МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Швыряев Павел Сергеевич

Киберпреступность как социальная проблема: стратегии противодействия

Специальность: 5.4.7 Социология управления

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата социологических наук

Москва – 2024

Работа выполнена на кафедре социологии управления факультета государственного управления Московского государственного университета имени М.В. Ломоносова.

Научный руководитель – **Судас Лариса Григорьевна**
доктор философских наук, профессор

Официальные оппоненты – **Петрунин Юрий Юрьевич**
доктор философских наук, профессор, ФГБОУ ВО «Московский государственный университет имени М.В.Ломоносова», факультет государственного управления, заведующий кафедрой математических методов и информационных технологий в управлении

Вершинина Инна Альфредовна
доктор социологических наук, доцент, ФГБОУ ВО «Московский государственный университет имени М.В.Ломоносова», социологический факультет, доцент кафедры современной социологии

Стырин Евгений Михайлович
кандидат социологических наук, Национальный исследовательский университет «Высшая школа экономики», заведующий Международной лабораторией цифровой трансформации в государственном управлении

Защита диссертации состоится «25» июня 2024 г. в 16:00 на заседании диссертационного совета МГУ.054.2 Московского государственного университета имени М.В. Ломоносова по адресу: 119991, Москва, Ломоносовский проспект, д. 27, корп. 4, корпус «Шуваловский», ауд. Е-834.

E-mail: msu.054.2@spa.msu.ru.

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на портале: https://dissovet.msu.ru/dissertation/2875

Автореферат разослан « » мая 2024 г.

Ученый секретарь
диссертационного совета,
кандидат социологических наук Е.В. Батоврина

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Киберпреступность – одна из главных угроз для человечества в XXI веке. Это неотъемлемый спутник цифровизации, но, к сожалению, негативная и крайне опасная сторона технологического развития. По мере нарастания масштабов технологической трансформации проблема киберпреступности вставала все более остро и в настоящий момент приобрела черты глобальной угрозы.

События нескольких последних лет показали, что глобальная система безопасности оказалась не готова к серьезным трансформационным изменениям. Не готова и социальная система: стремительный переход в онлайн во время пандемии, форсированная цифровизация и глобальные кибервойны стали вызовом для значительной части населения планеты и социальных институтов, чем оперативно воспользовались кибермошенники. Рост числа киберпреступлений в масштабах всей планеты – яркое проявление назревших проблем и противоречий, которые оказывают влияние и на восприятие технологий. По данным консалтинговой фирмы Edelman, 71% респондентов по всему миру обеспокоены вопросами кибербезопасности. Новые технологии могут обещать эру процветания, но одновременно вместо этого все чаще усугубляют проблемы доверия и выступают катализатором социальной нестабильности. Это еще раз подчеркивает важность и актуальность социологического анализа и осмысления проблем технологического развития в общем, и проблемы киберпреступности в частности; поднимает вопрос о реализации социально ориентированного технологического развития в масштабах всего человечества.

В настоящий момент накоплен колоссальный опыт для рефлексии и анализа событий последних нескольких лет. Очевидно, что актуальные стратегии цифровой безопасности и противодействия киберпреступности не эффективны на всех уровнях и требуют скорейшего пересмотра.

Очевидно также, что простого и быстрого решения через ужесточение законодательства или разработку нового антивируса не существует. Более того, за бесконечным обсуждением предложений об ужесточении мер за киберпреступления и попытками определить очередной источник нападения упускается сама суть киберпреступности как прежде всего социальной проблемы, которая исходит из социума и направлена на социум. Для решения потребуются методы иного порядка – интегративные, учитывающие как технологическую, так и социальную составляющую.

Таким образом, социальная проблема заключается в неконтролируемом росте масштабов и глубины киберпреступности, с одной стороны, и неэффективности используемой стратегии борьбы, с другой. Научная проблема заключается в недостаточной проработанности социологического понимания феномена киберпреступности при его возрастающей значимости.

Степень разработанности темы исследования. Несмотря на то, что активно подчеркивается значимость проблемы киберпреступности и растет ее влияние в последние годы, адекватный подход к ее решению еще только предстоит выработать. Безусловно, говоря о проблеме киберпреступности, нельзя не отметить достижения исследователей в области технологий и защиты информации. Однако в данном исследовании нас интересуют, прежде всего, исследования из области социальных наук.

Киберпреступность является объектом междисциплинарных исследований. Однако, безусловно доминирующим подходом к ее исследованию является правовой подход. Киберпреступность как объект правового регулирования в своих работах рассматривают Христинина Е.В., Медведева Е.И. и Крошилин С.В., Старостенко О.А., Тимофеев А.В. и Комолов А.А., Бутусова Л.И., Алексеев С.В., Кобец П.Н., Витвицкая С.С., Витвицкий А.А., Исакова Ю.И, Волынская О.В., Кумышева М.К. и Геляхова Л.А., Мартьянов Н.Р., Тарасик Н.М., Карцхия А.А. и Макаренко Г.И. и

другие[1]. В рамках данного направления авторы исследуют вопросы специфики правового регулирования киберпреступлений, правовые основы предупреждения киберпреступлений, понятия и классификации киберпреступлений в российском и зарубежном праве, актуальное состояние и перспективы правового регулирования киберпреступлений, особенности уголовно-правовой борьбы с киберпреступлениями.

Еще один контекст, в котором анализируется проблема киберпреступности, – концепция корпоративной социальной

---

[1] Христинина Е.В. К вопросу об уголовно-правовом противодействии киберпреступности / Е.В. Христинина // Вестник Сибирского юридического института МВД России. – 2021. – №4 (45). – С. 150 – 154.

Медведева Е.И., Крошилин, С. В. Финансовое мошенничество в период пандемии COVID–19 / Е. И. Медведева, С. В. Крошилин // Народонаселение. – 2022. – Т. 25. – № 1. – С. 29–42.

Старостенко О.А. Закономерности становления и развития кибермошенничества в России и за рубежом / О.А. Старостенко // Вестник Уральского юридического института МВД России. 2021. №1. С. 138 – 143.

Тимофеев А.В., Комолов А.А. Киберпреступность как социальная угроза и объект правового регулирования / А.В. Тимофеев, А.А. Комолов // Вестник МГОУ. Серия: Философские науки. – 2021. – №1. – С. 95–101.

Бутусова Л.И. К вопросу о киберпреступности в международном праве / Л.И. Бутусова // Вестник экономической безопасности. – 2016. – №2. – С. 45–55.

Алексеев С.В. Специфика правового регулирования киберпреступлений, совершаемых преступной группой / С.В. Алексеев // Вопросы российского и международного права. – 2020. – Том 10. № 11А. – С. 97–102.

Кобец П.Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт / П.Н. Кобец // Научный вестник Омской академии МВД России. – 2022. №2 (85). – С. 101–105.

Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие / С.С. Витницкая, А.А. Витницкий, Ю.И. Исакова // Правовой порядок и правовые ценности. – 2023 – Т.1 №1. – С. 18–27.

Волынская О.В. Развитие юридической мысли и перспективы в борьбе с киберпреступностью в сфере уголовного судопроизводства / О.В. Волынская // Вестник Московского университета МВД России. – 2020. – № 3. – С. 72–74.

Кумышева М.К., Геляхова Л.А. К вопросу о киберпреступности в России и мире / М.К. Кумышева, Л.А. Геляхова // Пробелы в российском законодательстве. – 2018. – № 4. – С. 383–385.

Мартьянов Н.Р. Уголовно-правовая борьба с киберпреступлениями на современном этапе / Н.Р. Мартьянов // Государственная служба и кадры. – 2020. – № 1. – С. 175–177.

Тарасик Н.М. Анализ правовых основ борьбы с киберпреступностью / Н.М. Тарасик // Успехи в химии и химической технологии. – 2016. – № 5(174). – С. 66–68.

Карцхия А.А. и Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности / А.А. Карцхия, Г.И. Макаренко // Вопросы кибербезопасности. – 2023. – № 1 (53). – С. 58–74.

ответственности. В условиях непрерывной цифровой трансформации компании все чаще выходят за рамки традиционных стратегий корпоративной социальной ответственности и развивают свою корпоративную цифровую ответственность, проводят ответственную цифровую трансформацию. Вопросы ответственной корпоративной цифровой трансформации исследуются в работах таких авторов, как Мюллер Б., Хамади Х. и Манзо К. и другие[2].

Набирают популярность и исследования цифровой трансформации на уровне индивида. Исследованию процессов интегрирования цифровых технологий в рабочих и нерабочих активностях посвящены работы авторов: Кастеллано С., Чандавимол К., Кхеллади И. и Орхан М.А., Даравонг С., Дери К., Себастьян И.М. и Ван Дер Мейлен Н. и других[3].

Таким образом, исследуется происходящий на всех трех уровнях – социальном, организационном и индивидуальном – общий тотальный процесс цифровой трансформации, опирающийся на единый набор ценностей: безопасность, стабильность, устойчивость.

Важно отметить, что значительная часть современных исследований проблемы киберпреступности имеет узконаправленный, прикладной характер, что делает особенно актуальным запрос на проведение глубокого и комплексного анализа проблемы киберпреступности.

Можно выделить несколько направлений в рамках исследования социальных аспектов технологического развития, которые имеют важное методологическое значение для исследования проблемы киберпреступности.

---

[2] Mueller, B. Corporate Digital Responsibility. Bus Inf Syst Eng 64, 689–700 (2022).
Hamadi H, Manzo C. (2021) Corporate digital responsibility – a study on managerial challenges for AI integration in business. Lund University, Lund.

[3] Castellano, S., Chandavimol, K., Khelladi, I., & Orhan, M. A. (2021). Impact of selfleadership and shared leadership on the performance of virtual R&D teams. Journal of Business Research, 128, 578–586.
Darawong C. (2018). Dynamic capabilities of new product development teams in performing radical innovation projects. International Journal of Innovation Science, 10 (3), 333–349.
Dery, K., Sebastian, I. M., and van der Meulen, N. (2017). The Digital Workplace is Key to Digital Innovation. MIS Quarterly Executive, 16(2), 135–152.

Одно из ключевых направлений – концепция «социальной оценки техники» (Technology Assessment), которая объединяет исследователей социальных аспектов развития технологий. К ведущим зарубежным представителям данного направления относятся Грунвальд А., Скот Дж. и Рип А., Грин Дж. и другие, Гастон Д. и Саревич Д. и другие[4]. Среди российских исследователей можно отметить работы Хана Ю. и Кулакова П., Попковой Н.В., Розина В.М., Дубровского Д.И., Гаврилиной Е.А., Ефременко Д.В., Пржиленского В.И., Михайлова И.Ф., Никифоровой Н.В., Пирожковой С.В. и других[5]. В рамках данного направления исследователи затрагивают вопросы пути развития глобальной социальной оценки техники,

---

[4] Grunwald A. Technology Assessment or Ethics of Technology? Reflections on Technology Development between Social Sciences and Philosophy // Ethical Perspectives. – 1999. – vol. 6. – P. 170–182.

Schot J., Rip A. The past and future of constructive technology assessment // Technological Forecasting and Social Change. – 1997. – vol. 54, no. 2–3. – P. 251–268.

Grin J., van de Graaf H., Hoppe R., Groenewegen, P. Technology assessment through interaction. A guide // Den Haag: Rathenau Instituut. – 1997. – P. 98.

Guston D.H., Sarewitz D. Real-time technology assessment // Technology in Society. – 2002. – vol. 24. – P. 93–109.

[5] Хан Ю., Ладикас М., Кулаков П. Развитие глобальной социальной оценки техники: пути продвижения, параметры и ограничения // Философия науки и техники. – 2019. – №2. – С. 96 – 108.

Попкова Н.В. Место философии в культуре техногенного общества: критика технического разума / Н.В. Попкова // Культура и искусство. – 2019. – № 4. – С. 37–52.

Розин В.М. Изучение и понятие техники (взгляд от методологии и культурологии) / В.М. Розин // Культура и искусство. – 2021. – № 4. – С. 74–81.

Дубровский Д.И. Развитие искусственного интеллекта и глобальный кризис земной цивилизации (к анализу социогуманитарных проблем) / Д.И. Дубровский // Философия науки и техники. – 2022. – Т. 27. № 2. – С. 100–107.

Гаврилина Е.А. Редукция человеческой агентности в технологическом контексте / Е.А. Гаврилина // Философия науки и техники. – 2022. – Т. 27. № 2. – С. 108–120.

Ефременко Д.В. Введение в оценку техники. М.: Изд-во Международного независимого эколого–политологического ун-та. – 2002. – 186 с.

Пржиленский В.И. Понятие цифровой реальности: значение и смысл / В.И. Пржиленский // Философия науки и техники. – 2021. – Т. 26. № 2. – С. 68–80.

Михайлов И.Ф. Вычислительный подход в социальном познании / И.Ф. Михайлов // Философия науки и техники. – 2021. – Т. 26. № 1. – С. 23–37.

Никифорова Н.В. Эстетическое измерение техники: динамо–машина как технологическое возвышенное на рубеже XIX и XX вв. / Н.В. Никифорова // Философия науки и техники. – 2020. Т. 25. № 2. – С. 37–50.

Пирожкова С.В. Форсайт («Foresight») как форма социального проектирования / С.В. Пирожкова // Философия науки и техники. – 2019. Т. 24. № 2. – С. 109–123.

рассматривают вопросы оценки техники, что имеет важное значение, в том числе и для понимания природы киберпреступности.

Значимым направлением анализа одного из аспектов проблемы цифровизации является исследование цифрового неравенства. Данная проблема остается актуальной в России и является одним из барьеров на пути борьбы с киберпреступностью. Исследования цифрового неравенства в России частично представлены в трудах Добринской Д.Е. и Мартыненко Т.С., Волченко О.В., Ициксона А.И. и других[6].

Информационные технологии – важный фактор социализации. Проблематике влияния технологий на поведение и развитие человека посвящены работы Вершининой И.А. и Лядовой А.В., Шаполовой И.С., Джулай Д.В., Паклиной В.В. и Бондарева С.И., Краснокутского Д.Н., Бойко Н.Л., Абрадовой Е.С. и Кисловской Е.В. и других[7].

Таким образом, актуальные вопросы и проблемы цифровизации не остаются без внимания социологической науки, в том числе и киберпреступность. Однако исследуются преимущественно отдельные

---

[6] Добринская Д.Е., Мартыненко Т.С. Перспективы российского информационного общества: уровни цифрового разрыва / Д.Е. Добринская, Т.С. Мартыненко // Вестник РУДН. Серия: Социология. – 2019. – №1. – С. 108–120.

Волченко О.В. Динамика цифрового неравенства в России / О.В. Волченко // Мониторинг общественного мнения : Экономические и социальные перемены. – 2016. – No 5. – С. 163–182.

Ициксон А.И. Устранение цифрового неравенства / А.И. Ициксон // Вестник ЮУрГУ. Серия «Экономика и менеджмент». – 2017. – Т. 11, № 4. – С. 156–164.

[7] Вершинина И.А., Лядова А.В. Трансформация повседневности современного человека под влиянием технологий искусственного интеллекта / И.А. Вершинина, А.В. Лядова // Теория и практика общественного развития. – 2023. – № 6. – С. 73–78.

Шаповалова И. С. Влияние интернет-технологий на поведение и интеллектуальное развитие молодежи / И.С. Шаповалова // Социологические исследования. – 2015. – № 4 (372). – С. 148–151.

Джулай Д.В., Паклина В.В., Бондарев С.И. Анализ влияния интернета на современную молодежь / Д.В. Джулай, В.В. Паклина, С.И. Бондарев // Известия Института систем управления СГЭУ. – 2015. – № 2 (12). – С. 51–54.

Краснокутский Д.Н. Молодежь и социальные сети интернет: теоретико-прикладной анализ / Д.Н. Краснокутский // Общество и право. – 2017. – № 1 (59). – С. 196–199.

Бойко Н.Л. Молодежь эпохи интернет на пороге взрослой жизни: социологический анализ / Н.Л. Бойко // Социологический альманах. – 2014. – № 5. – С. 358–366.

Абрадова Е.С., Кисловская Е.В. Молодежь в социальных сетях / Е.С. Абрадова и Е.В. Кисловская // Власть. – 2018. – Т. 26. № 3. – С. 150–153.

аспекты киберпреступности. Социальная природа киберпреступности, ее социальные основания и механизмы формирования исследованы слабо, а социологическое понимание киберпреступности еще только предстоит выработать. Данное положение вещей еще раз обосновывает актуальность темы исследования и необходимость глубокого и комплексного анализа этой проблемы с привлечением ресурсов социологии и социологии управления.

Актуальность проблемы и ее недостаточная проработанность, необходимость более глубокого социологического анализа феномена киберпреступности предопределили цели и задачи данного исследования.

Объект исследования – киберпреступность как социальное явление.

Предмет исследования – стратегии противодействия киберпреступности.

Цель исследования – на основании выявления социальной природы киберпреступности сформулировать предложения по оптимизации стратегии противодействия киберпреступности.

Данная цель реализуется посредством решения следующих **задач**:

1. Проанализировать актуальное состояние киберпреступности в России и выявить ключевые тенденции развития проблемы за последние 5 лет.
2. Раскрыть и обосновать социальную природу киберпреступности, предложить социологическое определение данного понятия.
3. Определить уровень понимания социальной природы киберпреступности и рисков цифровой трансформации экспертным сообществом и общественностью.
4. Обосновать объективную потребность и основные направления коррекции существующих подходов в противодействии киберпреступности.
5. Развить концептуальную основу возможной альтернативной стратегии противодействия киберпреступности.

6. Сформулировать основные принципы и составляющие альтернативной стратегии противодействия киберпреступности.

Гипотеза исследования. Глубокое понимание социальной природы киберпреступности позволит обосновать неэффективность актуальных стратегий в борьбе с киберпреступностью и будет способствовать выработке альтернативной, более эффективной стратегии противодействия киберпреступности.

В качестве **теоретико-методологической основы** диссертационного исследования используются общенаучные методы (анализ и синтез, индукция и дедукция, сравнительный анализ и др.), подходы из области социологии управления, цифровой социологии, социологии преступности, социальной оценки технологий. Использованы достижения исследований науки и технологий (STS, Science and Technology Studies) и их ключевых представителей – Бруно Латура[8] и Джона Ло[9]. В работе применены идеи теории социального конструирования технологий[10] (SCOT), понимание технологических артефактов как социальных конструкций, а развития технологий – как непрерывного конфликтного процесса обсуждения и поиска консенсусного варианта среди различных социальных групп через множество итераций, а также развиваемая Полом Эдвардсом идея со-конструирования общества и технологий[11].

При проведении прикладного социологического исследования использовался метод экспертного опроса.

---

[8] Латур Б. Об интеробъективности / Пер. с англ. А. Смирнова под науч. ред. В. Вахштайна / Социологическое обозрение. – 2007. – Том 6. № 2. – С. 81–98.

[9] Ло Дж. После метода: беспорядок и социальные науки. М.: Издательство института Гайдара. – 2015. – 352 с.

[10] Pinch, Trevor J. and Wiebe E. Bijker. The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other // Social Studies of Science. – 1984. – Vol. 14. – P. 399–441.

[11] Edwards P. N. Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems // Modernity and Technology. Cambridge, MA: MIT Press. – 2003. – P. 185–225.

Информационная база исследования. В диссертационном исследовании использованы нормативные правовые акты в сфере противодействия киберпреступности и информационных технологий в России; данные статистики; материалы специализированных сайтов; деловые периодические издания, отражающие тенденции и актуальное состояние киберпреступности в России и мире. Использованы материалы многопрофильных исследовательских центров Pew Research Center и НАФИ, Банка России, материалы компаний DoubleVerify, McKinsey & Company, Edelman, Upwork, InfoWatch, Hootsuite, Gartner, Всемирного экономического форума, Surfshark, SEON, Positive Technologies, материалы мероприятий в сфере кибербезопасности: Цифровая устойчивость и информационная безопасность России 2024, SberProTech 2023, доклады, сделанные на Международном Конгрессе по кибербезопасности, а также данные авторского экспертного опроса.

Научная новизна исследования состоит в социологической концептуализации феномена киберпреступности, позволившей по-новому подойти к выработке эффективной научно обоснованной стратегии противодействия киберпреступности. Автором лично получены следующие результаты:

1. Раскрыта социальная природа киберпреступности, показан социальный механизм ее формирования и функционирования, ее социальные основания. Это открывает новые возможности концептуализации происходящих в этой сфере процессов, прогнозирования их динамики, а также новые перспективы в решении проблемы регулирования киберпреступности.

2. На основании теоретической модели и статистики МВД РФ и аналитических отчетов исследовательских компаний проанализировано актуальное состояние киберпреступности в России. Выявлены и теоретически интерпретированы ключевые тренды последних 5 лет: рост

количества зарегистрированных киберпреступлений более чем в 5 раз; рост доли нераскрытых киберпреступлений; рост количества утечек конфиденциальных данных, персональных данных и платежной информации; рост количества атак на малые и средние предприятия; рост количества киберпреступлений, совершенных с использованием методов социальной инженерии; рост доли утечек информации умышленного характера; рост количества атак из-за пределов страны.

3. На основе выявленной динамики киберпреступности и ее характера обоснован и подтвержден экспертными интервью вывод об ограниченности и неэффективности актуальной стратегии борьбы с киберпреступностью, не позволяющей взять ее под контроль, и необходимости выработки и реализации стратегии, основанной на более глубоком понимании социальной природы и социального механизма формирования и функционирования киберпреступности.

4. Развивается концепция устойчивого цифрового развития, которая используется в диссертации в качестве основы альтернативной стратегии противодействия киберпреступности.

5. Обоснованы основные принципы и характерные особенности альтернативной стратегии противодействия киберпреступности, которая базируется на новом ценностном подходе, в основе которого – приоритет безопасности, надежности, устойчивости, и носит системный, долговременный, непрерывный, упреждающий характер.

Положения, выносимые на защиту.

1. Киберпреступность пока не удается взять под контроль. Рост масштабов киберпреступности, глубины ее проникновения в общество, ее разрушительного воздействия на общества, проходящие стадию цифровой трансформации, требует перехода от тактических мер по решению текущих проблем к стратегическим решениям, переводит в практическую повестку

дня вопрос о выработке эффективной долговременной стратегии противодействия киберпреступности.

2. Понимание социальной природы киберпреступности может быть основано на идее социального и технического со-конструирования социотехнических систем, которые формируются при появлении новых технических возможностей в борьбе противоборствующих интересов различных социальных групп. *Под киберпреступностью понимается незаконная деятельность по поиску и эксплуатации социальных и технических уязвимостей социо-цифровой системы.* Киберпреступность возникает и активизируется на стыке технического и социального, в условиях дисбаланса между ними, возникающего, когда происходит освоение обществом новых цифровых технологий. Современные масштабы и последствия киберпреступности – это симптом перехода преступности в киберпространство и ее превращения в одного из основных бенефициаров цифровизации, при одновременном нарастании рисков и угроз для других сторон этого процесса.

3. Анализ пятилетней динамики развития киберпреступности в России позволяет сделать вывод о критическом росте значения социальных факторов киберпреступности. По мере нарастания технических возможностей защиты фокус внимания киберпреступного сообщества сместился в сторону человека – к самому слабому звену в системе защиты от киберугроз.

4. Актуальное состояние социо-цифровой системы характеризуется высоким динамизмом и в то же время недостаточным вниманием к ее социальной стороне. В результате в системе непрерывно возникают, но не нейтрализуются уязвимости, которые активно эксплуатируются киберпреступниками. Эффективная стратегия противодействия киберпреступности должна быть направлена на создание такого состояния

системы, в котором вероятность эксплуатации уязвимостей минимизирована, а порог проникновения сквозь защитный барьер системы высок и сложен.

5. Эффективная стратегия противодействия киберпреступности может быть выстроена на основе концепции устойчивого цифрового развития, которая активно вырабатывается в последние годы. Для устойчивого цифрового развития характерен такой подход к проектированию, внедрению и масштабированию цифровых продуктов и устройств, который обеспечивает минимальные риски (технологические и социальные) зарождения и распространения преступной деятельности в рамках как всей социо-цифровой системы, так и ее отдельных частей. Конечные цели стратегии противодействия киберпреступности при таком подходе заключаются в переходе к устойчивому цифровому развитию с приоритетом кибербезопасности и выработки «цифрового иммунитета», т.е. создание цифровых систем, способных выдержать широкий диапазон рисков и уязвимостей, т.е. устойчивых к киберпреступности.

6. Основные принципы эффективной стратегии противодействия киберпреступности – системность, долговременность, непрерывность, упреждающий характер. Она должна базироваться на новом ценностном подходе при проектировании, разработке и внедрении цифровых систем, в основе которого – приоритет надежности и устойчивости социо-цифровых систем. Стратегия противодействия должна включать непрерывный аудит, направленный на поиск и прогнозирование уязвимостей социо-цифровой системы; выстраивание и реализацию долговременной политики по подготовке и удержанию высококвалифицированных ИТ-специалистов; долгосрочную, масштабную и тщательную работу с населением в области повышения цифровой грамотности и уровня информирования, формирование культуры цифрового доверия; оперативное и своевременное правовое сопровождение; модернизацию правоохранительной системы; поддержание

доверительных международных отношений в противодействии киберпреступности и расследовании кибер-инцидентов.

Теоретическая значимость диссертационной работы заключается в развитии теоретических и методологических основ изучения феномена киберпреступности, задающих перспективу его дальнейшего социологического и междисциплинарного исследования; в углублении теоретических представлений о социальной природе киберпреступности, социальном механизме, социальных основаниях и закономерностях ее формирования и функционирования. Развиваемая теоретическая концепция позволяет объяснить динамику киберпреступности в России, низкую эффективность актуальной стратегии противодействия киберпреступности и сформулировать принципы альтернативной стратегии, привлекая концепцию устойчивого цифрового развития.

Практическая значимость диссертационной работы заключается в возможности использовать полученные результаты в рамках разработки эффективных стратегий противодействия киберпреступности на межгосударственном, государственном и организационном уровнях. Результаты диссертационного исследования могут быть использованы органами государственной власти, менеджментом организаций, в учебном процессе при подготовке курсов «Социология управления», «Социология преступности», «Государственное и муниципальное управление», «Социология киберпреступности» в высших учебных заведениях.

Апробация результатов исследования. Результаты исследования были представлены на научных конференциях, в числе которых:

1. Международная научная конференция студентов, аспирантов и молодых ученых «Ломоносов-2020».

2. XVII Международная научно-практическая конференция, посвященная памяти М.И. Ковалева, 2020 год.

3. Международная научная конференция студентов, аспирантов и молодых ученых «Ломоносов-2023».

Публикации. По теме исследования опубликовано 5 научных работ общим объемом 4,5 п.л. (3,7 авторских п.л.), в том числе 5 статей объемом 4,5 п.л. (3,7 авторских п.л.) в изданиях, рекомендованных для защиты в диссертационном совете МГУ имени М.В. Ломоносова по специальности 5.4.7 – Социология управления. Публикации, выполненные автором лично, в которых отражены основные результаты, положения и выводы исследования, использованы при подготовке диссертационной работы.

Структура, содержание и объем диссертации позволяют раскрыть поставленные задачи исследования и достичь заявленной цели. Работа изложена на 189 страницах, состоит из введения, двух глав, заключения, списка литературы, включающего 264 источников, содержит 9 рисунков, 1 приложение.

II. ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во Введении обосновывается актуальность заявленной темы, степень ее разработанности, формулируется объект, предмет, цели, задачи исследования и гипотеза, описываются теоретико-методологические основы, информационная база исследования, научная новизна, перечисляются положения, выносимые на защиту. Формулируется теоретическая и практическая значимость работы и освещаются основные формы апробации результатов.

Первая глава «**Социологическая концептуализация киберпреступности**» посвящена исследованию актуального состояния киберпреступности в России и динамики развития проблемы в стране в последние 5 лет. В ней выстраивается теоретическая социологическая модель киберпреступности.

В параграфе 1.1 «**Актуальное состояние и динамика киберпреступности в России**» анализируется официальная статистика МВД

РФ за 2017-2023 годы и аналитические отчеты российской исследовательской компании InfoWatch. Цель данного анализа – выявить ключевые тенденции развития киберпреступности в России и мире за последние несколько лет.

В рамках данного параграфа используется определение Министерства внутренних дел РФ. Киберпреступность – *преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.*

В начале параграфа рассматриваются определения киберпреступности с позиций правовой и криминологической науки. Отмечается, что несмотря на популярность термина «киберпреступность» среди российских публичных должностных лиц и СМИ, термин не используется и не раскрывается в современном российском законодательстве, что поднимает вопрос о своевременном и адекватном правовом сопровождении борьбы с киберпреступностью.

На основании обобщенного анализа официальной статистики, новостной повестки, отчетности аналитических центров и оценок экспертов выявлены ключевые тенденции последних 5 лет.

По состоянию на 2024 год в России киберпреступность приобрела черты угрозы государственного масштаба.

Отмечается тренд на рост количества киберпреступлений с использованием методов социальной инженерии в России. Данный процесс является проявлением глобального тренда на «поворот» от технологии к человеку – наиболее незащищенному элементу системы.

Сохраняется высокая доля нераскрытых киберпреступлений и высокая степень латентности киберпреступности.

Увеличивается количество атак из других стран, в том числе недружественных.

В российском обществе сформировался отчетливый запрос на безопасные технологические системы. Существует и запрос на повышение цифровой грамотности населения.

Фиксируется значительный рост количества утечек конфиденциальных данных в 2022 году: более чем в 2,1 раза по сравнению с 2021 годом. Проблема утечек конфиденциальных данных приобрела массовый характер и в настоящее время затрагивает практически все активное население страны.

Согласно официальным данным Банка России, в 2022 году главными потерпевшими по операциям, произведенным без согласия клиентов финансовых организаций, являются физические лица. Причем точность киберпреступных атак растет: если раньше были популярны масштабные охватные кампании, рассчитанные на большое количество потенциальных жертв, то в настоящее время киберпреступники фокусируются на конкретных жертвах.

В 2022 году, на фоне беспрецедентного санкционного давления, российская экономика взяла курс на импортозамещение, в том числе и технологических систем. Данный процесс – очередной масштабный виток технологического развития страны, который сопряжен с серьезными рисками и угрозами, в том числе и со стороны киберпреступного сообщества.

Отток высококвалифицированных специалистов в 2022 году – серьезный удар для российской экономики и технологического развития на годы вперед. Данная проблема имеет отложенный эффект, и степень серьезности ее последствий можно будет оценить только спустя годы.

Таким образом, в России еще не сложилась надежная, отказоустойчивая система безопасности, готовая успешно отражать как внутренние, так и внешние вызовы и угрозы, назрела потребность в пересмотре сложившейся стратегии борьбы с киберпреступностью.

Параграф 1.2 **«Социальная природа киберпреступности»** направлен на углубление понимания феномена киберпреступности.

В рамках первого параграфа использовалось понятие киберпреступности, используемое прежде всего в целях квалификации определенных деяний как киберпреступлений. Во втором параграфе киберпреступность рассматривается как социальное явление и определяется как непрерывная криминальная деятельность по поиску и эксплуатации социальных уязвимостей социо-цифровой системы. Социо-цифровая система состоит из двух составляющих: первая – цифровая – как совокупность цифровых продуктов и технологий, по поводу которых и возникают социальные отношения. Вторая – социальная – как совокупность всех социальных отношений по поводу производства и использования цифровых технологий и продуктов, а также социальные отношения, протекающие в цифровой реальности. В совокупности эти составляющие и образуют социо-цифровую систему, в среде которой исследуется киберпреступность в рамках диссертационной работы.

Данное понимание киберпреступности дает перспективу для дальнейшего глубокого анализа социальной природы киберпреступности как сознательной, целенаправленной преступной деятельности с использованием цифровых технологий и устройств. В параграфе описывается краткая история развития киберпреступности, анализируется процесс ее превращения в глобальную проблему, которая в настоящее время глубоко интегрирована в социальную жизнь.

Анализ кибер-инцидентов последних лет показал, что вслед за все более обстоятельной интеграцией цифровых технологий в жизнь человека растет и уровень угроз, в том числе и киберпреступности. Эти кибер-инциденты, в том числе и связанные с киберпреступностью, имеют не случайный, а закономерный, системный характер и рассматриваются как единый процесс через призму постоянной смены цифровых эпох и формирования нового состояния социо-цифровой системы.

Цифровая технология или цифровое устройство – это продукты человеческой деятельности, которые аккумулируют в себе культурные ценности конкретного этапа технологического развития. Со-конструирование социальной и технической стороны единой социо-цифровой системы – это двусторонний процесс. Данное понимание технологического развития дает перспективу для более системного и глубокого понимания феномена киберпреступности, фокусирует внимание прежде всего на анализе возможностей и ограничений социальной системы, ее активного участия в процессе технологического развития, наращивания возможностей влияния общества и государства, в том числе через усиления контроля над киберпреступностью.

Тенденции последних лет в России, связанные с периодами форсированной цифровизации, курсом на импортозамещение, реализацией глобальных цифровых проектов в масштабах всей страны, сформировали новое, разбалансированное состояние системы, что отчетливо проявилось в росте количества киберпреступности и кибер-инцидентов в последние 5 лет.

Решение проблемы киберпреступности в сложившейся ситуации требует более глубоких, системных мер с использованием инструментов долгосрочного социального прогнозирования и мониторинга с целью выстраивания гармоничного баланса между технологическим и социальным, и в конечном итоге переходу к устойчивому цифровому развитию. Исследованию данного вопроса посвящена вторая глава диссертации.

Во второй главе **«Стратегия противодействия киберпреступности в парадигме устойчивого цифрового развития»** ставится цель выработать и обосновать долгосрочный эффективный подход к борьбе с киберпреступностью.

Параграф 2.1 «**Проблема киберпреступности в России в оценке экспертов**» направлен на исследование восприятия проблемы цифрового

развития и киберпреступности в российском обществе и профессиональном сообществе.

В 2023 году в рамках проекта «Концепт “цифрового рая” как пространство общественных ожиданий и страхов» было проведено исследование рабочей группой, в которую вошли эксперты Центра СИТИ НИУ ВШЭ и Фонда «Петербургская политика». Результаты исследования показали, что несмотря на рост количества кибер-инцидентов в последние годы в России и мире, 60% россиян можно охарактеризовать как технооптимистов: они положительно оценивают роль цифровых технологий в будущем. Не проявляется высокий уровень осознания важности и серьезности проблемы киберпреступности и при оценке минусов цифровизации. Несмотря на то, что проблема киберпреступности сегодня касается каждого гражданина страны, приоритетными являются экономические страхи и личные переживания из-за сокращения социальной коммуникации. Лишь третьим пунктом идет страх утечек конфиденциальных данных, что является важной, но далеко не единственной опасностью, исходящей от киберпреступности.

Исследование в рамках диссертационной работы представлено результатами экспертного опроса специалистов, направленного на выявление уровня понимания социальной природы киберпреступности в экспертном сообществе и представлений о стратегиях противодействия данному явлению.

Исследование проведено в июле-августе 2023 года. Экспертная выборка (17 человек) включает как теоретиков, исследующих проблемы киберпреступности, так и практиков – бывших следователей, которые непосредственно работали в сфере расследования киберпреступлений, а также преподавателей, работающих в образовательных учреждениях по подготовке специалистов для расследования, в том числе и преступлений с

использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

В вопросе анализа и оценки актуального состояния киберпреступности в России практически все эксперты отмечают высокую степень важности проблемы, особенно в последние несколько лет, и фиксацию показателей на высоких уровнях по состоянию на 2023 год. Эксперты отмечали, что в России фактически упустили нарастающую проблему, которая активно формировалась в течение последних нескольких лет. Также эксперты обратили внимание на то, что официальная статистика лишь отчасти отражает действительность, но не передает фактического масштаба проблемы. Отмечается и возросшее количество кибератак, в том числе и на критическую инфраструктуру России, которые совершаются из-за рубежа.

Предлагаемые экспертами решения по исправлению ситуации можно разбить на несколько ключевых блоков.

1. Более масштабная, глубокая и системная работа с населением по повышению осведомленности, цифровой грамотности и образованности.
2. Модернизация правоохранительных органов, которые, по мнению экспертов, оказались не готовы к быстрому переходу преступности в цифровой сектор.
3. Более тесное международное сотрудничество, необходимость которого вытекает из трансграничной сущности киберпреступности.
4. Решение проблемы дефицита высококвалифицированных кадров как для всей российской ИТ-отрасли для построения надежных и устойчивых к проникновению цифровых систем, так и в правоохранительных органах для эффективного расследования совершенных преступлений и проведения профилактических мероприятий.
5. Выделение дополнительного финансирования на проекты по борьбе с киберпреступностью.

6. Эффективное и оперативное взаимодействие правоохранительных органов, банков и операторов связи для блокировки мошеннических ресурсов и номеров.

7. Совершенствование российского законодательства в сфере информационных технологий.

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.

Результаты исследования показывают, что в экспертном сообществе существуют ожидания роста количества киберпреступлений в России в ближайшие годы, сохранения невысокой доли раскрываемости преступлений, отмечается отсутствие системной работе на опережение в борьбе с киберпреступностью.

В параграфе 2.2 «**Устойчивое цифровое развитие как основа альтернативной стратегии борьбы с киберпреступностью»** обосновывается возможность и необходимость разработки альтернативной стратегии противодействия киберпреступности в парадигме устойчивого цифрового развития с целью долгосрочного и эффективного противодействия киберпреступности.

Устойчивое цифровое развитие – это новый подход к развитию социо-цифровых систем, новая концепция технологического цифрового развития, в которой приоритетной является задача минимизации вероятности возникновения и масштабирования реальных и потенциальных киберугроз. Это социально ориентированное развитие цифровых технологий, где приоритет отдается надежности и устойчивости системы. Аналогии с концепцией устойчивого развития здесь не случайны. Подобно тому, как бездумное использование природных ресурсов опасно в долгосрочной перспективе для всего человечества, аналогичная проблема назрела и по

отношению к технологиям. Переход к устойчивому цифровому развитию создает возможность выработки и реализации комплексного стратегического подхода к решению проблемы киберпреступности.

Появление концепции устойчивого цифрового развития – это попытка переосмыслить развитие цифровых технологий за последние десятки лет: глобальные кибератаки, угрозы для критической инфраструктуры, рост киберпреступности и ее оформление в полноценную индустрию, проблемы искусственного интеллекта, принудительная цифровизация и многое другое; это попытка решения вопроса двойственного влияния технологий – как мощного инструмента достижения целей устойчивого развития и одновременно источника большой опасности для всего населения планеты.

Концепция устойчивого цифрового развития – это основа для формирования эффективной стратегии противодействия киберпреступности, которая должна базироваться на принципах системности, долговременности, носить непрерывный, упреждающий характер. Такая стратегия должна включать следующие основные направления и конкретные меры.

1. Переориентация на новый ценностный подход при проектировании, разработке и внедрении ИТ-систем, в основе которого – приоритет надежности и устойчивости социо-цифровых систем.

2. Более активная роль государства и общественных объединений как ключевых проводников на пути к построению устойчивого цифрового развития.

3. Непрерывный аудит, направленный на поиск и прогнозирование уязвимостей социо-цифровой системы через методы социальной оценки технологий.

4. Долгосрочная, масштабная и тщательная работа с населением в области повышения цифровой грамотности, формирования цифровой культуры и кибербезопасности. Расширение инфраструктуры по повышению

осведомленности граждан об угрозах со стороны киберпреступности и способах защиты.

5. Выстраивание и реализация долговременной политики по подготовке и удержанию высококвалифицированных ИТ-специалистов.

6. Оперативное правовое сопровождение.

7. Модернизация правоохранительной системы. Развитие государственно-частного партнерства.

8. Развитие и поддержание конструктивных международных отношений в противодействии киберпреступности и расследовании кибер-инцидентов.

9. Развитие и поддержание общественных объединений и инициатив в области кибербезопасности и расследования киберинцидентов, в том числе и с использованием искусственного интеллекта. Обязательное раскрытие информации о киберинцидентах.

10. Создание единого аналитического центра по противодействию киберпреступности, разработке и реализации системной стратегии противодействия киберпреступности.

Обобщая проведенный анализ, представим схему эффективной стратегии противодействия киберпреступности[12]:

1. Принципы, на которых основана стратегия. Ценностные приоритеты.

2. Интересы, которые она призвана защищать.

3. Инструменты, которые используются для продвижения и защиты этих интересов.

4. Киберугрозы и проблемы, которые представляют угрозу безопасности.

5. Приоритетные задачи политики кибербезопасности.

---

[12] Использовались материалы Управления ООН по наркотикам и преступности. Кибербезопасность и предупреждение киберпреступности: стратегии, политика и программы [Электронный ресурс]. Режим доступа: https://www.unodc.org/e4j/ru/cybercrime/module-8/index.html (дата обращения: 14.04.2024).

6. Ресурсы, которые необходимы для выполнения этих задач.

7. Ожидаемые результаты и инструменты оценки.

В **Заключении** изложены основные результаты диссертационного исследования, а также проблемы, которые требуют особого внимания.

В качестве альтернативного подхода к борьбе с киберпреступностью рассмотрена стратегия в парадигме устойчивого цифрового развития. Ее ключевое преимущество заключается в акценте на анализ социальных корней проблемы киберпреступности, минимизацию социальных уязвимостей системы через выработку кибер- и социального иммунитета. Это долгосрочный комплекс мер по выстраиванию социального мониторинга технологического развития с фокусом на выявление и дальнейшее устранение уязвимостей социальной природы. Конечная цель данного комплекса мер – установление нарушенного в настоящий момент баланса между технологическим и социальным и его дальнейшее поддержание за счет мер упреждающего, стратегического характера.

Выявляются существующие серьезные риски реализации предлагаемой стратегии. Они связаны прежде всего со сложившейся геополитической ситуацией. Геополитическая напряженность ведет к смещению стратегических приоритетов, обостряя проблемы кадровой и финансовой обеспеченности борьбы с киберпреступностью, остро ставя задачу технологической независимости, ограничивая возможности международного технологического сотрудничества и международного противодействия киберпреступности, обмена опытом и реализации совместных долгосрочных программ в борьбе с киберпреступностью. Существуют также риски, связанные с изменениями, происходящими в самой киберпреступности, такими как рост квалификации, профессионализма и самоорганизации киберпреступников; снижение порога входа в киберпреступную деятельность – киберпреступность как способ незаконного заработка становится доступна для все большего количества людей; создание устойчивых преступных групп

с централизованным управлением; рост количества технически сложных, точечных атак на критическую инфраструктуру; рост использования социальной инженерии как одного из наиболее эффективных методов совершения киберпреступлений. Все это делает еще более актуальной разработку эффективной стратегии противодействия киберпреступности.

III. СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях, рекомендованных Ученым советом МГУ имени М.В.Ломоносова для защиты в диссертационном совете МГУ по специальности 5.4.7 – Социология управления:

1. Швыряев П.С. Проблема киберпреступности в России: актуальное состояние и перспективы решения // Уровень жизни населения регионов России. – 2023. – Том 19. – № 4. – С. 616–629. – 1 п.л. (авт. 1 п.л.). – Импакт–фактор РИНЦ: 1,470.
2. Швыряев П.С. Кадровая обеспеченность в сфере информационных технологий в России: проблемы и перспективы // Государственное управление. Электронный вестник. – 2023. – № 97. – С. 231–240. – 0,7 п.л. (авт. 0,7 п.л.). – Импакт–фактор РИНЦ: 1,687.
3. Швыряев П.С. Утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. – 2022. – № 91. – С. 226–241. – 1 п.л. (авт. 1 п.л.). – Импакт–фактор РИНЦ: 1,687.
4. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства // Государственное управление. Электронный вестник. – 2021. – № 89. – С. 184–196. –0,9 п.л. (авт. 0,9 п.л.). – Импакт–фактор РИНЦ: 1,687.
5. Судас Л.Г., Оносов А.А., Бесланеев А.Ж., Манкевич Ю.В., Пивоварова М.Б., Правосудова В.А., Рассадина Д.С., Швыряев П.С. Конфликтный потенциал дистанционного формата занятости // Государственное управление. Электронный вестник. – 2021. – № 86. – С. 284–306. – 0,9 п.л. (авт. 0,1 п.л.). – Импакт–фактор РИНЦ: 1,687.