2 до 34,8% соответственно[1]. В 2023 г. рост составил 29,7% по сравнению с предыдущим, а в количественном выражении это практически 676 тысяч преступлений[2]. В первом квартале 2024 г. тенденция не изменилась: вновь зафиксирован рост на 17,6%, при этом в общем числе зарегистрированных преступлений их удельный вес увеличился с 31,5% в январе – марте 2023 г. до 37,9%.[3]

Анализ структуры компьютерных преступлений показывает, что основная их масса (80–99%) совершается с использованием ИТТ или в ИТС, то есть «неквалифицированными» преступниками. Самыми распространенными преступлениями в данной сфере, согласно данным статистики МВД, являются: *мошенничества* (и его специальные составы: мошенничество с использованием электронных средств платежа и мошенничество в сфере компьютерной информации) и *кражи* (в том числе кражи, совершенные с банковского счета или в отношении электронных денежных средств), совершенные с использованием информационно-коммуникационных технологий (до 80%)[4]. Так, например, мошенничество с использованием электронных средств платежа выросло с 85 случаев в 2017 г. до 7288 в 2022 г.[5].

На втором месте – сбыт наркотических средств и психотропных веществ с помощью информационно-коммуникационных технологий (около 10%). Оставшуюся долю делят между собой преступления в сфере компьютерной информации (неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ); публичные призывы к экстремистской деятельности, совершенные с использованием сети Интернет; нарушение авторских и смежных прав. Так, количество случаев неправомерного доступа к компьютерной информации выросло с 1930 в 2017 г. до 9308 в 2022 г.[6].

---

[1] Состояние преступности в России за январь-декабрь 2013: стат. сб. // МВД РФ ФКУ «Главный информационно-аналитический центр». М. 2013. 54 с.; Состояние преступности в России за январь-декабрь 2023: стат. сб. // МВД РФ ФКУ «Главный информационно-аналитический центр». М., 2023. 64 с.

[2] Состояние преступности в России за январь-декабрь 2023: стат. сб. // МВД РФ ФКУ «Главный информационно-аналитический центр». М., 2023. 64 с.

[3] Состояние преступности в России за январь-март 2024: стат. сб. // МВД РФ ФКУ «Главный информационно-аналитический центр». М., 2024. 64 с.

[4] Мошенничество в сети: судебная практика и ключевые аспекты // TRM GROUP. 2021. URL: https://rtmtech.ru/research/online-fraud-research/ (дата обращения: 20.04.2024)

[5] Колесникова Н. В. Данные из формы федерального статистического наблюдения № 1-ЕГС «Единый отчет о преступности» (за 2012, 2017 и 2022 годы) // Отдел правовой статистики и информационного обеспечения прокурорской деятельности Ун-та прокуратуры РФ. URL: https://crimas.ru/wp-content/uploads/2023/03/Dannye-po-vsem-statyam-UK-12-17-22.docx?ysclid=lxbnm44csi831424838 (дата обращения: 01.06.2024).

[6] Там же.

Один из наиболее популярных видов кибер-мошенничества – фи́шинг (от англ. phishing, от fishing – рыбная ловля, выуживание). Целью этого киберпреступления является получение доступа к конфиденциальным данным (данные банковских карт, паспортов, логины, пароли, пин-коды, коды верификации и др.). Данное преступление традиционно осуществляется через электронные письма, сообщения в мессенджерах, поддельные сайты, а также телефонные звонки («вишинг») и SMS («смишинг»). Сообщение может содержать ссылку на поддельный сайт, который визуально напоминает настоящий и предназначен для кражи личных данных. Мошенники часто подделывают сайты известных компаний. Например, на поддельном сайте РЖД предлагались дешевые билеты на «Сапсан», а на якобы официальных сайтах «ресторанов» просят внести предоплату за бронь столика.

Количество фишинговых сайтов в России в 2023 г. резко возросло. Компания по управлению цифровыми рисками BI.ZONE обнаружила 70 тыс. подобных сайтов в 2021 г., 111 тыс. в 2022 г. и уже 212 тыс. в 2023 г.[1]. Только за январь и февраль 2024 г. было выявлено 41 тыс. мошеннических ресурсов. При этом доля блокировки незаконных сайтов составляет от 10 до 30%[2]. Опрошенные нами специалисты полагают, что ключевая причина увеличения количества фишинговых сайтов – появление возможностей сделать такой сайт обычному пользователю с помощью распространившихся «конструкторов сайтов», которые может использовать человек, не обладающий навыками программирования.

Значительно возросло телефонное мошенничество, которое также эволюционировало, внедряя интернет-технологии (например, интернет-телефонию) для реализации своих схем. В 2022 г. число таких попыток в отношении граждан России достигло 5 млн в сутки, в 2024 г. – уже 20 млн в сутки. Доля телефонного мошенничества в общем объеме кибермошенничества составляет 90%[3]. Согласно опросу ВЦИОМ, телефонные звонки от мошенников получают две трети граждан России[4]. Наши исследования также подтверждают эти данные. При этом, несмотря на ввод в строй Роскомнадзором в январе 2023 г. платформы «Антифрод», предназначенной для борьбы с этим явлением, рост сохраняется (см. табл. 1). По словам зампреда «Сбера» Станислава Кузнецова, примерно в одном случае из 100 люди верят телефонным мошенникам. То есть порядка 200 тыс. граждан в сутки могут попадаться на их обман.

---

[1] Threat Zone 2024. Исследование российского ландшафта киберугроз // BI.ZONE. 2024. URL: https://bi.zone/upload/for_download/Threat_Zone_2024_BI.ZONE_Research_rus.pdf (дата обращения: 01.05.2024).

[2] Фишинг, недорого // Коммерсант. 2024. 14 марта. URL: https://www.kommersant.ru/doc/6563591 (дата обращения: 01.05.2024).

[3] Павленко О. Сбербанк зафиксировал рост числа попыток телефонного мошенничества в отношении россиян до 8,6 млн в сутки // Коммерсант. 2024. 14 июня. URL: https://www.kommersant.ru/doc/6043349 (дата обращения: 14.05.2024).

[4] Телефонное мошенничество: мониторинг // ВЦИОМ. 2024. 20 февраля. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 20.11.2024).

Таблица 1 (Table 1)

Результаты опроса ВЦИОМ по телефонному мошенничеству за 2021, 2022, 2023 годы,
% от всех опрошенных[1]

Results of the WCIOM survey on telephone fraud for 2021, 2022, 2023,
% of all respondents

Вид мошенничества	Год проведения опроса		
	2021	2022	2024
Звонки	57	63	67
Смс	19	20	17
Ничего такого не было	35	33	30
Затруднились с ответом	1	1	1

Анализ распространенности киберпреступности в России свидетельствует о том, что, несмотря на общее снижение традиционных видов преступлений, общество сталкивается с новыми вызовами, возникающими в условиях цифровизации. С ростом интернет-пространства и массовым переходом в онлайн-сферу, киберпреступность становится не просто уголовной, но и социальной проблемой, изменяя некоторые привычные модели поведения и способы взаимодействия. Проникновение технологий в повседневную жизнь может изменить восприятие безопасности и доверия, как к другим людям, так и к цифровым системам.

Киберпреступность: восприятие гражданами России

Результаты опроса, проведенного сектором социологии девиантного поведения ИС ФНИСЦ РАН, среди городского трудоспособного населения в возрасте 18–60 лет, демонстрируют высокую степень озабоченности россиян по поводу киберугроз, что свидетельствует о растущем осознании рисков, связанных с цифровой безопасностью. Две трети опрошенных респондентов (в среднем 69%) считают вероятность стать жертвой кибермошенников высокой и очень высокой, особенно опасения вызывают незаконное использование (75%) и кража персональных данных (73%), а также взломы электронной почты (73%). Несколько в меньшей степени респонденты опасаются телефонного мошенничества (67%) и мошенничества в Интернете (66%). Меньше всего респонденты опасаются стать жертвой банковских махинаций (58%) (табл. 2).

Женщины относятся к киберпреступлениям более настороженно: в среднем 78% из них считают, что стать жертвой киберпреступника сегодня весьма и очень вероятно (среди мужчин таковых 63%). Это связано с различиями в восприятии риска, цифровой грамотности и различным опытом использования Интернета и технических устройств.

[1] Телефонное мошенничество: мониторинг // ВЦИОМ. 2024. 20 февраля. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 20.05.2024).

Таблица 2 (Table 2)

Распределение ответов на вопрос:
«Как Вам кажется, на сегодняшний день какова вероятность стать жертвой перечисленных видов преступлений для Вас и Ваших близких?», *% от ответивших*
Distribution of answers to the question: «What do you think is the probability of becoming a victim of these types of crimes for you and your loved ones today?», % of the respondents

Виды преступлений	Очень вероятно	Весьма вероятно	Мало-вероятно	Практически не вероятно	Затрудняюсь ответить
Банковские махинации (при кредитовании, при рассчетно-кассовом обслуживании, с депозитами и др.)	22	36	24	10	8
Кража персональных данных в Интернете (паспортные данные, СНИЛС, ИНН, номера счетов, коды банковских карт, паролей и др.)	34	39	15	8	4
Незаконное использование персональных данных	31	44	13	7	5
Мошенничество в Интернете (шантаж, «развод» на деньги в долг, подставные сайты, письма о якобы «выигрыше» и т. п.)	32	34	17	12	5
Взлом электронной почты, личной страницы, компьютера	32	41	14	7	6
Телефонное мошенничество (преступники выдают себя за сотрудника банка или разыгрывают из себя жертву и т. д.)	38	30	15	12	5

Данные свидетельствуют о разном восприятии угроз в зависимости от возраста. Молодые респонденты (18–23 и 24–29 лет) показывают относительно низкий уровень опасений по поводу киберугроз (57 и 63% соответственно). Поколения, выросшие в цифровую эпоху, могут ощущать уязвимость менее остро, полагаясь на свои адаптивные стратегии безопасности. Люди старшего возраста склонны воспринимать угрозы серьезнее: доля тех, кто считает вероятность стать сегодня жертвой того или иного киберпреступления высокой и очень высокой, составляет в среднем 69% в группе 30–39 лет, 71% – в группе 40–49 лет, и 76% в группе 50–60 лет. Эти возрастные группы, как правило, имеют больше финансовых активов и ресурсов, несут определенную финансовую ответственность за благополучие семьи, активно используют технологии в повседневной жизни, включая онлайн-банкинг, социальные сети и электронную почту.

Отметим, что в исследовании, проведенном ВЦИОМ, была выделена группа респондентов старше 60 лет, в которой сильные опасения киберугроз несколько снижались[1], что может быть связано с меньшей вовлеченностью в цифровое пространство и низким уровнем цифровой грамотности в этой возрастной группе. Эксперт по кибербезопасности отметил, что пожилые люди реже используют интернет, избегают сложных онлайн-транзакций и социальных сетей, чаще полагаются на помощь и поддержку своих детей или других родственников в вопросах, связанных с технологиями и безопасностью, больше доверяют традиционным методам защиты, таким как личные визиты в банк или хранение важных документов в бумажном виде.

Опасения трудоспособного населения относительно киберпреступлений связаны с уровнем их материального благосостояния. Полученные в нашем исследовании данные указывают на обратную зависимость между материальным благосостоянием и уровнем опасений перед киберпреступлениями: среди респондентов с низким и ниже среднего уровнем благосостояния тревожность достигает 73–75%, тогда как для респондентов среднего достатка показатель составляет 69%, а в группе с высоким уровнем благосостояния (выше среднего и богатые) – 61%. Обеспеченные респонденты проявляют больше «цифровой уверенности», вероятно, благодаря большим возможностям для инвестирования в меры кибербезопасности и обладают большим доступом к информационным ресурсам, что снижает их чувство уязвимости. Напротив, низкий уровень благосостояния может ограничивать доступ к качественным защитным технологиям и усиливает ощущение тревоги.

Самые распространенные киберпреступления, с которыми лично сталкивались респонденты: телефонное мошенничество (55%), мошенничество в интернете (41%), взлом электронной почты (33%), незаконное использование персональных данных (20%), кража персональных данных (15%), банковские махинации (10%). Данные опроса показывают любопытный контраст между уровнем опасений респондентов перед киберугрозами и их фактическим опытом столкновения с некоторыми киберпреступлениями. Так, например, считая наиболее вероятными киберпреступлениями незаконное использование и кражу персональных данных, респонденты сталкивались с ними относительно редко. Наоборот, в меньшей степени опасаясь телефонного мошенничества, респонденты сталкивались с ним чаще всего. Также отметим, что, согласно данным ВЦИОМ, лишиться денежных средств в результате действий телефонных мошенников *не опасаются* 73% опрошенных (отметили, что это вряд ли случится или не случится никогда)[2].

Согласно данным, полученным нами из опроса экспертов по кибербезопасности, телефонное мошенничество кажется людям менее сложным технически, а потому менее опасным по сравнению с кражей персональ-

[1] Цифровая самооборона // ВЦИОМ. 2024. 12 марта. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/cifrovaja-samooborona (дата обращения: 20.05.2024); Телефонное мошенничество: мониторинг // ВЦИОМ. 2024. 20 февраля. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 20.05.2024).

[2] Телефонное мошенничество: мониторинг // ВЦИОМ. 2024. 20 февраля. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 20.05.2024).

ных данных. Кроме того, относительно масштабное освещение в СМИ данной проблемы, предупреждения, рассылаемые различными организациями, в том числе правоохранительными органами, произвели определенный профилактический эффект. Эксперт отмечает: *«Многие наши соотечественники имеют опыт подобных историй, поэтому относятся весьма настороженно ко всем непонятным звонкам. Люди уже знакомы с такими сценариями мошенничества, как звонки с просьбами о личных данных или фальшивые уведомления о выигрышах, и более уверенно реагируют на эти ситуации»*.

Незаконное использование и кража персональных данных вызывает сильную тревогу из-за таких потенциальных долговременных серьезных последствий, как финансовые потери и нарушение личной безопасности. Эксперт–участковый инспектор говорит: *«Меньшее количество фактических случаев кражи персональных данных – это видимость. Такие преступления менее очевидны, их сложнее заметить, кроме того, в отношении этих случаев все-таки предпринимаются меры для их предотвращения»*.

Исследование выявило, что уровень образования выступает значимым дифференцирующим фактором в отношении вероятности столкновения с киберугрозами: чем выше образовательный уровень, тем чаще респонденты сообщают об опыте взаимодействия с киберпреступлениями (табл. 3).

Таблица 3 (Table 3)

Опыт столкновения горожан с киберпреступлениями в зависимости от уровня образования, %

Experience of citizens facing cybercrime depending on the level of education, %

Виды преступлений	Уровень образования			
	Среднее общее (11 классов) n = 102	Среднее специальное n = 387	Незаконченное высшее и высшее n = 646	Два высших, ученая степень n = 79
Банковские махинации (при кредитовании, при рассчетно-кассовом обслуживании, с депозитами и др.)	8	7	9	12
Кража персональных данных в Интернете (паспортные данные, СНИЛС, ИНН, номера счетов, коды банковских карт, паролей и др.)	9	10	16	30
Незаконное использование персональных данных	9	15	22	32
Мошенничество в Интернете (шантаж, «развод» на деньги в долг, подставные сайты, письма о якобы «выигрыше» и т. п.)	18	35	45	56
Взлом электронной почты, личной страницы, компьютера	23	27	37	39
Телефонное мошенничество (преступники выдают себя за сотрудника банка или разыгрывают из себя жертву и т. д.)	34	51	58	56

Анализ данных продемонстрировал различную степень связи между уровнем образования и типами киберпреступлений, с которыми сталкивались респонденты. Так, для банковских махинаций не было обнаружено статистически значимой связи ($\chi^2 = 7{,}491$; $p = 0{,}112$; $V = 0{,}076$), что, вероятно, обусловлено влиянием иных факторов, например, финансовой грамотности. В случаях взлома электронной почты и незаконного использования персональных данных выявлена слабая, но значимая связь с уровнем образования ($\chi^2 = 17{,}738$; $p = 0{,}001$; $V = 0{,}118$ и $\chi^2 = 22{,}721$; $p = 0{,}000$; $V = 0{,}133$, соответственно). Более выраженная связь обнаружена при анализе краж персональных данных ($\chi^2 = 33{,}775$; $p = 0{,}000$; $V = 0{,}162$) и интернет-мошенничества ($\chi^2 = 39{,}776$; $p = 0{,}000$; $V = 0{,}176$), что можно объяснить высокой активностью людей с высоким уровнем образования в цифровой среде, включающей онлайн-банкинг и социальные сети. Наиболее выраженная зависимость выявлена между уровнем образования и частотой столкновения с телефонным мошенничеством ($\chi^2 = 65{,}352$; $p = 0{,}000$; $V = 0{,}226$).

Важно отметить, что взаимосвязь между уровнем образования и частотой столкновений с мошенничеством едва ли обусловлена целенаправленным выбором образованных людей в качестве жертв. Как поясняет эксперт-социолог, активное использование цифровых технологий и онлайн-сервисов – от мобильных приложений и социальных сетей до банковских услуг – делает людей с высоким уровнем образования более подверженными контакту с киберпреступлениями. Хотя у этих респондентов развиты навыки критического мышления и осведомленность о мошенничестве, что помогает им быстрее распознавать угрозы, цифровая активность оставляет их в зоне риска. Эксперт по кибербезопасности добавляет, что как доступ к технологиям, так и высокий уровень цифровой грамотности служат одновременно факторами риска и защиты. Таким образом, более образованные люди оказываются, с одной стороны, более защищенными, но, с другой стороны, более вероятными целями для киберпреступников.

Особенности и тенденции киберпреступности в России

Особенности киберпреступности в России представляют собой сложную и развивающуюся картину, отражающую более широкие глобальные тенденции, но в то же время проявляющую и свою специфику. Большинство опрошенных нами экспертов сходятся во мнении, что для российской компьютерной преступности характерны следующие признаки:

1. На фоне тесной взаимосвязи с другими видами преступности, у киберпреступности имеется отчетливый самостоятельный характер, например, киберподразделения внутри традиционных преступных организаций способны функционировать автономно. *«Традиционные преступные организации, та же оргпреступность, начали формировать внутри свои отделы для совершения цифровых преступлений или для помощи в совершении традиционных преступлений, или даже для сокрытия привычных обычных преступлений»* – отмечает эксперт-криминолог.

2. Технологическая сложность и постоянная эволюция технологий и методов преступлений. Эксперты считают, что развитие искусственного интеллекта (ИИ) создало новую эру цифровых угроз. Эксперт-социолог говорит: *«Развитие интернета было своего рода первой технологической революцией. А появление и, главное, доступность искусственного интеллекта сегодня – это уже новая эра в технологиях, все последствия которой еще не видны и не осознаны»*. Криминолог добавляет: *«В отношении цифровых преступлений "ИИ" плюс интернет нам сразу дают колоссальную прибавку в скорости и масштабе»*.

3. Двойственная природа киберпреступности, сочетающая организованность и структурированность с гибкостью и адаптивностью. *«Мы имеем дело с противником, который одновременно структурирован, имеет четкую иерархию, разделение ролей и задач, и в тоже время непредсказуем за счет быстрой адаптации к изменениям. Организованные преступные группы могут использовать продвинутые техники планирования и атаки, но их гибкость позволяет им быстро изменять тактику при появлении новых защитных технологий, что требует от специалистов по безопасности постоянного мониторинга и адаптации мер защиты»*, – отметил специалист по информационной безопасности. Эксперт-криминолог дополнил, что *«в России одни из лучших IT-специалистов, и проблема не в технологической составляющей, а в том, что правоохранители ограничены правовыми нормами, процессуальностью действий. А преступники, считай, ничем не ограничены. Но даже в таких условиях около 25% киберпреступлений все-таки удается раскрыть»*.

4. Эксперты по кибербезопасности отмечают профессионализм и высокий уровень технологических навыков киберпреступников в России: *«Это не случайные кибератаки, а тщательно спланированные стратегии, направленные на использование конкретных уязвимостей в системах своих жертв»*.

5. Среди факторов уязвимости все эксперты назвали низкую киберграмотность населения и общий дефицит общественного и индивидуального понимания того, как обеспечить технологическую безопасность и защитить персональные данные. Как показало исследование, проведенное Минцифры России совместно с ГК «Солар», консалтинговым агентством НАФИ и СПбГУТ им. М. А. Бонч-Бруевича в 2022 г., общий индекс киберграмотности населения России составил 48,2 пункта из 100 возможных, 41% опрошенных не смогли назвать вообще ни одной киберугрозы. Опрос показал, что проблема фундаментальнее, нежели недостаточный опыт или владение цифровыми технологиями, – у людей, несмотря на доступность информации, не сложилось понимания того, что такое киберграмотность и зачем она нужна[1].

[1] Седов О. Кибергигиена: как защититься от мошенников // РБК. 2023. 30 ноября. URL: https://www.rbc.ru/opinions/society/30/11/2023/65671add9a79479923d8c15c (дата обращения: 16.06.2024).

6. Неосведомленность жертвы и высокая латентность явления. Зачастую жертвы киберпреступлений не подозревают, что они стали жертвами или пострадали. Утечка данных может оставаться незамеченной до тех пор, пока данные не будут использованы преступниками.

7. На фоне низкой информационной грамотности и невысокой осведомленности жертвы осведомленность преступников о жертве, напротив, часто относительно высокая. Киберпреступники могут быть хорошо информированы о своих целях, проводя предварительную разведку для использования конкретных уязвимостей. «*Социальные сети и онлайн-платформы предоставляют множество информации о пользователях, что увеличивает их уязвимость перед киберугрозами*», – отмечает эксперт-социолог.

8. Трансграничный и транснациональный характер преступлений, а также дистанционный характер преступных действий. По мнению эксперта-социолога, «*киберпреступность можно рассматривать как следствие глобальных экономических и социальных процессов, которые создают новые возможности для преступной деятельности. Ни одна страна не может эффективно противостоять этой угрозе в одиночку, но в этом моменте мы упираемся в различные геополитические процессы, которые затрудняют совместную работу*».

9. Сложность мотивов киберпреступников. Чаще всего целью киберпреступников является финансовая выгода: кража денежных средств, продажа данных. Однако необходимо отметить и другие цели: кража данных с целью манипуляции или шантажа, нарушение рабочих процессов в системах, вывод из строя критически важных объектов и провокация таким способом хаоса и страха, политические или идеологические цели, дезинформация или навязывание определенной позиции, шпионаж и др. Не менее важными являются психологические причины – удовлетворение потребности во власти и контроле, а также признании (например, в хакерских сообществах).

Все эти особенности делают киберпреступность куда более эффективной, нежели другие преступные отрасли.

Абсолютно все эксперты предрекли дальнейший рост киберпреступности в России и в мире, несмотря на достаточно профессиональные усилия правоохранительных органов. Это связано как с самой спецификой киберпреступлений, так и с переходом технических возможностей на совершенно новый уровень с появлением искусственного интеллекта (AI). Социологи и эксперты по кибербезопасности отметили, что со временем некоторые виды киберпреступлений все-таки исчерпают себя, но это произойдет не ранее, чем совершится следующий технологический скачок.

Выводы

Исследование продемонстрировало, что киберпреступность в России значительно возросла за последние годы, особенно в сфере телекоммуникаций и компьютерной информации: с 2013 по 2023 гг. количество пре-

ступлений увеличилось в 62 раза и продолжает расти. Основными видами киберпреступлений стали мошенничества с использованием электронных средств платежа и кражи, особенно в банковской сфере, что свидетельствует об адаптации киберпреступников к технологическим изменениям и применении ими все более изощренных методов.

Результаты проведенных опросов показывают, что значительная часть российских интернет-пользователей считает вероятность стать жертвой кибермошенничества высокой. Наибольшую опасность, по их мнению, представляют кражи и незаконное использование персональных данных, а также взломы электронной почты, что указывает на осознание рисков в цифровом пространстве. На фоне высокого уровня опасений перед интернет-угрозами одним из существенных факторов уязвимости остается низкая IT-грамотность населения. Несмотря на широкое распространение интернета и цифровых технологий, многим пользователям все еще недостает знаний для надежной защиты своих данных и устройств. При этом анонимность сети и трансграничный характер киберпреступлений усложняют их выявление и расследование, что усиливает латентность этих преступлений.

Проведенное нами исследование позволяет сделать вывод, что киберпреступность в России и мире приводит к изменениям, которые затрагивают не только технологическую сферу, но и структуру общества, поднимая новые вопросы безопасности, приватности и справедливости, а также этики. Распространение киберугроз выявляет важную проблему – растущее цифровое неравенство. Разные уровни цифровой грамотности и доступа к киберзащите формируют новую форму социального неравенства: те, кто может себе позволить более защищенные устройства и услуги, оказываются в привилегированном положении. Низкий уровень киберграмотности и невозможность обеспечить надежную защиту делают определенные группы особенно уязвимыми к киберпреступлениям, что углубляет социальные различия. Цифровая грамотность становится новой социальной нормой, а навыки безопасности в сети – столь же необходимыми, как и базовые образовательные умения. Все это актуализирует проблему социальной справедливости и доступности киберзащиты для всех слоев населения, включая малоимущих, пожилых людей и жителей сельских районов.

Развитие киберпреступности провоцирует глобальную дискуссию о правах на приватность и этике использования личных данных. Атаки на данные пользователей акцентируют внимание на том, как, кто и в каких целях имеет право на доступ к личной информации, и порождают общественный запрос на усиление политики приватности и правового регулирования в сфере защиты данных. В условиях глобальных изменений возникает потребность в обеспечении не только правовой, но и психологической и моральной безопасности пользователей, особенно в контексте таких явлений, как кибербуллинг, шантаж и мошенничество. Эти проблемы затрагивают уже не только финансовую стабильность, но и эмоциональное благополучие граждан. В этом контексте возникает новая этическая дилемма: в стремлении защитить общество от киберугроз расширяется

государственный контроль в цифровой среде, что вызывает опасения за права на личную свободу и приватность. Все более актуальной становится проблема баланса между безопасностью и свободой, что, в свою очередь, требует взвешенной политики, обеспечивающей прозрачность и обоснованность мер цифрового контроля. Данная дискуссия выходит за рамки национальных границ, предполагая необходимость международного сотрудничества и установления общих стандартов кибербезопасности. Однако политические и правовые барьеры усложняют процесс стандартизации, поэтому координация между странами остается проблематичной.

Таким образом, киберпреступность в России стала одной из самых острых проблем в сфере безопасности. Учитывая высокий уровень технических навыков киберпреступников и трансграничный характер угроз, эффективная борьба с ними требует координации на всех уровнях общества. Образовательные программы, направленные на повышение цифровой грамотности, играют ключевую роль в предотвращении кибератак и защите личных данных. Важным шагом также становится сотрудничество и обмен информацией между правоохранительными органами, коммерческими организациями и образовательными учреждениями. И социологическое изучение возникающих угроз и реакции общества на них, представляется безусловно важным.

Библиографический список

1. Аносов А. В. Современные тенденции развития цифровой криминологии // Академическая мысль. 2021. № 4(17). С. 56–59. EDN: RYTJNP.

2. Витвицкая С. С., Витвицкий А. А., Исакова Ю. И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. Т. 1. № 1. С. 18–27. DOI: 10.23947/2949-1843-2023-1-1-126-136; EDN: OKGPLW.

3. Гребеньков А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex Russica (Русский закон). 2018. № 4(137). С. 108–120. DOI: 10.17803/1729-5920.2018.137.4.108-120; EDN: XMJNCX.

4. Евдокимов К. Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д. юр. н. М.: Ун-т прок-ры РФ, 2022. 557 с.

5. Каримов А. М. Преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационно-коммуникационных технологий: сравнительно-правовой аспект // Вестник КЮИ МВД России. 2023. Т. 14. № 1(51). С. 75–82. DOI: 10.37973/KUI.2023.93.91.010; EDN: HZGCMZ.

6. Кибакин М. В. Актуальные проблемы рефлексии цифровой социальной реальности: переосмысление научных концепций // Цифровая социология. 2019. Т. 2. № 1. С. 4–9. DOI: 10.26425/2658-347X-2019-1-4-9; EDN: QODQXM.

7. Комлев Ю. Ю. Девиантность и преступность в эпоху high-tech, консьюмеризма и глэм-капитализма // Вестник КЮИ МВД России. 2018. № 1(31). С. 23–34. DOI: 10.24420/KUI.2018.31.11105; EDN: QMUQSH.

8. Комлев Ю. Ю. От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии // Российский девиантологический журнал. 2022. №2 (1) С. 17–26. DOI: 10.35750/2713-0622-2022-1-17-26; EDN: CLLGON.

9. Коробеев А. И., Дремлюга Р. И., Кучина Я. О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 416–425. DOI: 10.17150/2500-4255.2019.13(3).416-425; EDN: XBLGEH.

10. Крылова Ю. В. Компьютерная преступность: новые вызовы обществу // ЭКО. 2006. № 11(389). С. 174–179. EDN: HVNOKT.

11. Ницевич В. Ф. Цифровая социология: теоретико-методологические истоки и основания // Цифровая социология. 2018. Т. 1. № 1. С. 18–28. DOI: 10.26425/2658-347X-2018-1-18-28; EDN: YSZPRR.

12. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1(24). С. 45–55. EDN: OYYFEN.

13. Сергеев А. Ю., Широкова О. В. Мошенничество в цифровом обществе в условиях социальных изменений // Цифровая социология. 2023. Т. 6. № 1. С. 59–71. DOI: 10.26425/2658-347X-2023-6-1-59-71; EDN: GPOMJX.

14. Швыряев П. С. Киберпреступность как социальная проблема: стратегии противодействия: дис. ... к. социол. н. М.: МГУ им. М. В. Ломоносова, 2024. 189 с.

15. Kryshtanovskaya O. V., Chernavin Y. A., Lavrov I. A. Digital Generation: Mechanisms of Socialization and Social Prospects // Lecture Notes in Networks and Systems. 2022. Vol. 398 LNNS. P. 346–354. DOI: 10.1007/978-3-030-94870-2_44; EDN: UOABEN.

Получено редакцией: 25.06.24

СВЕДЕНИЯ ОБ АВТОРАХ

Позднякова Маргарита Ефимовна, кандидат философских наук, ведущий научный сотрудник Центра исследования адаптационных процессов в меняющемся обществе

Брюно Виктория Владимировна, кандидат социологических наук, старший научный сотрудник Центра исследования адаптационных процессов в меняющемся обществе

DOI: 10.19181/vis.2024.15.4.12

Development of the Information and Network Environment and Deviant Behaviour: Cybercrime as a New Social Threat

Margarita E. Pozdnyakova

Institute of Sociology of FCTAS RAS, Moscow, Russia
margo417@mail.ru
ORCID: 0000-0002-7896-5115

Victoriya V. Bruno

Institute of Sociology of FCTAS RAS, Moscow, Russia
victoria.bruno@mail.ru
ORCID: 0000-0001-9735-024X

For citation: Pozdnyakova M. E., Bruno V. V. Development of the Information and Network Environment and Deviant Behaviour: Cybercrime as a New Social Threat. *Vestnik instituta sotziologii.* 2024. Vol. 15. No. 4. P. 235–254. DOI: 10.19181/vis.2024.15.4.12; EDN: HOJENA.

Abstract. The presented article considers the problem of new digital threats. The study focuses on the main trends in the development of cybercrime in Russia and its specific country features. The authors' analysis of statistical data from various departments (the Ministry of Internal Affairs, the Prosecutor General's Office, Roskomnadzor) on the state and structure of crime showed that cybercrime in Russia has increased significantly in recent years, especially in the field of telecommunications and computer information. The most common types of cybercrime in Russian society are identified and analysed – various types of fraud and theft committed using information and communication technologies.

For the empirical basis of the study the data of an online survey of the urban working-age population (18–60 years old), conducted by employees of the Sector of Sociology of Deviant Behaviour of the Institute of Sociology of FCTAS RAS using a multi-stage quota sample (March-May 2024) is used. The attitude of city residents to various types of digital crime was assessed. It was found that many respondents consider the probability of becoming a victim of cyber fraud to be high, especially with regard to the illegal use of personal data and hacking of email.

It was found that the number of respondents who fear becoming a victim of cyber-crime increases with age. At the same time, these fears decrease in the oldest age groups. The level of education is also an important differentiating factor in relation to encountering cyber threats – the higher its level, the more often respondents have experience of encountering cyber crime.

A survey of experts was conducted to identify the key features of cyber-crime in Russia. Specialists from various fields were involved in the examination – from deviant researchers to practitioners involved in information security and with experience in working with cyber-crime. Their forecast for the coming years is disappointing – a further increase in cyber-crime is expected, the complexity of the techniques used, including the use of artificial intelligence, and therefore the development of specialised security solutions is necessary. It is shown that the main factors in the growth of cybercrime in Russia are its dual nature, manifested in simultaneous organisational complexity and structure, on the one hand, and flexibility and adaptability, on the other. In addition, cybercrime exacerbates an important social problem – growing digital inequality. Thus, cyber-crime in Russia poses a serious threat that requires a comprehensive approach and coordinated efforts at all levels of society to effectively suppress it.

Keywords: deviant behavior, cybercrime, information and communication technologies, cyber fraud, social engineering, computer crime, working-age urban population

References

1. Anosov A. V. Modern trends in the development of digital criminology. *Akademicheskaya mysl'*, 2021: 4(17): 56–59 (in Russ.). EDN: RYTJNP.

2. Vitvitskaya S. S., Vitvitsky A. A., Isakova Yu. I. Cybercrimes: concept, classification, international countering. *Pravovoy poryadok i pravovye tsennosti,* 2023: 1(1): 18–27 (in Russ.). DOI: 10.23947/2949-1843-2023-1-1-126-136; EDN: OKGPLW.

3. Grebenkov A. A. The concept of computer crimes, place in the criminal legislation of Russia and the place of information features in the structure of the elements. *Lex russica (Russkiy Zakon),* 2024: 4(137): 108–120 (in Russ.). DOI: 10.17803/1729-5920.2018.137.4.108-120; EDN: XMJNCX

4. Evdokimov K. S. Protivodeystvie komp'yuternoy prestupnosti: teoriya, zakonodatel'stvo, praktika [Combating computer crime: theory, legislation, practice]: dis. ... Dr. of Law. Moscow, Un-t prok-ry RF, 2022: 557 (in Russ.).

5. Karimov A. M. Computer crimes and crimes committed through the use of modern technology: a comparative legal aspect. *Vestnik KYuI MVD Rossii,* 2023: 14: 1(51): 75–82 (in Russ.). DOI: 10.37973/KUI.2023.93.91.010; EDN: HZGCMZ.

6. Kibakin M. V., Grishaeva S. A. The current problems of the digital reflection of social reality: rethinking scientific concepts. *Tsifrovaya sotsiologiya,* 2019: 2(1): 4–9 (in Russ.). DOI: 10.26425/2658-347X-2019-1-4-9; EDN: QODQXM.

7. Komlev Yu. Yu. Deviation and crimes in time of high-tech, consumerism and glamour capitalism. *Vestnik KYuI MVD Rossii,* 2018: 1(31): 23–34 (in Russ.). DOI: 10.24420/KUI.2018.31.11105; EDN: QMUQSH.

8. Komlev Yu. Yu. From digitalization of society to cybercrime, cyber deviance and the development of digital deviantology. *Rossiyskiy deviantologicheskiy zhurnal,* 2022: 2(1): 17–26 (in Russ.). DOI: 10.35750/2713-0622-2022-1-17-26; EDN: CLLGON.

9. Korobeev A. I., Dremlyuga R. I., Kuchina Ya. O. Cybercrimes in the Russian federation: criminological and criminal law analysis of the situation. *Vserossiyskiy kriminologicheskiy zhurnal,* 2019: 13(3): 416–425 (in Russ.). DOI: 10.17150/2500-4255.2019.13(3)416-425; EDN: XBLGEH.

10. Krylova Yu. V. Komp'yuternaya prestupnost': novye vyzovy obshchestvu [Computer Crime: New Challenges to Society]. *EKO,* 2006: 11(389): 174–179 (in Russ.). EDN: HVNOKT.

11. Nitsevich V. F. Digital sociology: theoretical and methodological origins and bases. *Tsifrovaya sotsiologiya,* 2018: 1(1): 18–28 (In Russ.). DOI: 10.26425/2658-347X-2018-1-18-28; EDN: YSZPRR.

12. Nomokonov V. A., Tropina T. L. Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new digital threat]. *Kriminologiya: vchera, segodnya, zavtra,* 2012: 1(24): 45–55 (in Russ.). EDN: OYYFEN.

13. Sergeyev A. Yu., Shirokova O. V. Fraud in a digital society in the context of social change. *Tsifrovaya sotsiologiya,* 2023: 6(1): 59–71 (in Russ.). DOI: 10.26425/2658-347X-2023-6-1-59-71; EDN: GPOMJX.

14. Shvyriaev P. S. Kiberprestupnost' kak sotsial'naya problema: strategii protivodeystviya. [Cybercrime as a Social Problem: Countermeasure Strategies]: dis. … cand. of social. sci. Moscow, Lomonosov MSU, 2024: 189 (in Russ.).

15. Kryshtanovskaya O. V., Chernavin Y. A., Lavrov I. A. Digital Generation: Mechanisms of Socialization and Social Prospects. *Lecture Notes in Networks and Systems,* 2022: 398: 346–354. DOI: 10.1007/978-3-030-94870-2_44; EDN: UOABEN.

The article was submitted on: June 25, 2024

INFORMATION ABOUT THE AUTHORS

Margarita E. Pozdnyakova, Candidate of Philosophical Sciences, Leading Researcher of the Center for the Study of Adaptation Processes in a Changing Society

Victoriya V. Bruno, Candidate of Sociological Sciences, Senior Research of the Center for the Study of Adaptation Processes in a Changing Society