МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

На правах рукописи

Швыряев Павел Сергеевич

Киберпреступность как социальная проблема: стратегии противодействия

Специальность: 5.4.7 Социология управления

Диссертация на соискание ученой степени
кандидата социологических наук

Научный руководитель:
доктор философских наук, профессор
Л.Г. Судас

Москва – 2024

Оглавление

Введение

Актуальность темы исследования. На начало 20-х годов XXI века приходится очередная волна масштабных, глубоких цифровизационных трансформаций. Отправной точкой резкой смены привычных устоев общественной жизни послужила пандемия COVID-19, которая спровоцировала всплеск вынужденной, ускоренной цифровизации различных областей человеческой деятельности в масштабах всего человечества. Обстоятельства пандемии можно рассматривать как триггер для технологической трансформации процессов в государстве, обществе и бизнесе. Однако эти изменения не ограничиваются сроками пандемии и продолжаются по настоящее время и будут с разной степенью интенсивности продолжаться в будущем. Пандемия выступила мощным катализатором трансформационных изменений в общественной жизни на базе нового технологического уклада. Эти изменения – бесконечный спиралевидный процесс, суть которого – непрерывная адаптация социальной системы к новым обстоятельствам внешней среды. Обстоятельства могут иметь самую разную природу: пандемии, войны, катаклизмы, масштабные бедствия и катастрофы, глобальные кризисы и технологические аварии, становление нового миропорядка и общественного устройства.

События во время пандемии показали, что глобальная система безопасности оказалась не готова к серьезным трансформационным изменениям. Не готова и социальная система: резкий переход в онлайн привычной общественной жизни стал вызовом для значительной части населения планеты и социальных институтов. Рост числа киберпреступлений в масштабах всей планеты – яркое проявление назревших проблем, которые оказывают влияние и на восприятие технологий. По данным консалтинговой фирмы Edelman, 71% респондентов по всему миру обеспокоены вопросами

кибербезопасности[1]. Новые технологии могут обещать эру процветания, но одновременно вместо этого все чаще усугубляют проблемы доверия и выступают катализатором социальной нестабильности[2]. В настоящий момент со стороны общества отчетливо формулируются требования к безопасности и надежности технологий, которые не могут быть проигнорированы. 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 России назрела потребность в аудите системы безопасности, которая столкнулась с беспрецедентным давлением в период пандемии и геополитической нестабильности 2022-2023 годов. Как в новых реалиях обеспечить цифровую стабильность и устойчивое развитие российской экономики и общества в целом? В настоящий момент это один из ключевых вопросов, которым задаются российские управленцы, исследователи и лица, принимающие решения.

Существующие стратегии противодействия киберпреступности показали свою ограниченность и низкую эффективность. Эти стратегии в большинстве своем – ответная реакция на сложившуюся ситуацию, попытки минимизировать последствия, а не провести системную работу по анализу и ликвидации причин. В последние годы, с обострением проблемы киберпреступности, сформировался отчетливый тренд на ужесточение

---

[1] EDELMAN TRUST BAROMETER 2022 [Электронный ресурс]. Режим доступа: https://www.edelman.com/sites/g/files/aatuss191/files/2022-10/2022%20Trust%20Barometer%20Special%20Report_Trust%20in%20Technology%20Final_10-19.pdf (дата обращения: 04.02.2024).

[2] EDELMAN TRUST BAROMETER 2024 [Электронный ресурс]. Режим доступа: https://www.edelman.com/sites/g/files/aatuss191/files/2024-01/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL_1.pdf (дата обращения: 04.02.2024).

законодательства за совершения преступных деяний в цифровой среде. Об этом заявляли эксперты[3], данная политика реализуется через принятие соответствующих законопроектов[4]. Но какой может быть эффективность таких законотворческих мер в условиях, когда правоохранительные органы отстают от киберпреступников в техническом обеспечении и инструментах связи[5], а источник атак нередко находится за пределами государства[6]? Когда законодательство не успевает за стремительным развитием информационных технологий и правовая система не успевает регламентировать отношения в цифровой среде? Помимо этого, в России сохраняется низкий процент раскрываемости киберпреступлений, что будет подробно рассмотрено на данных официальной статистики за последние годы. Насколько целесообразно в таком случае ужесточение законодательства, если процент раскрываемости киберпреступлений сохраняется в России на низком уровне? Или же ситуация не столь линейна и требует более глубокого анализа?

Таким образом, события пандемии и ускоренной цифровизации продемонстрировали высокую степень актуальности проблемы киберпреступности. Существует настоятельная потребность в том, чтобы углубить понимание природы киберпреступности и на основе такого понимания разработать более эффективные научно обоснованные стратегии противодействия.

Таким образом, социальная проблема заключается в неконтролируемом росте масштабов и глубины киберпреступности и

---

[3] Российская Газета. Необходимо ужесточить ответственность за киберпреступления – эксперты [Электронный ресурс]. Режим доступа: https://rg.ru/2021/08/05/neobhodimo–uzhestochit–otvetstvennost–za–kiberprestupleniia–eksperty.html (дата обращения: 16.07.2023).

[4] Интерфакс. Президент подписал закон о конфискации имущества у киберпреступников [Электронный ресурс]. Режим доступа: https://www.interfax.ru/russia/906019 (дата обращения: 16.07.2023).

[5] ТАСС. ГП: правоохранительные органы отстают в технических возможностях от киберпреступников [Электронный ресурс]. Режим доступа: https://tass.ru/politika/8915711 (дата обращения: 16.07.2023).

[6] Известия. ФСБ сообщила об участии Пентагона в кибератаках против России [Электронный ресурс]. Режим доступа: https://iz.ru/1497823/2023–04–13/fsb–soobshchilo–ob–uchastii–pentagona–v–kiberatakakh–protiv–rossii (дата обращения: 16.07.2023).

неэффективности используемой стратегии борьбы. Научная проблема заключается в недостаточной проработанности социологического понимания феномена киберпреступности при его возрастающей значимости.

Степень разработанности темы исследования. В литературе по социальным наукам проблема киберпреступности привлекает все больше внимания. Несмотря на то, что исследователями активно подчеркивается значимость данной проблемы, комплексный подход к ее пониманию только предстоит выработать. Безусловно, говоря о проблеме киберпреступности, нельзя не отметить достижения исследователей в области технологий и защиты информации. Однако в рамках анализа степени научной разработанности нас интересуют прежде всего исследователи из области социальных наук.

Доминирующим подходом к исследованию киберпреступности является правовой. 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[7]. В рамках данного

[7] 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.

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 и т.д.

Проблемы цифровой криминологии рассматриваются в трудах Суходолова А.П., Иванцова С.В., Молчановой Т.В., Спасенникова Б.А., Калужиной М.А., Веденина Д.В., Серебренниковой А.В., Мосечкина И.Н., Аносова А.В., Комлева Ю.Ю., Максимова С.В., Васина Ю.Г., Утарова К.А. и других[8]. В рамках данного направления исследуются вопросы развития

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.

[8] Суходолов А.П., Иванцов С.В., Молчанова Т.В., Спасенников Б.А., Калужина М.А. Цифровая криминология: математические методы прогнозирования (часть 1) / А.П. Суходолов, С.В. Иванцов., Т.В. Молчанова, Б.А. Спасенников, М.А. Калужина // Всероссийский криминологический журнал. – 2018. – №2. – С. 230–236.

Веденин Д.В. Общая характеристика лиц, совершающих преступления с использованием информационно–телекоммуникационных технологий или в сфере компьютерной информации / Д.В. Веденин // Вестник Уральского юридического института МВД России. – 2023. – № 2. – С. 127–131.

цифровой криминологии, ответственности за совершенные киберпреступления, возможности цифровой криминологии как инструмента борьбы с различного рода преступлениями.

Новое актуальное направление в рамках виктимологии – кибервиктимологию – исследуют Никитин Е.В., Жмуров Д.В., Коробеев А.И., Стяжкина С.А., Старостенко О.А., Рыжова Н.И. и Громова О.Н., Игнатов А.Н. и Соловьев В.С. и другие[9]. Среди зарубежных работ в рамках данного направления можно отметить труды следующих исследователей: Алшалан А., Халдер Д. и Джайшанкар К., Хайндуджа С. и Патчин Дж., Ластовка Ф. и Хантер Д., Ли К., Лайптон Дж., Нгоу Ф. и Патерностер Р.,

---

Серебренникова А.В. Криминологические проблемы цифрового мира (цифровая криминология) / А.В. Серебренникова // Всероссийский криминологический журнал. – 2020. – №3. – С. 423–430.

Мосечкин И.Н. Уголовная ответственность за организацию устойчивой группы лиц, созданной для совершения преступлений в сфере компьютерной информации» / И.Н. Мосечкин // Вестник Санкт-Петербургского университета. – 2022. – Право 1. – С. 28–45.

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

Комлев Ю.Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии / Ю.Ю. Комлев // Вестник Казанского юридического института МВД России. – 2020. – №1 (39). – С. 31–40.

Максимов С.В., Васин Ю.Г., Утаров К.А. Цифровая криминология как инструмент борьбы с организованной преступностью / С.В. Максимов, Ю.Г. Васин, К.А. Утаров // Всероссийский криминологический журнал. – 2018. – №4. – С. 476–484.

[9] Никитин Е. В. Обеспечение виктимологической безопасности и профилактики преступлений с использованием информационных технологий / Е.В. Никитин // Виктимология. – 2022. – Т. 9, № 2. – С. 204–212.

Жмуров Д.В. Кибервиктимология: методы и метрика / Д.В. Жмуров // Baikal Research Journal. – 2022. – Т.13, №1. – С. 1–29.

Коробеев А.И., Жмуров Д.В. Кибервиктимология фейка: первичное досье / А.И. Коробеев, Д.В. Жмуров // Вестн. Том. гос. ун-та. – 2021. – №471. – С. 250–257.

Стяжкина С.А. Виктимологическая профилактика кибермошенничества / С.А. Стяжкина // Вестник Удмуртского университета. Серия «Экономика и право». – 2022. – №3. – С. 546–552.

Старостенко О.А. Виктимологические проблемы обеспечения безопасности личности в сети интернет / О.А. Старостенко // Вестник Сибирского юридического института МВД России. – 2022. – №2 (47). – С. 157–161.

Рыжова Н.И., Громова О.Н. Киберугрозы цифрового социума и их профилактика в рамках виктимологической деятельности / Н.И. Рыжова, О.Н. Громова // Вестник РУДН. Серия: Информатизация образования. – 2020. – №3. – С. 254–268.

Игнатов А.Н., Соловьев В.С. Информационно-когнитивные технологии в механизме цифровой виктимизации / А.Н. Игнатов и В.С. Соловьев // Вестник Казанского юридического института МВД России. – 2023. – Т. 14. № 1 (51). – С. 59 – 66.

Робертс Л., Йяр М. и другие[10]. Исследуются вопросы метода кибервиктимологии, профилактики кибермошенничества и новых технологий в механизме цифровой виктимизации.

Исследование психологии киберпреступников, их мотивов и целей, очень важно для выработки эффективных стратегий противодействия совершаемым действиям и профилактики возможных рецидивов. Исследованию психологии злоумышленников посвящены труды Полякова В.В. и Поповой Л.А., Косенковой А.Н. и Черного Г.А., Федосеевой О.И., Пучковой О.А., Костомоловой М.В. и других[11].

---

[10] Alshalan A. (2006). Cyber-crime fear and victimization: An analysis of a national survey. PhD Dissertation submitted to Mississippi State University.

Halder D., & Jaishankar K. (2015). Irrational coping theory and Positive Criminology: A frame work to protect victims of cyber crime. In N. Ronel and D. Segev (eds.), Positive Criminology (pp. 276–291).

Hinduja S., & Patchin J. W. (2007). Offline consequences of online victimization: School violence and delinquency. Journal of School Violence, 6(3), 89–112.

Lastowka F.G., & Hunter D. (2004). Virtual crimes. New York Law School Law Review, 49, 293–316.

Li Q. (2007). Bullying in the new playground: Research into cyberbullying and cyber victimisation. Australasian Journal of Educational Technology, 23(4), 435–454.

Lipton J. D. (2011). Combating cyber-victimization. Berkeley Technology Law Journal, 26, 1103–1156.

Ngo F. T., Paternoster R. (2011). Cybercrime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5(1), 773–793.

Roberts L. (2008). Cyber-victimisation in Australia: Extent, impact on individuals and responses. TILES Briefing Paper No. 6.

Yar M. (2012) E-Crime 2.0: the criminological landscape of new social media. Information & Communications Technology Law, 21(3), 207–219.

[11] Поляков В.В., Попов Л.А. Особенности личности компьютерных преступников / В.В. Поляков, Л.А. Попов // Известия АлтГУ. – 2018. – №6 (104). – С. 256–259.

Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника / Косенков А.Н., Черный Г.А. // Всероссийский криминологический журнал. – 2012. – №3. – С. 87–94.

Федосеева О.И. Психологические особенности формирования личности несовершеннолетнего киберпреступника / О.И. Федосеева // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2022. – № 4 (60). – С. 174–178.

Пучков О.А. Мотивация действий хакеров в современной цифровой среде: междисциплинарный подход / О.А. Пучков // Проблемы современного педагогического образования. – 2020. – №67–3. – С. 306–308.

Костоломова М.В. Цифровая девиация как феномен новой социальной реальности: методологические основания и концептуализация понятия / М.В. Костомолова // Социологическая наука и социальная практика. – 2020. – Т. 8. № 2. – С. 41–53.

Один из наиболее эффективных и опасных методов совершения киберпреступления – социальную инженерию – в своих работах рассматривают Унукович А.С., Созаев С.С. и Кунашев Д.А., Янгаева М.О., Ревенков П.В. и Бердюгин А.А., Алмутайри Б. и Алгамди А., Апау Р. и Корантенг Ф., Конте Н., Салахдин Ф. и Каабуш Н. и другие[12].

Наиболее радикальная и опасная форма проявления киберпреступности – кибертерроризм – рассмаривается в работах Вехова В.Б. и Ковалева С.А., Галушкина А.А., Бураевой Л.А., Тамбиева С.А. и Кочесоковой З.Х., Арипшева А.М., Тарчкова Б.А., Геляховой Л.А., Аккаевой Х.А., Альбахара М., Бэкхауса С., Кларка Р., Гарцке Е., Гросса М., Канетти Д. и Вашди Д., Херцога С. и других специалистов[13].

---

[12] Унукович А.С. Социальная инженерия и кибербезопасность: виктимологический аспект / А.С. Унукович // Психопедагогика в правоохранительных органах. – 2021. – №3 (86). – С. 346–351.

Созаев С.С., Кунашев Д.А. Социальная инженерия, ее техники и методы ее противодействия / С. С. Созаев, Д. А. Кунашев // Международный журнал «Вестник науки». – 2020. – № 2 (23). – Т. 1. – С. 85–88.

Янгаева М.О. Методы (техники) социальной инженерии, используемые при совершении преступлений в сфере компьютерной информации / М.О. Янгаева // Криминалистика: вчера, сегодня, завтра. – 2021. – Т. 18. – № 2. – С. 145–151.

Ревенков П.В., Бердюгин А.А.. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания / П.В. Ревенков, А.А. Бердюгин // Национальные интересы: приоритеты и безопасность. – 2017. – Т. 13, № 9. – С. 1747–1760.

Almutairi B. S., & Alghamdi A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. Journal of Information Security, 13(04), 363–379.

Apau R., Koranteng F. N. (2019). Impact of cybercrime and trust on the use of ecommerce technologies: An application of the theory of planned behavior. International Journal of Cyber Criminology, 13(2).

Conteh, N.Y., (2021). The dynamics of social engineering and cybercrime in the digital age. In Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 144–149).

Salahdine F., Kaabouch N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

[13] Вехов В.Б., Ковалев С.А. Проблемы борьбы с кибертерроризмом / В.Б. Вехов, С.А. Ковалев // Правопорядок: история, теория, практика. – 2018. – №1 (16). – С. 89–93.

Галушкин А.А. К вопросу о кибертерроризме и киберпреступности / А.А. Галушкин // Вестник РУДН. Серия: Юридические науки. – 2014. – №2. – С. 44–49.

Бураева Л.А. Кибертерроризм в молодежной среде / Л.А. Бураева // Проблемы экономики и юридической практики. – 2016. – №2. – С. 271–274.

Тамбиев С.А., Кочесокова З.Х. Международный опыт противодействия кибертерроризму / С.А. Тамбиев, З.Х. Кочесокова // Право и управление. – 2023. – №2. – С. 160–164.

Сегодня государство остается ключевым актором в вопросах противодействия киберпреступности. Исследованию вопросов государственной политики в области противодействия киберпреступности посвящены работы Прокофьевой Т.В., Кобец П.Н., Чимарова С.Ю. и Бялт В.С., Антонян Е. А. и Клещиной Е. Н. и других[14].

Киберпреступность носит транснациональный характер, это проблема глобального характера вне зависимости от географии или степени защищенности того или иного государства. В этой связи важное место в противодействии киберпреступной деятельности занимает международное сотрудничество, которое исследуется в работах Евдокимова К.Н. и

Арипшев А.М. Кибертерроризм: проблемы в понимании и способы противодействия / А.М. Арипшев // Журнал прикладных исследований. – 2023. – №4. – С. 109–112.

Тарчоков Б.А. К вопросу о понятии кибертерроризма и некоторых способах противодействия / Б.А. Тарчоков // Право и управление. – 2023. – №2. – С. 170–174.

Геляхова Л.А. Международно-правовые основы противодействия кибертерроризму / Л.А. Геляхова // Пробелы в российском законодательстве. – 2017. – № 3. – С. 65–67.

Аккаева Х.А. Международный кибертерроризм как политический феномен / Х.А. Аккаева // Социально-политические науки. – 2018. – № 1. – С. 138–140.

Albahar M (2019) Cyber attacks and terrorism: a twenty-first century conundrum. Science and Engineering Ethics 25(4), 993–1006.

Backhaus S et al. (2020) A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. Cyberpsychology, Behavior, and Social Networking 23(9), 595–603.

Gartzke E (2013) The myth of cyberwar: bringing war in cyberspace back down to earth. International Security 38(2), 41–73.

Gross ML, Canetti D and Vashdi DR (2016) The psychological effects of cyber terrorism. Bulletin of the Atomic Scientists 72(5), 284–291.

Herzog S (2011) Revisiting the Estonian cyber attacks: digital threats and multinational responses. Journal of Strategic Security 4(2), 49–60.

[14] Прокофьева Т.В. О мерах по совершенствованию борьбы с киберпреступностью в Российской Федерации / Т.В. Прокофьева // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. – 2022. – Вып. 1(842). – С. 142–146.

Кобец П.Н. Совершенствование межгосударственного сотрудничества в сфере информационной безопасности: основа противодействия международной киберпреступности / П.Н. Кобец // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2023. – № 1. – С. 83–89.

Чимаров С.Ю., Бялт В.С. Зарубежный опыт противодействия киберпреступности: в контексте опоры полиции на потенциал общественности / С.Ю. Чимаров, В.С. Бялт // Международный журнал гуманитарных и естественных наук. – 2023. – №1–3 (76). – С. 147–149.

Антонян Е.А., Клещина Е.Н. Киберпреступность на современном этапе: тенденции и направления противодействия / Е.А. Антонян, Е.Н. Клещина // Вестник экономической безопасности. – 2022. – № 5. – С. 11–15.

Хобонковой К.В., Ситкова А.С., Клевцова К.К., Мороз Н.О., Дубень А.К., Атнашева В.Р. и Яхъеевой С.Н. и других[15].

Киберпреступность тесно связана с характером цифровизации и цифровой трансформации социума. Исследованию вопросов цифровой трансформации посвящены работы Назарова В.Л., Жердева Д.В. и Буйначевой А.В., Термелевой А.Е., Вертаковой Ю.В. и Крыжановской О.А., Сорочан В.В. и Гаврилюка Н.П. и других[16]. Среди иностранных работ можно выделить работы Каррена Д., Фрэнка А., Даленогэра Л. и Аяла Н., Хивина К. и Пауэр Д., Пайола М., Текича З. и Коротеева Д. и других[17].

---

[15] Евдокимов К.Н., Хобонкова К.В. К проблеме совершенствования международного сотрудничества в сфере противодействия киберпреступности / К.Н. Евдокимов, К.В. Хобонкова // Сибирский юридический вестник. – 2022. – №3 (98). – С. 90–95.
Ситков А.С. Международное сотрудничество полиции в рамках Интерпола по противодействию киберпреступности и обеспечению кибербезопасности / А.С. Ситков // Вестник Московского университета МВД России. – 2022. – № 5. – С. 238–242.
Клевцов К.К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам / К.К. Клевцов // Вестник Санкт–Петербургского университета. – 2022. – Т. 13. Вып. 3. – С. 678–695. Мороз Н.О. Особенности международно-правового сотрудничества в борьбе с киберпреступностью в рамках ЕС / Н.О. Мороз // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». – 2018. – №4 (16). – С. 87–94.
Дубень А.К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению / А.К. Дубень // Международное право и международные организации. – 2022. – №1. – С. 24–33.
Атнашев В.Р., Яхъеева С.Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом / В.Р. Атнашев, С.Н. Яхъеева // Евразийская интеграция: экономика, право, политика. – 2019. – №3 (29). – С. 37–42.

[16] Назаров В.Л., Жердев Д.В., Буйначева А.В. Актуальные проблемы цифровой трансформации среднего образования / В.Л. Назаров, Д.В. Жердев, А.В. Буйначева // Образование и наука. – 2023. – № 25(4). – С. 109–166.
Термелева А.Е. Цифровая трансформация на современном этапе и ее влияние на инновационную деятельность / А.Е. Термелева // Вестник Самарского университета. Экономика и управление. 2022. Т. 13, № 3. С. 50–58.
Вертакова Ю.В., Крыжановская О.А. Особенности развития организаций в условиях цифровой трансформации / Ю.В. Вертакова и О.А. Крыжановская // Вестник университета. – 2020. – № 10. – С. 33–39.
Сорочан В.В., Гаврилюк Н.П. Цифровая социология: от цифровизации общества к цифровизации науки / В.В. Сорочан и Н.П. Гаврилюк // Этносоциум и межнациональная культура. – 2023. – № 174. – С. 37 – 46.

[17] Curran D. (2018), Risk, innovation, and democracy in the digital economy, European Journal of Social Theory, Vol. 21 No. 2, pp. 207-226.

Искусственный интеллект может выступать эффективным инструментом как совершения, так и предотвращения киберпреступлений. Вопросы использования искусственного интеллекта при совершении киберпреступлений и инструменты противодействия киберпреступлениям с использованием искусственного интеллекта поднимаются в работах: Бычкова А.М. и Суходолов А.П., Кибальник А.Г., Волосюк П.В., Тирранен А.В. и других[18].

Еще один контекст, в котором может анализироваться проблема киберпреступности, – концепция корпоративной социальной 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., Кольманн П., Вайсенбергер Б.Е. и Марокко А. и другие[19].

Frank, A.G., Dalenogare, L.S. and Ayala, N.F. (2019), Industry 4.0 technologies: implementation patterns in manufacturing companies, International Journal of Production Economics, Vol. 210, pp. 15-26.

Heavin, C. and Power, D.J. (2018), Challenges for digital transformation – towards a conceptual decision support guide for managers, Journal of Decision Systems, Vol. 27 No. 1, pp. 38-45.

Paiola, M. (2018), Digitalization and servitization: opportunities and challenges for Italian SMES, Sinergie Italian Journal of Management, Vol. 36 No. 107, pp. 11-22.

Tekic, Z. and Koroteev, D. (2019), From disruptively digital to proudly analog: a holistic typology of digital transformation strategies, Business Horizons, Vol. 62, pp. 683-693.

[18] Бычкова А.М., Суходолов А.П. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции / А.М. Бычкова, А.П. Суходолов // Всероссийский криминологический журнал. – 2018. – № 6. – С.753–766.

Кибальник А.Г., Волосюк П.В. Искусственный интеллект: вопросы уголовно-правовой доктрины, ожидающие ответов / А.Г. Кибальник, П.В. Волосюк // Юридическая наука и практика. Вестник Нижегородской академии МВД России. – 2018. – № 3 (44). – С.173-178.

Тирранен В. А. Искусственный интеллект и нейронные сети как инструмент современной киберпреступности // Уголовное право: стратегия развития в XXI веке : материалы XVI Междунар. науч.-практ. конф. (24—25 янв. 2019 г.) М. : РГ-Пресс, 2019. – С. 135—140.

[19] Mueller, B. Corporate Digital Responsibility. Bus Inf Syst Eng 64, 689–700 (2022).

Набирает популярность и исследования цифровой трансформации на уровне индивида. Исследованию процессов интегрирования цифровых технологий в рабочие места, присвоении и использовании цифровых технологий в рабочих и нерабочих активностях посвящены работы авторов: Кастеллано С., Чандавимол К., Кхеллади И. и Орхан М.А., Даравонг С., Козловски С.В., Чао Г.Т. и Ван Фоссен Дж., Де Брюйне Э. и Герритс Д., Дери К., Себастьян И.М. и ван дер Мейлен Н. и других[20].

Таким образом, на всех трех уровнях – социальном, организационном и индивидуальном – происходит общий процесс, опирающийся на единый набор ценностей: безопасность, стабильность, устойчивость.

Активный и живой интерес к проблеме киберпреступности со стороны представителей юридической науки и правоохранительных органов не отменяет проблемы того, что феномен киберпреступности с позиций социологии исследован недостаточно. Данное положение вещей вызывает серьезную озабоченность, поскольку киберпреступность – это прежде всего социальная проблема, феномен общества на определенном этапе его развития, один из продуктов цифровизации. Такая многогранная сущность киберпреступности требует активного подключения междисциплинарных

Hamadi H, Manzo C (2021) Corporate digital responsibility – a study on managerial challenges for AI integration in business. Lund University, Lund.

Kohlmann P (2019) Kapitel 7: Corporate digital responsibility for internet of things technology. In: Spraul K (ed) Nachhaltigkeit und digitalisierung: wie digitale innovationen zu den sustainable development goals beitragen. Nomos, Kreuzberg, pp 165–182.

Weißenberger BE, Marrocco A (2022) Corporate Digital Responsibility und Ihre Integration in die Unternehmensfu¨hrung. In: RothS, Corsten H (eds) Handbuch Digitalisierung. Vahlen, Berilin, pp 41–58.

[20] 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.

Kozlowski, S. W., Chao, G. T., & Van Fossen, J. (2021). Leading virtual teams. Organizational Dynamics, 50(1), 1–11.

De Bruyne, E., and Gerritse, D. (2018). Exploring the future workplace: results of the futures forum study. Journal of Corporate Real Estate, 20(3), 196–213.

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.

исследований. Достижения одной конкретной дисциплины – это лишь фрагмент пазла, из которого предстоит выстроить целостную картинку и углубить понимание именно социальной природы киберпреступности. А эффективный подход к решению данной проблемы невозможен без ее комплексного, глубокого понимания, в том числе с позиции социологической науки.

Сложившийся в настоящее время подход к исследованию проблемы киберпреступности имеет две ключевые проблемы. Во-первых, значительная часть актуальных исследований проблемы киберпреступности имеет узконаправленный, прикладной характер, что делает особенно актуальным запрос на проведение глубокого и комплексного анализа проблемы киберпреступности, выявления и описания ее сложной, многогранной социальной природы. Разрозненные исследования представителями различных научных дисциплин уводят в частности и мешают посмотреть на проблему целиком, не позволяют добиться синергетического эффекта от мер, которые предлагаются представителями различных научных дисциплин. Как итог, вместо единой и эффективной политики по борьбе с киберпреступностью мы имеем ряд зачастую несогласованных, несистемных частных мер, которые не позволяют добиться как стабилизации ситуации сейчас, так и формирования безопасного и надежного каркаса цифрового будущего. Во-вторых, влияние некогда популярного технократического подхода, который упускает из фокуса внимания социальную природу киберпреступности. Важно подчеркнуть, что киберпреступность – это противоправная деятельность, которая совершается с использованием информационных технологий. Технологии выступают лишь инструментом для совершения действия. Стремление свести исследовательский фокус только до инструмента – бесперспективен, неэффективен и вреден. Данный тезис подтверждает накопленный опыт борьбы с киберпреступностью: даже самый совершенный антивирус или антифрод-системы не спасает от

человеческого фактора, чем особенно успешно пользуются мошенники в последние годы, используя методы социальной инженерии. Все эти замечания позволяют поставить вопрос о пересмотре сложившегося подхода к исследованию феномена киберпреступности на иных, более фундаментальных основаниях для выработки системной, комплексной и эффективной стратегии противодействия, основанной на понимании социальной природы данного феномена.

Можно выделить несколько направлений в исследовании технологий представителями социальных наук, которые имеют важное методологическое значение для анализа проблемы киберпреступности.

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., Декер М. и Ладикас М., Елиа А., Ван Званенберг П. и Стирлинг А., Хеннен Л. и Нирлинг Л., Ладикас С. и другие[21]. Среди российских исследователей можно отметить работы Хана Ю. и Кулакова П., Попковой Н.В, Розина В.М., Дубровского Д.И,

[21] 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.
Decker M., Ladikas M. Bridges between science, society and policy. Technology assessment – methods and impacts // Berlin: Springer. – 2004. – P. 252.
Ely A., van Zwanenberg P., Stirling A. New Models of Technology Assessment for Development // Brighton: STEPS Centre. – 2011. – P. 47.
Hennen L., Nierling L. A next wave of Technology Assessment? Barriers and opportunities for establishing TA in seven European countries // Science and Public Policy. – 2015. – vol. 42. – P. 44–58.
Ladikas M., Chaturvedi S., Zhao Y., Stemerding D. Science and Technology Governance and Ethics. A Global Perspective from Europe, India and China // Springer International Publishing. – 2015. – P. 173.

Гаврилиной Е.А., Ефременко Д.В., Трахтенберга А.Д., Горохова В.Г., Пржиленского В.И., Михайлова И.Ф., Никифоровой Н.В., Пирожковой С.В. и других[22]. Представители данного направления затрагивают вопросы пути развития глобальной социальной оценки техники, рассматривают вопросы оценки техники, место философии в культуре техногенного общества, оценку техники как новую методологическую дисциплину, ее возможности и ограничения. Важно подчеркнуть, что проблемы в области исследования социальной оценки техники разрабатывались в Институте философии Академии наук СССР еще в советское время, до начала процессов цифровизации.

[22] 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.
Трахтенберг А.Д. Идеологический концепт электронного правительства: как работает риторика разрыва? / Д.А. Трахтенберг // Научный ежегодник Института философии и права Уральского отделения Российской академии наук. – 2017. – Т. 17. Вып. 2. – С. 41–58.
Горохов В.Г. Оценка техники как прикладная философия техники и новая научно-техническая дисциплина / В.Г. Горохов // Гений Шухова и современная эпоха. Материалы Международного конгресса. М.: Изд–во МБГТУ им. Н.Э. Баумана, 2015. С. 241–249.
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.

Информационные технологии – важный участник социального взаимодействия и фактор социализации. Проблематике влияния технологий на поведение и развитие человека посвящены работы Вершининой И.А. и Лядовой А.В., Шаполовой И.С., Мартышенко С.Н., Дяксул О.Ю. и Фещенко Н.В., 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[23].

Исследованию особенностей взаимодействия пожилых людей и технологий посвящены работы Корниловой М.В., Даринской Л.А., Молодцовой Г.И. и Москвичевой Н.Л., Воронина Г.Л. и Курячьевой М.М. и других[24].

---

[23] 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. Шаполова // Социологические исследования. – 2015. – № 4 (372). – С. 148–151.

Мартышенко С.Н. Влияние интернета на формирование коммуникационной среды современной молодежи / С.Н. Мартышенко // АНИ: педагогика и психология. – 2020. – №1 (30). – С. 185–189.

Дяксул О.Ю., Фещенко Н.В. Влияние интернета на современную молодежь / О.Ю. Дяксул, Н.В. Фещенко // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. – 2017. – Т. 1. – С. 263–266.

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.

[24] Корнилова М.В. Интернет как адаптационный ресурс пожилых пользователей / М.В. Корнилова // Изв. Сарат. ун-та Нов. сер. Сер. Социология. Политология. – 2018. – №3. – С. 250–259.

Даринская Л.А., Молодцова Г.И., Москвичева Н.Л. Пожилой человек и цифровое пространство: точки соприкосновения / Л.А. Даринская, Г.И. Молодцова, Н.Л. Москвичева // Человек и образование. – 2016. – №3 (48). – С. 151–157.

Воронин Г.Л., Курячьева М.М. Интернет-пространство старшего поколения: анализ проблемы вхождения в цифровую эпоху / Г.Л. Воронин, М.М. Курячьева // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Социальные науки. – 2018. – №3 (51). – С. 55–65.

К не менее важному направлению социального исследования аспектов технологического развития относятся исследования цифрового неравенства. Цифровое неравенство – важная проблема в России и мире, которая оказывает прямое влияние на состояние киберпреступности. Устранение цифрового неравенства, грамотная цифровая социализация населения и минимизация рисков совершения киберпреступлений в отношении новых, неопытных пользователей – важные шаги на пути построения безопасного мироустройства будущего. Исследования цифрового неравенства в России частично представлены в трудах Басовой Е.А., Добринской Д.Е. и Мартыненко Т.С., Волченко О.В., Ициксона А.И., Вершинской О.Н., Короткова А.В. и других исследователей[25].

Исследования проблем цифровизации социума и связанного с этим процесса роста киберпреступности, ее влияния на социальное развитие представлены в работах Комлева Ю.Ю., Карповой Д.Н., Сергеева А. Ю. и Широковой О. В. и ряда других авторов[26].

---

[25] Басова Е.А. Цифровое неравенство российских регионов: современные проблемы и пути преодоления / Е.А. Басова // Вопросы территориального развития. – 2021. – №4.– С.1–17.
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.
Вершинская О.Н. Информационное неравенство как социологическая проблема / О.Н. Вершинская // Информационное общество. – 2001. – № 4. – С. 45–50.
Коротков А.В. Цифровое неравенство в процессах стратификации информационного общества / А.В. Коротков // Информационное общество. – 2003. – № 5. – С. 24–35.

[26] Комлев Ю.Ю. От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии / Ю.Ю. Комлев // Российский девиантологический журнал. – 2022. – №2(1) – С. 17–26.
Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение / Д.Н. Карпова // Власть. – 2014. – №8. – С.46–50.
Сергеев А.Ю., Широкова О.В. Мошенничество в цифровом обществе в условиях социальных изменений / А.Ю. Сергеев, О.В. Широкова // Цифровая социология. – 2023. – №1. – С. 59–71.

Таким образом, актуальные вопросы и проблемы цифровизации не остаются без внимания социологической науки, в том числе и киберпреступность. Однако исследуются преимущественно отдельные 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 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 в коррекции существующих подходов в противодействии киберпреступности, их ограниченность и неэффективность.

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 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[27] и Джона Ло[28]. В работе применены идеи теории социального конструирования технологий[29] (SCOT) о понимании технологических артефактов как социальных конструкций, а развития технологий – как непрерывного процесса обсуждения и поиска консенсусного варианта среди различных социальных групп. Значимую роль с точки зрения теоретико-методологической основы в данной работе занимает развиваемая Полом Эдвардсом идея со-конструирования общества

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

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

[29] 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.

и технологий[30]. Данная идея используется в диссертационном исследовании при рассмотрении феномена киберпреступности как социальной проблемы, уберегает от уклона в технократизм.

При проведении прикладного социологического исследования использовался метод экспертного опроса.

Информационная база исследования. В диссертационном исследовании использованы нормативные правовые акты в сфере противодействия киберпреступности и информационных технологий в России; деловые периодические издания, отражающие тенденции и актуальное состояние киберпреступности в России и мире. Использованы материалы многопрофильных исследовательских центров Pew Research Center[31] и НАФИ[32], Банка России[33], материалы компаний DoubleVerify[34], McKinsey & Company[35], Edelman[36], Upwork[37], InfoWatch[38], Hootsuite[39],

---

[30] 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.

[31] Pew Research Center. About three-in-ten U.S. adults say they are ‘almost constantly’ online. [Электронный ресурс]. Режим доступа: https://www.pewresearch.org/fact–tank/2021/03/26/about–three–in–ten–u–s–adults–say–they–are–almost–constantly–online/ (дата обращения: 11.02.2022).

[32] НАФИ. Уровень цифровой грамотности в России и Беларуси. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/uroven–tsifrovoy–gramotnosti–v–rossii–i–belarusi/ (дата обращения: 07.03.2023).

[33] Банк России. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/statistics/ib/review_1q_2023/ (дата обращения: 12.06.2023).

[34] DoubleVerify. Four Fundamental Shifts in Media & Advertising During 2020. [Электронный ресурс]. Режим доступа: https://doubleverify.com/four–fundamental–shifts–in–media–and–advertising–during–2020/ (дата обращения: 17.12.2021).

[35] McKinsey & Company. US digital payments: Achieving the next phase of consumer engagement. [Электронный ресурс]. Режим доступа: https://www.mckinsey.com/industries/financial–services/our–insights/banking–matters/us–digital–payments–achieving–the–next–phase–of–consumer–engagement (дата обращения: 18.12.2021).

[36] EDELMAN TRUST BAROMETER 2024 [Электронный ресурс]. Режим доступа: https://www.edelman.com/sites/g/files/aatuss191/files/2024-01/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL_1.pdf (дата обращения: 04.02.2024).

Gartner[40], Всемирного экономического форума[41], Surfshark[42], SEON[43], Positive Technologies[44], материалы мероприятий в сфере кибербезопасности: Цифровая устойчивость и информационная безопасность России 2024[45], SberProTech 2023[46], доклады, сделанные на Международном Конгрессе по кибербезопасности[47], а также данные результатов 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:

---

[37] Upwork. Economist Report: Future Workforce [Электронный ресурс]. Режим доступа: https://www.upwork.com/press/releases/economist–report–future–workforce (дата обращения: 18.12.2021).

[38] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

[39] Hootsuite. The Global State of Digital 2021. [Электронный ресурс]. Режим доступа: https://www.hootsuite.com/pages/digital–trends–2021#c–274407 (дата обращения: 16.12.2021).

[40] Gartner. 7 Top Trends in Cybersecurity for 2022 [Электронный ресурс]. Режим доступа: https://www.gartner.com/en/articles/7–top–trends–in–cybersecurity–for–2022 (дата обращения: 10.12.2023).

[41] World Economic Forum. The Global Risks Report 2023 18th Edition [Электронный ресурс]. Режим доступа: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (дата обращения: 09.12.2023).

[42] Surfshark. Cybercrime statistics [Электронный ресурс]. Режим доступа: https://surfshark.com/research/data–breach–impact/statistics (дата обращения: 10.12.2023).

[43] SEON. Global Cybercrime Report: Which Countries Are Most at Risk in 2023? [Электронный ресурс]. Режим доступа: https://seon.io/resources/global–cybercrime–report/ (дата обращения: 10.12.2023).

[44] Positive Technologies. Актуальные киберугрозы: итоги 2022 года. [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru–ru/research/analytics/cybersecurity–threatscape–2022/#id9 (дата обращения: 12.06.2023).

[45] Цифровая устойчивость и информационная безопасность России 2024 [Электронный ресурс]. Режим доступа: https://ib-bank.ru/secural/program (дата обращения: 28.03.2024).

[46] SberProTech [Электронный ресурс]. Режим доступа: https://sber.pro/digital/sberprotech/ (дата обращения: 28.03.2024).

[47] Международный Конгресс по кибербезопасности [Электронный ресурс]. Режим доступа: https://icc.moscow/ru/ (дата обращения: 28.03.2024).

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 её 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 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 его 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 её 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.

Глава 1. Социологическая концептуализация киберпреступности

Первая глава посвящена исследованию актуального состояния киберпреступности в России и динамики развития проблемы в стране в последние 5 лет. Ставится задача проанализировать актуальное состояние и динамику киберпреступности в России в последние годы. Результаты данного анализа дают дальнейшую перспективу для более глубокой теоретической проработки данного феномена и определения тех факторов прежде всего социальной природы, которые лежат в основе проблемы киберпреступности.

§ 1.1 Актуальное состояние и динамика киберпреступности в России[48]

Перед тем, как перейти к анализу актуального состояния киберпреступности, рассмотрим некоторые определения данного понятия.

Эксперты Организации Объединенных Наций определяют «киберпреступность» как «любое преступление, совершаемое посредством эксплуатации компьютерной системы, в ее рамках или против нее[49]».

Известный российский криминалист Е.П. Ищенко определяет киберпреступность как «преступления в сфере высоких информационных технологий, совершаемые злоумышленниками, использующими эти технологии в противоправных целях[50]».

---

[48] При подготовке данного раздела использованы следующие публикации, выполненные автором лично, в которых отражены основные результаты, положения и выводы исследования: Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства / П.С. Швыряев // Государственное управление. Электронный вестник. – 2021. – № 89. – С. 184–196. Швыряев П.С. Проблема киберпреступности в России: актуальное состояние и перспективы решения / П.С. Швыряев // Уровень жизни населения регионов России. – 2023. – Том 19. – № 4. – С. 616–629.

[49] Ищенко Е.П. О криминалистическом обеспечении раскрытия и расследования киберпреступлений / Е.П. Ищенко // Деятельность правоохранительных органов в современных условиях: сборник материалов 20-й международной научно-практической конференции. В 2 томах. – 2015. – Т. 1. – С. 336–337.

[50] Ищенко Е.П. О криминалистическом обеспечении раскрытия и расследования киберпреступлений / Е.П. Ищенко // Деятельность правоохранительных органов в

Ряд исследователей для определения киберпреступности используют термин «киберпространство». В.А. Номоконов и Т.Л. Тропина определяют киберпреступность как «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных[51]». В Проекте Концепции Стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)[52]».

Важно отметить, что киберпреступность в рамках приводимых в данном параграфе определений является прежде всего правовой категорией. Данные официальные юридические определения важны для выстраивания дальнейшей структуры и логики первого параграфа, в которой анализируются данные государственной статистики, однако совершенно недостаточны для понимания природы данного явления, глубокая социальная сущность которого будет подробно рассмотрена во втором параграфе и второй главе данного исследования.

Также кратко рассмотрим историю определения понятия киберпреступности в российской правовой практике. В Российской

современных условиях: сборник материалов 20-й международной научно-практической конференции. В 2 томах. – 2015. – Т. 1. – С. 336–337.

[51] Номоконов В.А., Тропина Т.Л.. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012 – № 24. – С. 45–55.

[52] Проект Концепции стратегии кибербезопасности Российской Федерации [Электронный ресурс]. Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 30.11.2023).

Федерации правовая основа борьбы с киберпреступлениями впервые появилась с принятием Уголовного кодекса Российской Федерации, вступившего в силу с 01 января 1997 года, в котором появилась глава 28 «Преступления в сфере компьютерной информации», хотя отдельные законопроекты появлялись и ранее, однако не были приняты[53]. Однако популярный в настоящее время в средствах массовой информации и заявлениях публичных должностных лиц термин «киберпреступность» не используется[54] и не раскрывается в современном российском законодательстве[55].

Как итог, в настоящее время в российском законодательстве отсутствует четкое, полное определение понятия «киберпреступление». Более того, сохраняется проблема малорегламентированности или вовсе отсутствия регламентации со стороны нормативно-правовых актов[56], что поднимает вопрос о необходимости своевременного и адекватного правового сопровождения. Однако данное положение не отменяет необходимости дать его в рамках данной работы с целью дальнейшего продуктивного анализа проблемы. В рамках данного параграфа под киберпреступностью будем понимать *преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.* Именно таким образом Министерство внутренних дел РФ характеризует киберпреступность в своих отчетах о состоянии преступности в стране[57].

---

[53] Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству / Л.В. Иванова // Юридические исследования. – 2019. – №1. – С. 25–33.

[54] Кириленко В.П. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы / В.П. Кириленко, Г.В. Алексеев // Всероссийский криминологический журнал. – 2020. – Т. 14, № 6. – С. 898–913.

[55] Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству / Л.В. Иванова // Юридические исследования. – 2019. – №1. – С. 25–33.

[56] Плотникова Т.В., Котельникова О.В. Феномен киберпреступности в условиях XXI века / Т.В. Плотникова, О.В. Котельникова // Право: история и современность. – 2020. – № 3(12). – С. 141 – 150.

[57] https://мвд.рф/reports.

Социологическое определение феномена киберпреступности также нуждается в уточнении и детализации, поскольку полное, проработанное определение понятия киберпреступность – одна из отправных точек для глубокого и системного понимания данного феномена, которое необходимо для выработки эффективной стратегии противодействия. Рассмотрим существующие социологические определения понятия «киберпреступность». Д.Н. Карпова определяет киберпреступность как «акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет[58]». Доктор Грейз Варгезе в своем труде по социологическому исследованию различных типов киберпреступлений определяет киберпреступность как «все виды нежелательной, незаконной деятельности или злоупотреблений, имеющих место в киберпространстве и направленных против компьютера, Интернета и телекоммуникационных сетей, управляемых компьютером или технологией[59]». Радж Синха в работе по социологическому анализу социальных последствий киберпреступлений определяет киберпреступность как «преступления, совершаемые в Интернете с использованием компьютера в качестве инструмента или целевой жертвы[60]». Андреа де Никола в работе по социологическому исследованию организованных преступных группировок в киберпространстве определяет киберпреступность как «компьютерное мошенничество, преступления против личности, онлайн-вымогательство и программы-вымогатели, сексуальное насилие и эксплуатация над детьми в Интернете, отмывание

[58] Карпова Д.Н.: Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 46–50.
[59] Varghese Gr. (2016). A sociological study of different types of cyber crime, International Journal of Social Science and Humanities Research, Vol. 4, Issue 4, pp: (599-607).
[60] Sinha R. (2018). Social Impact of Cyber Crime: A Sociological Analysis, International Journal of Management, IT & Engineering Vol. 8 Issue 10(1).

денег в киберпространстве, которые чаще всего совершаются различными видами организованных преступных группировок[61]».

Проблема киберпреступности, важная и актуальная в последние годы, привлекает большой интерес представителей различных научных дисциплин, в том числе и социологов. В настоящий момент идет активное исследование различных аспектов данной проблемы и его влияние на разные стороны общественной жизни. Тем не менее, существующие в научной литературе социологические определения киберпреступности требуют уточнения и углубление. Выработка авторского определения данного понятия – одна из важных задач данного исследования.

Далее рассмотрим классификации киберпреступлений по различным основаниям. По объекту воздействия можно выделить следующие:

- киберпреступления против жизни и здоровья несовершеннолетних;
- против собственности, интеллектуальной собственности;
- общественной безопасности;
- общественного порядка;
- здоровья населения;
- общественной нравственности;
- компьютерной безопасности;
- против основ конституционного строя и безопасности государства, мира и безопасности человечества[62].

По способу и средствам совершения Межпарламентская Ассамблея государств – участников Содружества Независимых Государств разработала следующую классификацию киберпреступлений:

[61] Di Nicola, A. Towards digital organized crime and digital sociology of organized crime. Trends Organ Crim (2022).

[62] 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.

1) мошеннические действия с использованием сети Интернет, средств подвижной связи и систем дистанционного банковского обслуживания;

2) хищения через вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей путем подделки электронных средств идентификации платежей, использования идентификационных данных банковских карт;

3) иные способы хищений и причинения имущественного ущерба посредством использования средств подвижной связи (взимание повышенных сборов за телефонные звонки, мошенничество на платформах бесплатных объявлений, мошенничество в виде конкурса СМС-сообщений или теста на общие знания);

4) использование информационных технологий для совершения преступлений в сфере незаконного оборота наркотических средств, психотропных веществ и их прекурсоров;

5) использование информационных технологий с целью совершения преступлений против несовершеннолетних, в том числе склонение несовершеннолетних к совершению самоубийства, вовлечение их в порнобизнес;

6) использование информационных технологий для совершения преступлений террористического и экстремистского характера, в том числе кибертерроризма[63].

На основании статистических данных ГИАЦ МВД России исследователи выделили следующую структуру компьютерной преступности в стране:

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

[63] 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.

2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

3. Неправомерный доступ к компьютерной информации.

4. Создание, использование и распространение вредоносных компьютерных программ.

5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

6. Нарушение авторских и смежных прав, совершенное с использованием компьютерных и телекоммуникационных технологий.

7. Кража, совершенная с использованием компьютерных и телекоммуникационных технологий.

8. Мошенничество в сфере компьютерной информации.

9. Причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенное с использованием компьютерных и телекоммуникационных технологий.

10. Незаконные организация и проведение азартных игр, совершенные с использованием компьютерных и телекоммуникационных технологий.

11. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, совершенные с использованием компьютерных и телекоммуникационных технологий.

12. Незаконные изготовление и оборот порнографических материалов или предметов, совершенные с использованием компьютерных и телекоммуникационных технологий.

13. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием компьютерных и телекоммуникационных технологий.

14. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов, совершенное с использованием компьютерных и телекоммуникационных технологий[64].

Прежде чем перейти к детальному рассмотрению статистики по киберпреступлениям в России, дадим краткое описание актуального состояния киберпреступности в мире.

В 2023 году в отчете Всемирного экономического форума повсеместное распространение киберпреступности названо одним из главных глобальных рисков настоящего и будущего[65]. По итогам 2023 года общий ущерб от киберпреступности ожидается на уровне 8 триллионов долларов США с ростом до 10.5 триллионов к 2025 году[66]. Исследовательская компания Gartner прогнозирует[67], что к 2025 году 45% организаций по всему миру подвергнутся атакам на свои цепочки поставок программного обеспечения, что означает троекратный рост относительно 2021 года.

Уровень обеспокоенности растет и в экспертном сообществе. Экспертный опрос Всемирного экономического форума показал[68], что 74% из числа опрошенных экспертов в области информационных технологий не уверены в защите информационной инфраструктуры против кибератак.

---

[64] Скляров С.В., Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации / С.В. Скляров, К.Н. Евдокимов // Всероссийский криминологический журнал. – 2016. – №2 (Т. 10). – С. 322 – 330.

[65] World Economic Forum. The Global Risks Report 2023 18th Edition [Электронный ресурс]. Режим доступа: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (дата обращения: 09.12.2023).

[66] Cybercrime Magazine. Cybercrime To Cost The World 8 Trillion Annually In 2023 [Электронный ресурс]. Режим доступа: https://cybersecurityventures.com/cybercrime–to–cost–the–world–8–trillion–annually–in–2023/ (дата обращения: 10.12.2023).

[67] Gartner. 7 Top Trends in Cybersecurity for 2022 [Электронный ресурс]. Режим доступа: https://www.gartner.com/en/articles/7–top–trends–in–cybersecurity–for–2022 (дата обращения: 10.12.2023).

[68] World Economic Forum. State of the Connected World 2023 Edition [Электронный ресурс]. Режим доступа: https://www3.weforum.org/docs/WEF_State_of_the_Connected_World_2023_Edition.pdf (дата обращения: 10.12.2023).

В 2023 году Россия остается важным участником глобальной сети производства, обмена и потребления информации. Вызовы со стороны глобальной проблемы киберпреступности полностью актуальны и для нее. Компания в области кибербезопасности Surfshark в своем отчете[69] отмечает значительный рост количества взломанных аккаунтов электронной почты в России в 2022 году: около 8 из 10 российских интернет-пользователей столкнулись с данной проблемой в 2022 году. Это приблизительно в 17 раз выше, чем показатели по всему миру.

Компания по противодействию кибермошенничеству SEON составила свой индекс киберзащищенности стран мира[70], по результатам которого Россия заняла 37 место, оказавшись позади наиболее технологически развитых стран мира и заняв место между Новой Зеландией и Северной Македонией.

Перечисленная выше статистика вызывает озабоченность и требует более детального исследования состояния и динамики киберпреступности в России.

Для понимания масштаба проблемы киберпреступности в России проанализируем актуальные данные официальных органов власти. Важно подчеркнуть, что данная статистика отражает только официально зарегистрированные преступления и не учитывает те правонарушения, которые не были официально задокументированы. Тем не менее, данные официальной статистики дают представление о сложившемся в последние годы тренде и масштабе проблемы киберпреступности в России.

В качестве источника данных для анализа состояния киберпреступности в России будем использовать статистику Министерства внутренних дел РФ, которая публикуется на официальном сайте

[69] Surfshark. Cybercrime statistics [Электронный ресурс]. Режим доступа: https://surfshark.com/research/data–breach–impact/statistics (дата обращения: 10.12.2023).

[70] SEON. Global Cybercrime Report: Which Countries Are Most at Risk in 2023? [Электронный ресурс]. Режим доступа: https://seon.io/resources/global–cybercrime–report/ (дата обращения: 10.12.2023).

https://мвд.рф в разделе[71] отчетов о состоянии преступности в стране. В этом разделе на ежемесячной основе, начиная с 2003 года, происходит публикация отчета-характеристики о состоянии преступности в РФ за прошедший месяц.

Обратимся к содержимому данного отчета. Отчет содержит краткую характеристику о состоянии преступности в России, а также наиболее значимые тренды и изменения. Далее на странице располагается файл, содержащий более детальный отчет, который представлен в формате PDF. Данный файл содержит следующую информацию[72]: данные в разрезе по типам преступлений, информация о потерпевших и нарушителях порядка, данные о раскрытых преступлениях, а также региональная сводка.

Для анализа в рамках данного параграфа будет использоваться статистика по преступлениям, которые были совершены с использованием информационно-коммуникационных технологий или в сфере компьютерной информации.

Для иллюстрации стремительного нарастания проблемы киберпреступности в России построим график, который отражает количество официально зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в 2017-2023 годах.

[71] https://мвд.рф/reports.

[72] На примере краткой характеристики состояния преступности в Российской Федерации за январь–август 2021 года. Режим доступа: https://мвд.рф/reports/item/26023627/ (дата обращения: 10.06.2023).

Рисунок 1. Количество официально зарегистрированных преступлений в 2017-2023 годах, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Составлено автором по материалам кратких характеристик состояния преступности в Российской

Федерации за январь-декабрь 2017[73], 2018[74], 2019[75], 2020[76], 2021[77], 2022[78] и 2023[79] годов

Данный график отражает стремительный рост количества киберпреступлений за последние 6 лет в России. Начавшись еще за несколько лет до пандемии, нарастание проблемы продолжилось и в 2020 году, достигнув своих локальных максимумов и сохраняясь на них до сих пор. Как итог, по состоянию на 2024 год проблему киберпреступности можно охарактеризовать как одну из угроз национальной безопасности по степени проникновения и потенциальному масштабу ущерба для экономики и граждан России.

Кроме общего количества зарегистрированных киберпреступлений в абсолютных числах внимания заслуживают и относительные показатели. Далее проанализируем изменения доли киберпреступлений в общем объеме всех зарегистрированных преступлений в стране.

---

[73] Состояние преступности в Российской Федерации за январь – декабрь 2017 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/12167987/ (дата обращения: 10.06.2023).

[74] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2018 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/16053092/ (дата обращения: 10.06.2023).

[75] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2019 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/19412450/ (дата обращения: 10.06.2023).

[76] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2020 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/22678184/ (дата обращения: 10.06.2023).

[77] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/28021552/ (дата обращения: 10.06.2023).

[78] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/35396677/ (дата обращения: 10.06.2023).

[79] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/47055751/ (дата обращения: 10.04.2024).

Рисунок 2. Доля (в процентах) киберпреступлений по годам среди всех зарегистрированных преступлений в 2017-2023 годах. Составлено автором по материалам кратких характеристик состояния преступности в Российской Федерации за январь-декабрь 2017[80], 2018[81], 2019[82], 2020[83], 2021[84], 2022[85] и 2023[86] годов

Важно отметить, что всего за 4 года произошел более чем пятикратный рост доли киберпреступлений: начиная с 2020 года каждое четвертое преступление совершено с использованием информационно-телекоммуникационных технологий, в 2023 году – уже примерно каждое третье. Таким образом, всего за несколько лет проблема киберпреступности

[80] Состояние преступности в Российской Федерации за январь – декабрь 2017 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/12167987/ (дата обращения: 10.06.2023).
[81] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2018 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/16053092/ (дата обращения: 10.06.2023).
[82] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2019 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/19412450/ (дата обращения: 10.06.2023).
[83] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2020 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/22678184/ (дата обращения: 10.06.2023).
[84] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/28021552/ (дата обращения: 10.06.2023).
[85] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/35396677/ (дата обращения: 10.06.2023).
[86] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/47055751/ (дата обращения: 10.04.2024).

из проблемы локальной, отраслевой, касающейся лишь определенной части населения, переросла в угрозу национального масштаба для всего государства и вызов для правоохранительных органов. Сегодня киберпреступность становится одной из наиболее серьезных проблем современного российского общества, наносящей огромный урон российской экономике и благосостоянию граждан[87].

Важный аспект этой проблемы – это изобретательность и техническая подкованность правонарушителей, возможность быстро адаптироваться под меняющиеся условия. Сегодня наиболее продвинутые преступники в высочайшей степени освоили возможности технологий по обеспечению анонимности в Интернете, сбору данных о потенциальных жертвах, технических возможностях создания фальшивых личностей и психологических манипуляций. А огромные средства, полученные преступным путем, позволяют поддерживать высокий уровень анонимности и технической продвинутости для продолжения преступной деятельности.

В связи с этим особого внимания заслуживает изучение аналитики по раскрываемости киберпреступлений в России за последние годы. Это одна из самых важных характеристик, которая отражает возможности российского государства по противостоянию новой волне киберпреступности, а также уровень подготовленности к отражению подобных атак в будущем.

[87] Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства / П.С. Швыряев // Государственное управление. Электронный вестник. – 2021. – № 89. – С. 184–196.

Рисунок 3. Доля нераскрытых киберпреступлений относительно всех зарегистрированных преступлений в 2017-2023 годах. Составлено автором по материалам кратких характеристик состояния преступности в Российской Федерации за январь-декабрь 2017[88], 2018[89], 2019[90], 2020[91], 2021[92], 2022[93] и 2023[94] годов

Несмотря на некоторое улучшение ситуации в последние 2 года, ее общее состояние вызывает беспокойство. Причем в подавляющем

[88] Состояние преступности в Российской Федерации за январь – декабрь 2017 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/12167987/ (дата обращения: 10.06.2023).
[89] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2018 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/16053092/ (дата обращения: 10.06.2023).
[90] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2019 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/19412450/ (дата обращения: 10.06.2023).
[91] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2020 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/22678184/ (дата обращения: 10.06.2023).
[92] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2021 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/28021552/ (дата обращения: 10.06.2023).
[93] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/35396677/ (дата обращения: 10.06.2023).
[94] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/47055751/ (дата обращения: 10.04.2024).

большинстве случаев правоохранителям не удается не только привлечь к ответственности преступника, но даже идентифицировать его личность. Так, по заявлениям юриста и члена экспертного совета по экономике в Госдуме РФ Алексея Микаелова, по состоянию на 2021 год в 75% случаев производство по уголовным делам приостанавливают за неустановлением обвиняемого, и только 7% направляется в суд для дальнейшего разбирательства[95]. Данная статистика – показатель степени готовности российских правоохранительных органов к очередной волне цифровизации и пришедшему вместе с ней всплеску киберпреступности в последние годы. Серьезный кризис, связанный с возможностями раскрытия киберпреступлений, отмечается и на самом высоком уровне. Так, генпрокурор РФ Игорь Краснов в разгар пандемии в 2020 заявил о «низкой способности противостоять этому новому виду преступности», а кибермошенничество, по словами Краснова, «по сути, вообще не раскрывается»[96].

О превращении проблемы киберпреступности в угрозу национальной безопасности свидетельствует и тот факт, что акцентирует внимание на проблеме лично глава государства. На расширенной коллегии МВД в марте 2023 года Владимир Путин подчеркнул, что «один из безусловных приоритетов вашей работы – это борьба с преступностью с использованием информационных технологий», а количество киберпреступлений за 2022 год «впечатлило» президента[97]. В своей речи глава государства особое внимание

[95] Известия. Их слишком много: почему киберпреступления остаются нераскрытыми. [Электронный ресурс]. Режим доступа: https://iz.ru/1166840/mariia–nemtceva/ikh–slishkom–mnogo–pochemu–kiberprestupleniia–ostaiutsia–neraskrytymi (дата обращения: 12.06.2023).
[96] Интерфакс. Генпрокурор РФ заявил о бессилии правоохранительных органов перед киберпреступниками. [Электронный ресурс]. Режим доступа: https://www.interfax.ru/russia/699548 (дата обращения: 12.06.2023).
[97] РИА Новости. Путин прокомментировал рост киберпреступности. [Электронный ресурс]. Режим доступа: https://ria.ru/20230320/kiber–1859136636.html (дата обращения: 12.06.2023).

уделил информированию граждан о новых разновидностях преступлений и повышению цифровой грамотности населения.

Наиболее опасным и эффективным инструментом в арсенале кибермошенников сегодня является социальная инженерия. Согласно отчету[98] компании Positive Technologies за 2022 год, в мире данный метод использовался в 93% успешных атак на частных лиц и 43% – на организации. Данный метод популярен и в России, что отмечается в отчетности[99] Банка России: доля социальной инженерии в операциях без согласия клиентов за 2022 год составила чуть больше половины (50.4%). При этом в первом квартале 2023 года в Банке России отмечают значительный рост (на 69.94%) использования методов социальной инженерии по сравнению с 2022 годом. Данный метод совершения киберпреступлений набрал особую популярность в период пандемии и остается одним из наиболее эффективных по сегодняшний день. И это закономерно: киберпреступники, столкнувшись с серьезным отпором со стороны продвинутых цифровых систем безопасности, в период форсированной цифровизации во время пандемии осуществили «поворот» от технологий назад к человеку. Почему так произошло?

На протяжении последних десятилетий, по мере усложнения технологических систем, вопрос о защите цифровых систем вставал все острее. Массовые и серьезные по своим последствиям кибератаки на критическую инфраструктуру нашли ответ в развитии индустрии информационной безопасности. Безусловно, это касается не только защищенности цифровых платформ организаций, но и обучения персонала, в том числе и повышению защищенности в отношении методов социальной инженерии. Тем не менее, даже продвинутые в технологическом плане

[98] Positive Technologies. Актуальные киберугрозы: итоги 2022 года. [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru–ru/research/analytics/cybersecurity–threatscape–2022/#id9 (дата обращения: 12.06.2023).

[99] Банк России. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/statistics/ib/review_1q_2023/ (дата обращения: 12.06.2023).

организации становятся жертвами мошенников по причине халатности или ангажированности собственных сотрудников. Важно понимать, что с точки зрения информационной безопасности организация не представляет собой гомогенную сущность, противопоставленную внешнему миру, а каждый ее член рассматривается как потенциальная угроза и нарушитель конфиденциальности[100]. Такой подход формирует высокие стандарты информационной защиты в ведущих технологических компаниях России и мира, что в определенной степени позволило сгладить масштаб последствий во время ускоренной цифровизации времен пандемии. Чего нельзя сказать о более массовом сегменте – рядовых гражданах страны.

Если ресурсы технологических компаний или государственных органов позволяют обеспечивать высокий уровень технологической защищенности, то гражданское население и их имущество все еще остается под большой угрозой. Ретроспективно анализируя статистику за последние несколько лет, сегодня становится очевидным, что важные несколько лет до наступления 2020 года были потеряны с точки зрения обеспечения защищенности населения страны от киберугроз и формирования массового иммунитета. Еще в 2018 году эксперты НАФИ отмечали легкомысленность россиян в вопросах кибербезопасности[101]. Уже через несколько лет эта легкомысленность обернулась катастрофой государственного масштаба: по данным SuperJob, в 2021 году каждый шестой россиянин пострадал от действий только телефонных мошенников[102].

---

[100] Швыряев П.С. Утечки конфиденциальных данных: главный враг внутри / П.С. Швыряев // Государственное управление. Электронный вестник. – 2022. – № 91. – С. 226–241.

[101] РБК. Аналитики оценили уровень цифровой грамотности россиян. [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/20/06/2018/5b29331c9a79477930b03101 (дата обращения: 12.06.2023).

[102] РБК. Каждый шестой россиянин пострадал из–за телефонных мошенников. [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/02/10/2021/6156e99a9a794778904993ed (дата обращения: 12.06.2023).

По итогам 2022 года, общий объем средств по операциям, произведенным без согласия клиентов финансовых организаций, составил рекордные 14,1 млрд рублей[103]. При этом более 90% от этой суммы – 13,3 млрд – приходится на долю физических лиц. При этом заслуживает особого внимания динамика снижения количества таких операций: если в 2021 году таких было 1035,01 тыс. единиц, то в 2022 уже 876,59. Существенное снижение количества операций говорит о двух трендах. Во-первых, нельзя не отметить положительную динамику в вопросах информирования населения и совместной работе ЦБ, банков и операторов связи по противодействию мошенническим активностям в отношении населения страны. Несмотря на то, что по данному вопросе предстоит проделать еще очень много работы, позитивный сдвиг в вопросе противодействия мошенническим действиям есть. Во-вторых, растет средняя сумма одного хищения. Если в период пандемии мошеннические кампании можно было охарактеризовать как охватные и направленные на широкий круг потенциальных жертв, то сегодня мошенники все чаще предпочитают совершать точечные операции в отношении граждан, располагающих средствами, которые могут быть похищены. Доступ к информации, которая может быть использована для совершения противоправных действий, – еще одна важная проблема и направление для исследования.

В России в последние несколько лет отчетливо сформировался тренд на создание и наполнение масштабных баз данных, которые будут содержать информацию о населении страны. Например, в 2023 году ведется разработка электронного реестра военнообязанных, в которую войдут персональные данные из различных структур: ФНС, МВД, Центральной избирательной

[103] Банк России. Обзор операций, совершенных без согласия клиентов финансовых организаций. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 13.06.2023).

комиссии (ЦИК), ЗАГСов, медицинских и образовательных организаций[104]. Процесс оцифровки различных процессов, переноса информации с физических носителей на цифровые неизбежно сталкивается с проблемой надежного и безопасного хранения данных. Спешка, с которой такие базы могут создаваться и вводиться в эксплуатацию, – источник дополнительного риска с точки зрения компрометации данных этих баз. Поспешность и неосмотрительность в данном вопросе могут иметь крайне негативные последствия. Цена возможной ошибки – это конфиденциальная информация в руках мошенников, которая и используется при совершении противоправных действий. Конфиденциальная информация – это тот ресурс, который подпитывает киберпреступную деятельность и серьезно повышает эффективность совершаемых незаконных деяний. Ограничение несанкционированного доступа к конфиденциальной информации, снижение количества утечек и компрометации данных – одно из ключевых направлений деятельности в борьбе с киберпреступностью.

Для понимания актуального состояния проблемы утечек информации ограниченного доступа в России обратимся к отчету группы компаний InfoWatch за 2022 год[105].

[104] Forbes. Повестка дня: во сколько может обойтись создание электронного реестра военнообязанных. [Электронный ресурс]. Режим доступа: https://www.forbes.ru/tekhnologii/487484–povestka–dna–vo–skol–ko–mozet–obojtis–sozdanie–elektronnogo–reestra–voennoobazannyh (дата обращения: 15.06.2023).

[105] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

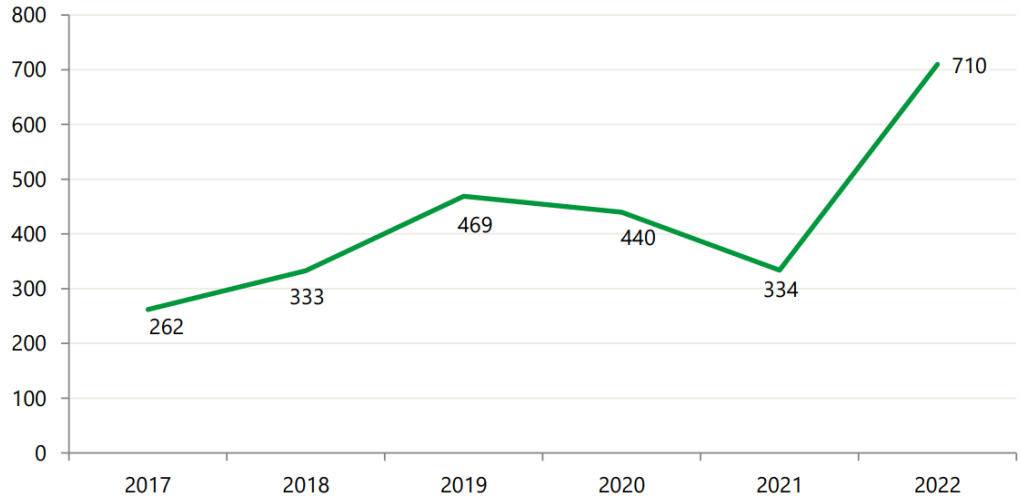

Рисунок 4. Количество утечек конфиденциальных данных в России в 2017-2022 гг.[106]

В 2022 году исследователи отмечают серьезный, более чем в 2,1 раза по сравнению с 2021 годом, рост количества зарегистрированных утечек информации. Такой резкий всплеск – ожидаемое явление на фоне экстраординарных событий в мире и России в 2022 году. Если в предыдущие пандемийные годы характер утечек носил скрытый характер, компрометацию данных не всегда можно было оперативно обнаружить, то в 2022 году эти данные попадали в публичное поле как инструмент достижения целей различными группами интересов. Исследователи отмечают[107] и повышение хакерской активности в 2022 году: противостояния между государствами и блоками стран сегодня неизбежно выливаются в конфронтацию и в киберпространстве.

Впечатляет и рост количества утекших записей персональных данных и платежной информации. За пять лет произошел скачок более чем в сто раз.

[106] Там же.

[107] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

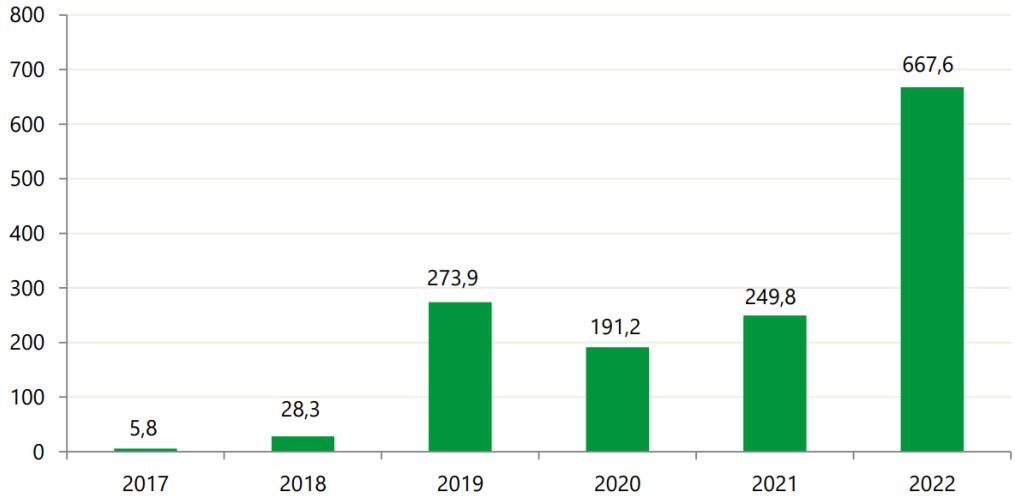

Рисунок 5. Количество утекших записей ПДн и платежной информации, млн: Россия, 2017-2022 гг.[108]

Очевидно, что утечка записей персональных данных в России в настоящее время приобретает неконтролируемый характер: регулярно приходят новости об утечках данных россиян из баз крупнейших российских компаний самых разных отраслей: банковский сектор, доставка, такси, электронная коммерция, сфера развлечений и другие.

Важно отметить еще один новый тренд в сфере утечек данных в России: проблема становится актуальной не только для крупного, но и для среднего и малого бизнеса.

[108] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

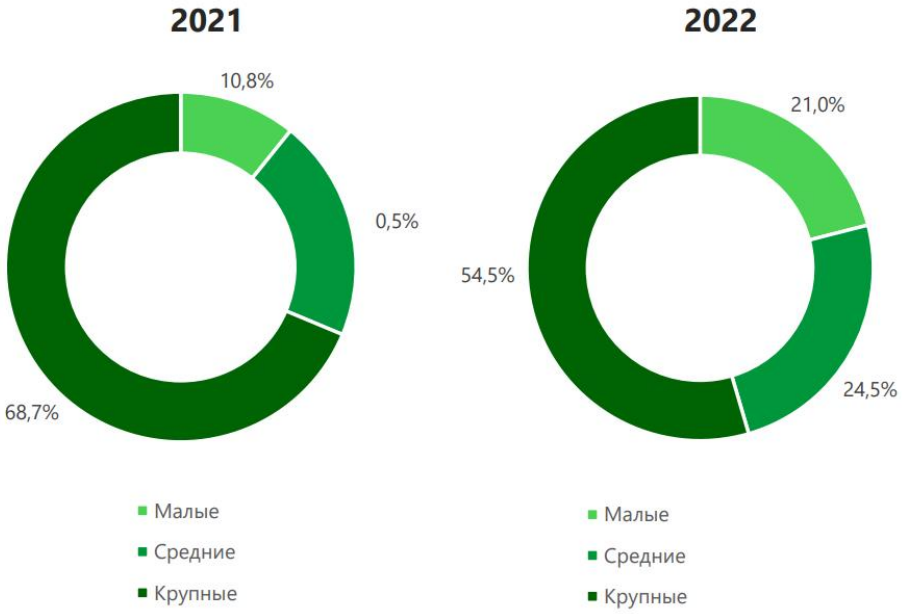

Рисунок 6. Распределение утечек данных по размеру пострадавших организаций: Россия, 2021-2022 гг[109].

Тренд на цифровизацию в последние годы затронул не только крупные компании, но и средний и малый бизнес. Перевод бизнеса в цифровое пространство во многом позволил пережить сложный период пандемийных ограничений, однако обернулся серьезными проблемами. В настоящий момент большое количество малых предприятий аккумулируют в своих базах чувствительную информацию о своей организации, клиентах и контрагентах, которая может представлять особый интерес для кибермошенников. При этом степень защищенности этих данных, уровень информационной безопасности на предприятии может быть крайне низким: в условиях решения вопроса выживаемости в агрессивных условиях проблемы защищенности данных нередко отходят на второстепенный план. С начала 2022 года российский бизнес находится в условиях экстремального санкционного давления, нарушения привычных цепочек поставок и переориентации на другие рынки. В таких условиях проблема утечек данных

[109] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

на предприятиях малого и среднего бизнеса может еще сильнее усугубиться в 2023 и последующих годах.

Еще один тренд прошедшего 2022 года – это отсутствие достаточного количества сведений, которые бы позволили идентифицировать источник и характер утечки[110].

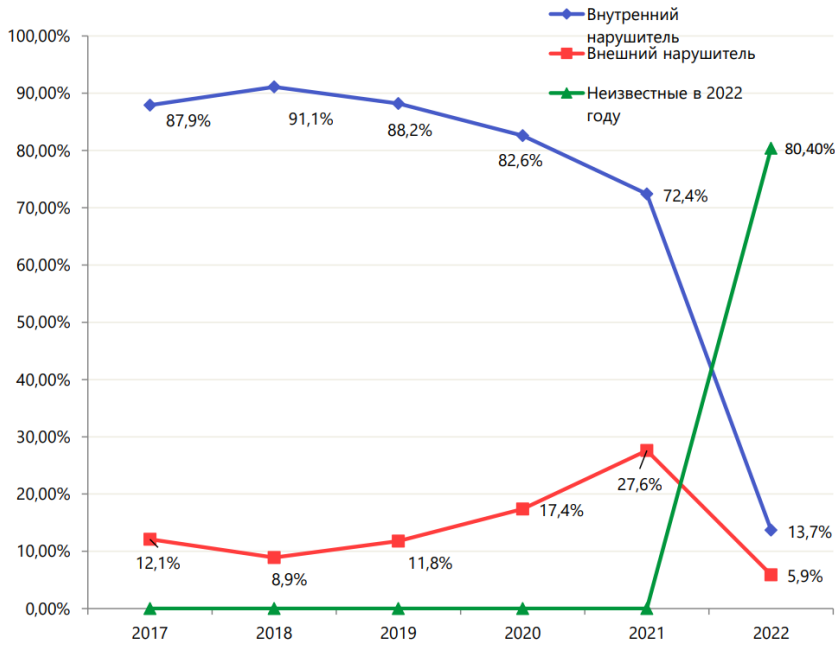

Рисунок 7. Распределение утечек информации по вектору воздействия (внешний/внутренний), в процентах: Россия, 2017-2022 гг.[111]

Рост количества такого рода атак, где достоверно источник атаки невозможно установить, либо он носит смешанный (внутренний и внешний) характер – еще одна проблема для исследователей и препятствие на пути анализа причин утечек данных. Если в предыдущие годы главным источником угрозы был внутренний нарушитель, то в 2022 году растет количество гибридных атак, что дополнительно затрудняет как

[110] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

[111] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

расследование таких инцидентов, так и реализацию мер по предотвращению подобных ситуаций в будущем. Это отмечают и исследователи: в последние годы возросла сложность по выявлению инцидентов и ликвидации их последствий, а кибератаки все чаще носят изощренный и целевой характер[112].

Растет и доля умышленных утечек конфиденциальных данных.

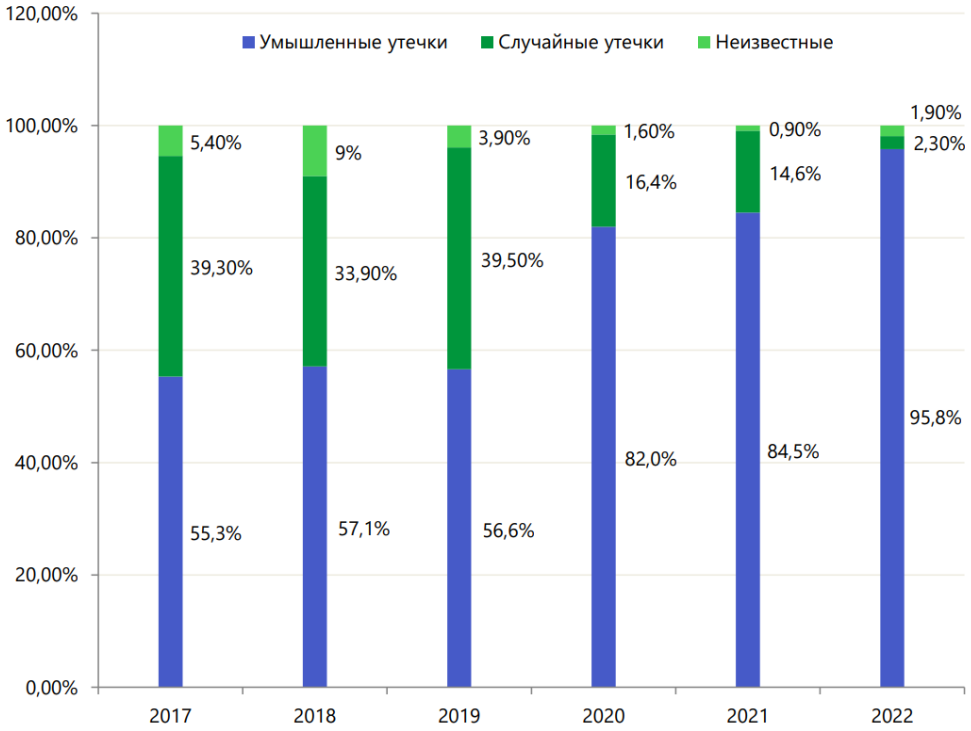

Рисунок 8. Распределение утечек информации по характеру умысла (умышленные и случайные, за счет как внешнего, так и внутреннего нарушителя), в процентах: Россия, 2017-2022 гг[113].

Можно сказать, что практически все утечки данных в России в 2022 году носят умышленный, то есть спланированный характер. Если проблему случайных утечек удалось в высокой степени побороть с помощью использования специальных DLP-систем и практик защиты информации, то

[112] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

[113] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

проблема умышленных утечек гораздо более серьезная и требующая значительных ресурсов для ее решения.

По итогам 2022 года физические лица остаются главными жертвами утечек данных.

Рисунок 9. Распределение утечек по типам данных: Россия, 2021-2022 гг[114].

Приведенная статистика наглядно показывает, что рядовой пользователь и его данные остаются главной добычей похитителей, и в дальнейшем активно используется для совершения преступных действий.

Таким образом, 2022 год стал беспрецедентным с точки зрения утечек данных как в России, так и во всем мире. По данным Роскомнадзора, в 2022 году в России произошло около 150 крупных утечек персональных данных, но суммарно суды по составленным протоколам назначили штрафов всего на 1 млн рублей[115] – несущественная сумма для российского бизнеса. В

[114] InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

[115] Forbes. Роскомнадзор насчитал около 150 крупных утечек личных данных в 2022 году. [Электронный ресурс]. Режим доступа: https://www.forbes.ru/tekhnologii/484301–roskomnadzor–nascital–okolo–150–krupnyh–utecek–licnyh–dannyh–v–2022–godu (дата обращения: 16.06.2023).

сложившейся ситуации государство решило пойти на ужесточение законодательства за утечки данных: предлагается ввести оборотные штрафы за утечки данных в 2023 году[116]. Безусловно, ужесточение ответственности за утечку данных будет иметь определенный положительный эффект. Но достаточны ли эти меры для решения проблемы утечек данных? По всей видимости, нет.

Исключительные события 2022 года показали незащищенность российской инфраструктуры перед лицом опасности, исходящей извне. Можно заключить, что цель нанести репутационный ущерб российскому бизнесу в определенной степени достигнута: массовые кибератаки вскрыли несовершенства систем безопасности, предстоит огромная работа над ошибками. Деятельность властей, конкретные меры по ужесточению ответственности за утечки можно назвать ожидаемыми, но нельзя охарактеризовать как достаточные для принципиального изменения ситуации. В перспективе ближайших лет количество утечек сохранится на высоком уровне: для решения проблемы требуется комплексный аудит используемых технологических систем, серьезные инвестиции в повышение информационной безопасности предприятий, обучение персонала. В агрессивных условиях последних нескольких лет, где многие отрасли бизнеса находятся на грани выживания, данная деятельность, по всей видимости, не будет являться первостепенной.

На основании анализа актуального состояния киберпреступности в России можно сделать следующие ключевые выводы.

1. По состоянию на 2024 год в России киберпреступность приобрела черты угрозы государственного масштаба. Данная проблема требует серьезного внимания со стороны всех заинтересованных субъектов:

[116] Ведомости. Путин поручил разобраться с оборотными штрафами за утечки данных к июлю. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/technology/articles/2023/01/13/959007–putin–oborotnimi–shtrafami (дата обращения: 16.06.2023).

бизнеса, общества и особенно государства, поскольку технологический прогресс и экономическая эффективность способствуют быстрому развитию и цифровизации всех сфер государственного управления[117].

2. Сложившаяся ситуация – это результат отсутствия системных, эффективных мер, направленных на решение проблемы. На графиках официальной статистики показано, что драгоценное время было упущено. Был не замечен или проигнорирован новый тренд – переход преступлений в цифровую реальность по мере углубляющегося процесса цифровизации в стране и мире. Как итог, данный процесс приобрел черты социального взрыва в 2020 году на фоне форсированной цифровизации в эпоху пандемии. Система оказалась не готова к масштабным изменениям, в то же время преступное сообщество умело воспользовалось моментом.

3. 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. Отмечается, что предпринимающиеся сегодня меры в данной области недостаточны: требуется более активное, комплексное и ресурсное участие как государственных, так и негосударственных акторов.

4. Сохраняется высокая доля нераскрытых киберпреступлений. Помимо того, что российские правоохранительные органы отстают в технических возможностях[118], проблема усугубляется ухудшением в 2022 году отношений с целым рядом технологически развитых стран, усложняется

[117] Стырин Е.М. Единая информационная система в сфере закупок как государственная цифровая платформа: современное состояние и перспективы / Е.М. Стырин, Ю.Д. РоДионова // Вопросы государственного и муниципального управления. – 2020. – № 3. – С. 49 – 70.

[118] ТАСС. ГП: правоохранительные органы отстают в технических возможностях от киберпреступников [Электронный ресурс]. Режим доступа: https://tass.ru/politika/8915711 (дата обращения: 16.07.2023).

обмен информацией по линии Интерпола[119]. Здесь важно еще раз подчеркнуть, что киберпреступность – это проблема международного характера, которая не имеет границ и требует тесного взаимодействия спецслужб и правоохранительных органов разных государств. Не только для более эффективной раскрываемости киберпреступлений, но и обмена опытом, передачи знаний и использования передовых наработок. В проекте Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях[120] сказано, что «преступления в сфере ИКТ представляют собой транснациональное явление, которое затрагивает общество и экономику всех государств, что обусловливает исключительно важное значение международного сотрудничества в области предупреждения указанных преступлений и борьбы с ними». О необходимости тесного международного сотрудничества в борьбе с киберпреступностью неоднократно заявляло высшее политическое руководство страны, включая Президента[121]. В 2022 году перспективы международного сотрудничества России по вопросам борьбы с киберпреступностью оказались под угрозой: накладываются санкции, нарушается обмен опытом и знаниями, замораживаются совместные проекты. Сложившаяся обстановка и серьезные внешние вызовы требуют пересмотра и актуализации стратегии борьбы с киберпреступностью в новых реалиях, в которых оказалось российское государство после февраля 2022 года.

---

[119] РБК. Интерпол решил не исключать Россию из организации [Электронный ресурс]. Режим доступа: https://www.rbc.ru/politics/11/03/2022/622a58609a794796f4c3dbe1 (дата обращения: 16.07.2023).

[120] Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно–коммуникационных технологий в преступных целях от 29.06.2021 [Электронный ресурс]. Режим доступа: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 17.07.2023)

[121] Kremlin.ru. Инвестиционный форум «Россия зовет!» [Электронный ресурс]. Режим доступа: http://kremlin.ru/events/president/transcripts/67241 (дата обращения: 17.07.2023).

5. Увеличивается количество атак из других стран, в том числе недружественных. Поскольку возможности международного взаимодействия по вопросам расследования подобного рода инцидентов в настоящий момент ограничены, актуальным становится вопрос о реализации стратегии по выработке защиты к подобного рода атакам, своего рода «иммунитета», причем как технологического, так и социального.

6. В российском обществе сформировался отчетливый запрос на безопасные технологические системы: для того, чтобы цифровой сервис был востребован, он должен быть надежным, гарантировать достоверность и безопасность данных[122]. Показательны результаты опроса, проведенные в 2021 году ВЦИОМ совместно с Ассоциацией больших данных[123]: 74% опрошенных россиян считают себя полностью не защищенными или скорее незащищенными от краж и утечек персональных данных. Существует в российском обществе и запрос на повышение цифровой грамотности населения. Данные социологического опроса[124] показывают: подавляющее большинство респондентов (80%) заявило о том, что хотело бы повысить уровень цифровой грамотности. Несмотря на все негативные события последних лет, связанных с технологическими инцидентами, Россия остается страной технооптимистов[125]. Более того, технологическое развитие является одним из приоритетов российского государства. Как в сложившейся

[122] Оценка цифровой готовности населения России [Текст] : докл. к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / Н. Е. Дмитриева (рук. авт. кол.), А. Б. Жулин, Р. Е. Артамонов, Э. А. Титов; Нац. исслед. ун–т «Высшая школа экономики». – М. : Изд. дом Высшей школы экономики, 2021. – 86 С.

[123] ВЦИОМ. Сохранность персональных данных [Электронный ресурс]. Режим доступа: https://wciom.ru/analytical–reviews/analiticheskii–obzor/sokhrannost–personalnykh–dannykh (дата обращения: 23.09.2023).

[124] ООО «Журнал «КО». Более 80% россиян готовы повысить свои знания в области цифровых прав [Электронный ресурс]. Режим доступа: https://ko.ru/news/bolee–80–rossiyan–gotovy–povysit–svoi–znaniya–v–oblasti–tsifrovykh–prav/ (дата обращения: 17.07.2023).

[125] ВЦИОМ. Россия – страна технооптимистов [Электронный ресурс]. Режим доступа: https://wciom.ru/analytical–reviews/analiticheskii–obzor/rossiya–strana–tekhnooptimistov (дата обращения: 17.07.2023).

ситуации не растерять веру граждан России в возможность безопасного технологического развития страны?

7. Фиксируется значительный рост количества утечек конфиденциальных данных в 2022 году: более чем в 2,1 раза по сравнению с 2021 годом. Россия столкнулась с беспрецедентным внешним давлением в том числе и в цифровой среде, что вылилось в рост количества инцидентов, наиболее опасные из которых – утечки конфиденциальных данных. Такой стремительный рост количества утечек – проявление тех проблем, которые накапливались в течение долгих лет и вылились наружу в период международной напряженности в 2022-2023 годах.

8. Проблема утечек конфиденциальных данных приобрела массовый характер и в настоящее время затрагивает практически все активное население страны. Исследователи отмечают возросшее количество атак не только на крупные, но средние и малые предприятия страны. Наряду с корпорациями и крупнейшими предприятиями, малый и средний бизнес аккумулирует чувствительную информацию о себе, своих клиентах и контрагентах. Но в отличие от крупного бизнеса, небольшие организации имеют гораздо более скромные возможности, ресурсы и бюджеты по обеспечению информационной безопасности и защиты от несанкционированного доступа к данным. Обеспечение безопасности и надежности цифровых систем малого и среднего бизнеса – еще одна важная задача в борьбе с киберпреступностью, поскольку именно скомпрометированные данные выступают важным источником информации в процессе подготовки и совершения незаконных действий в цифровой среде.

9. Согласно официальным данным Банка России[126], в 2022 году главными потерпевшими по операциям, произведенным без согласия

[126] Банк России. Обзор операций, совершенных без согласия клиентов финансовых организаций. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 13.06.2023).

клиентов финансовых организаций, являются физические лица. Причем точность киберпреступлений растет: если раньше были популярны масштабные охватные кампании, рассчитанные на большое количество потенциальных жертв, то в настоящее время киберпреступники фокусируются на конкретных жертвах. И значительную помощь в таких точечных атаках играют скомпрометированные данные, использование которых повышает эффективность атаки.

10. 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. Минимизировать риски перехода на отечественные информационные системы – одна из приоритетных задач, качество выполнения которой будет определять степень надежности российского технологического ландшафта в ближайшие годы.

11. 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. Но на сегодняшний момент очевидно, что предпринимаемые меры по возвращению уехавших специалистов носят ограниченный характер. Отъезд опытных ИТ-специалистов, в том числе в сфере информационной безопасности, и их переориентация на экономики других стран – еще одна серьезная проблема в борьбе с киберпреступностью.

Таким образом, решение проблемы киберпреступности в России сегодня остается крайне актуальным. Несмотря на предпринимаемые меры со стороны государства, общества и бизнеса, проблема остается особенно острой на протяжении последних трех лет. Можно констатировать, что

проблема киберпреступности в России сегодня идет по негативному сценарию.

Характерная черта политики в области противодействия киберпреступности в России – это ответная реакция на уже сложившуюся ситуацию и произошедшие инциденты, а не систематическая, фундаментальная работа на опережение для долгосрочного устойчивого развития государства. Отсутствует системный, эффективный план по устранению ситуации с акцентом на фундаментальные причины данной проблемы, которые лежат прежде всего в социальной, а не в технологической плоскости. Понимание социальной природы проблемы киберпреступности важно по следующим причинам. Во-первых, для осознания и понимания всей многогранности проблемы и факторов, влияющих на характер ее протекания. Во-вторых, только через глубокое понимание проблемы можно выработать комплексную и эффективную стратегию решения проблемы.

§ 1.2 Социальная природа киберпреступности

От анализа актуального состояния и динамики киберпреступности перейдем к рассмотрению природы данного явления.

Зародившись в XX веке, киберпреступность прошла несколько этапов своего развития:

1. Зарождение в 1960-х годах, на которые приходится появление сети Интернет.

2. Становление в 1970-х годах, на которые приходится появление субкультуры хакеров, представляющих собой преступников с высокой степенью знаний и подготовки в области компьютерных программ и устройств. Киберпреступность на данном этапе – деятельность узкого круга злоумышленников.

3. Глобальное распространение, которое продолжается с 1990-х годов в условиях, когда киберпреступность носит повсеместный, глобальный характер.

Исходя из описанных этапов, менялось и понимание киберпреступности в исследовательском сообществе. Дискуссии о природе киберпреступности продолжаются до сих пор, поскольку киберпреступность – объект исследования целого ряда наук.

Как противоправная деятельность киберпреступность рассматривается представителями юридических наук. Как несанкционированный доступ к системам, деятельность вредоносных программ – специалистами в области информационной безопасности. Социальные антропологи исследуют закономерности формирования и функционирования хакерских группировок, а экономисты – ущерб экономике от киберпреступной деятельности.

Киберпреступность – многогранная, уже глубоко укорененная в обществе социальная проблема. Описанные выше подходы к рассмотрению киберпреступности – важные элементы пазла для выстраивания целостного, системного понимания данного феномена, который сам по себе является социальной проблемой и имеет социальную природу. На описание социальной природы киберпреступности и направлен данный параграф диссертационного исследования.

В рамках данного параграфа рассмотрим два важных вопроса, необходимые для понимания социальных оснований проблемы киберпреступности. Цель данного параграфа – показать, что киберпреступность – многосоставная, сложная социальная проблема, которая затрагивает все сферы общества и требует комплексного, системного подхода к ее решению. Ответим на важный исследовательский вопрос: каковы причины считать данную проблему не просто социальной, но и глобальной, то есть касающейся всех стран и субъектов: населения,

государственных органов и политических акторов, коммерческих и некоммерческих организаций?

Одно из ключевых событий последних лет в рамках данного анализа – это масштабный по своему размаху и форсированный по своим темпам процесс цифровизации различных аспектов жизнедеятельности человека, особенно заметно проявивший себя во время пандемии COVID-19. Пандемия выступила «великим ускорителем»[127] процессов, на которые в «мирное» время могли потребоваться годы или даже десятилетия.

Сегодня ключевой тенденцией экономического развития стало проникновение новых цифровых технологий во все сферы жизнедеятельности человека[128]. Цифровизация – важный социальный процесс, повышающий уровень и качество жизни, благосостояние населения планеты и движущий вперед научно-технический прогресс.

Цифровые технологии все более прочно укореняются в жизни миллиардов людей. Данное обстоятельство создало благоприятную основу для распространения киберпреступности по всему миру. Особенно отчетливо это можно было наблюдать во время локдаунов в течение пандемии COVID-19, когда на проблему обратили внимание ведущие мировые лидеры[129][130]. В то время, как ежедневная рутинная активность сместилась с физического в онлайн-окружение, возможности для совершения преступлений, в свою очередь, также сместились в сторону

[127] Amankwah–Amoah J., Khan Z., Wood G., Knight G. 2021. COVID-19 and digitalization: The great acceleration // Journal of Business Research, Elsevier, vol. 136(C), pages 602–611.
[128] Ватутина Л.А., Злобина Е.Ю., Хоменко Е.Б. Цифровизация и цифровая трансформация бизнеса: современные вызовы и тенденции / Л.А. Ватутина, Е.Ю. Злобина, Е.Б. Хоменко // Вестник Удмуртского университета. Серия «Экономика и право». – 2021. – №4. – С. 545 – 551.
[129] Reuters. White House plans 30-country meeting on cyber crime and ransomware – official. [Электронный ресурс]. Режим доступа: https://www.reuters.com/world/us/white–house–plans–30–country–meeting–cyber–crime–ransomware–official–2021–10–01/ (дата обращения: 11.02.2022).
[130] Российская Газета. Путин и Байден обсудили борьбу с киберпреступностью. [Электронный ресурс]. Режим доступа: https://rg.ru/2021/12/07/putin–i–bajden–obsudili–borbu–s–kiberprestupnostiu.html (дата обращения: 11.02.2022).

киберпреступности[131]. В данном смысле киберпреступность можно рассматривать как естественную адаптацию криминалитета под меняющиеся условия внешней среды. Во времена, когда государства рассматривают вопрос об отказе от наличных денег[132], а доля безналичных платежей постоянно бьет новые рекорды[133], переход в киберсреду вполне закономерен. Как показывают события последних лет, киберпреступность по сравнению с обычной преступностью может иметь гораздо большую эффективность и приводить к масштабным негативным последствиям для всего человечества.

Согласно глобальному отчету Hootsuite[134], к началу 2021 года аудитория интернет-пользователей составляла 59.5% от всего населения планеты, а активных пользователей социальных сетей – 53.6%[135]. Очевидно, что данная тенденция роста доли интернет-пользователей, их вовлеченности в глобальную цифровую систему и зависимости от нее сохранится. Сегодня глобализация носит не только экономический, политический или культурный характер, но и цифровой. Аудитория соцсетей и цифровых сервисов постоянно растет, во время локдаунов в цифровой реальности нашли досуг миллионы человек, в том числе и люди пожилого возраста[136]. В наиболее развитых странах, например, США, количество пользователей Интернета среди взрослого населения уже приближается к 100%: в 2021 году этот

---

[131] David Buil–Gil, Fernando Miró–Llinares, Asier Moneva, Steven Kemp & Nacho Díaz–Castaño (2021) Cybercrime and shifts in opportunities during COVID–19: a preliminary analysis in the UK, European Societies, 23:sup1, S47–S59.

[132] Российская Газета. Крона уходит в сеть? [Электронный ресурс]. Режим доступа: https://rg.ru/2020/12/13/v–shvecii–otkazhutsia–ot–nalichnyh–deneg.html (дата обращения: 20.12.2021).

[133] Ведомости. ЦБ заявил о росте доли безналичных платежей до 75%. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/finance/news/2021/10/15/891393–o–roste–doli–beznalichnih–platezhei–do–75 (дата обращения: 20.12.2021).

[134] Канадская компания–разработчик платформы для управления социальными сетями.

[135] Hootsuite. The Global State of Digital 2021. [Электронный ресурс]. Режим доступа: https://www.hootsuite.com/pages/digital–trends–2021#c–274407 (дата обращения: 16.12.2021).

[136] Bloomberg. The ‘New Normal’ for Many Older Adults Is on the Internet. [Электронный ресурс]. Режим доступа: https://www.bloomberg.com/news/features/2020–05–06/in–lockdown–seniors–are–becoming–more–tech–savvy (дата обращения: 19.12.2021).

показатель составил 93%, тогда как в 2000 году был на уровне только 52%[137]. В 2021 году онлайн на ежедневной основе были 85% взрослого населения США[138].

Большие перспективы имеют глобальные цифровые проекты, например, спутникового Интернета в местах, где он на текущий момент является дорогим или труднодоступным. Разработками такого рода систем в настоящий момент занимается целый ряд компаний: Starlink, Facebook[139], Viasat, HughesNet, OneWeb, Telesat и другие[140].

В последние годы постоянно растет и времяпровождение населения в цифровой реальности. Например, согласно исследованию[141] DoubleVerify[142], объем ежедневного потребления цифрового контента в 2020 году удвоился: с 3 часов 17 минут до 6 часов 59 минут. В условиях пандемии усилились тенденции к внедрению цифровых технологий в платежах и розничной торговле[143], росту безналичной оплаты[144], популярности удаленной работы[145] и онлайн-образования[146].

---

[137] Pew Research Center. Internet/Broadband Fact Sheet. [Электронный ресурс]. Режим доступа: https://www.pewresearch.org/internet/fact–sheet/internet–broadband/ (дата обращения: 17.12.2021).

[138] Pew Research Center. About three–in–ten U.S. adults say they are ‘almost constantly’ online. [Электронный ресурс]. Режим доступа:: https://www.pewresearch.org/fact–tank/2021/03/26/about–three–in–ten–u–s–adults–say–they–are–almost–constantly–online/ (дата обращения: 11.02.2022).

[139] Компания Meta Platforms Inc., владеющая Facebook и Instagram, внесена в реестр экстремистских организаций, ее деятельность в России по поддержанию указанных соцсетей признана экстремистской деятельностью.

[140] Lenta.ru. Илон Маск объявил о запуске Starlink. Зачем миллиардеру проект спутникового интернета и как он изменит мир? [Электронный ресурс]. Режим доступа: https://lenta.ru/brief/2021/09/23/starlink/ (дата обращения: 17.12.2021).

[141] DoubleVerify. Four Fundamental Shifts in Media & Advertising During 2020. [Электронный ресурс]. Режим доступа: https://doubleverify.com/four–fundamental–shifts–in–media–and–advertising–during–2020/ (дата обращения: 17.12.2021).

[142] Компания–разработчик платформы для измерения, обработки данных и анализа цифровых медиа.

[143] McKinsey & Company. US digital payments: Achieving the next phase of consumer engagement. [Электронный ресурс]. Режим доступа: https://www.mckinsey.com/industries/financial–services/our–insights/banking–matters/us–digital–payments–achieving–the–next–phase–of–consumer–engagement (дата обращения: 18.12.2021).

Таким образом, сегодня цифровые технологии стали одним из базовых инструментов социального взаимодействия между людьми, а сама киберсреда – не просто популярным пространством коммуникации, а неотъемлемой частью жизни современного человека. Цифровая реальность имеет фундаментальные отличия от реальности физической, в связи с чем можно ставить вопрос об исследовании нового типа социального взаимодействия между людьми – цифрового. К ее особенностям можно отнести[147]:

– возникновение новых зависимостей пользователей сети «Интернет» от особой категории субъектов социального взаимодействия: модераторов, администраторов, владельцев ресурсов, контролирующих государственных органов, а также манипуляторов вниманием людей;

– специфическую мотивацию, проявляющуюся в таких феноменах, как гипертрофированное стремление к самопрезентации (селфи и т.п.);

– представление искаженного виртуального образа для коммуникации;

– повышенная активность в обращении к различным ресурсам (интернет-серфинг), а также широкая распространенность мотиваторов и оценочных средств: анонимных комментариев, лайков, постов, репостов, символических поощрений и наград;

---

[144] Ведомости. Доля безналичных платежей в России достигла 70%. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/finance/news/2021/02/12/857761–dolya–beznalichnih–platezhei–v–rossii–dostigla–70 (дата обращения: 18.12.2021).

[145] Upwork. Economist Report: Future Workforce [Электронный ресурс]. Режим доступа: https://www.upwork.com/press/releases/economist–report–future–workforce (дата обращения: 18.12.2021).

[146] Radha R., K. Mahalakshmi, V. Sathish Kumar, A. R. Saravanakumar, ELearning during Lockdown of Covid–19 Pandemic: A Global Perspective, IJCA, vol. 13, no. 4, pp. 1088–1099, Jun. 2020.

[147] Кибакин М.В., Гришаева С.А. Актуальные проблемы рефлексии цифровой социальной реальности: переосмысление научных концепций / М.В. Кибакин, С.А. Гришаева / Цифровая социология. – 2019. – №2(1). – С. 4–9.

– наличие различного рода дезинформации: цифровых клонов, дипфейков, фейковых новостей;

– анонимность;

– постоянное взаимодействие с незнакомыми или малознакомыми людьми: сотрудники банков и технической поддержки, таксисты, курьеры;

– молниеносная скорость распространения информации и различного контента, в том числе и компьютерных вирусов, фейков и т.п.;

– возможности интернет-рекламы, продвижения в соцсетях и точечного воздействия на целевую аудиторию;

– локализация данных на серверах и в дата-центрах корпораций и государственных органов; постоянное изменение цифровой среды: появление новых сервисов, непрерывное «оцифровывание» привычных ежедневных активностей человека, релизы и обновления программного обеспечения; рост популярности суперприложений, цифровых экосистем и метавселенных.

Таким образом, в контексте нашего исследования цифровую реальность можно охарактеризовать как непрерывно меняющуюся и усложняющуюся среду с высочайшей скоростью распространения информации и возможностями сохранения анонимности или использования цифровых двойников.

Те особенности, которые приобретает социальное взаимодействие в цифровой реальности и которое можно рассматривать как цифровое социальное взаимодействие, – еще один важный аспект в рамках нашего исследования. В эпоху широкого распространения цифровых каналов связи и доступности Интернета общение и взаимодействие в сети стало популярно и востребовано у населения различных возрастных групп. Соцсети, как, например, ВКонтакте, а также сервисы для звонков, как, например, ZOOM, – одни из немногих бенефициаров пандемии COVID-19. В высокой степени снижая трансакционные издержки физического общения, а в условиях пандемии уменьшая вероятность заражения коронавирусной инфекцией,

цифровое общение стало крайне востребовано и популярно в последние годы, о чем свидетельствуют данные отчетов, представленных выше. Однако инциденты последних лет, случающиеся со все большей регулярностью, показывают, что цифровая реальность все чаще становится опасной средой для рядового пользователя. Путешествия по Интернету и общение в мессенджерах сегодня все чаще можно сравнить с ходьбой по минному полю, где в каждую секунду человека поджидают разного рода опасности: фишинговые страницы, файлы с вирусами, звонки от мошенников. Возможности современных технологий сегодня крайне широки, и подделки голоса или изображений, которые еще пару десятков лет назад казались невозможными, сегодня уже вполне реальны и активно используются для введения в заблуждение или откровенного мошенничества. Например, в последнее время стали популярны созданные с помощью нейросетей «видеообращения» от предпринимателей с призывом вкладываться в мошеннические проекты. Качество такого рода подделок становится все более высоким, что уже сейчас поднимает вопрос о том, что сегодня уже невозможно в полной мере доверять своим органам чувств, а видеоконтент требует тщательной проверки с помощью специального программного обеспечения. В таком противостоянии человек все чаще оказывается за пределами поля боя, зачастую ему остается только принять финальное решение: например, на основании анализа антивируса продолжить посещение сайта, скачивать ли подозрительный файл. Несмотря на обилие различного рода продуктов по защите пользователей от вредоносного программного обеспечения, количество киберпреступлений постоянно растет. Объяснить это можно тем, что человек сегодня является самым слабым звеном в информационной системе. Каким бы надежным не был защитный периметр, именно пользователь принимает решение о том, что допускать внутрь системы и выводить наружу и как использовать полученную информацию. В отличие от антивирусного программного

обеспечения, которое оперативно обновляется для защиты от все новых появляющихся угроз, человеческие мышление и восприятие можно охарактеризовать как более инертные структуры, которые подвержены огромному количеству ошибок и искажений. Эксплуатация недостатков человеческой психики – одна из основ мошенничества во все времена, получившая небывалый размах в цифровую эпоху. Особую популярность приобрели методы социальной инженерии, построенные на использовании систематических отклонений в мышлении, поведении и восприятии людьми окружающей действительности – когнитивных искажений. И масштабы такого рода уловок безграничны: если еще несколько десятилетий назад зона воздействия мошенника ограничивалась лишь относительно малой территорией и небольшим кругом людей, то сегодня информационные технологии открывают доступ практически к любому человеку с устройством связи. А такое свойство интернет-контента, как его виральность, то есть вирусность и желание поделиться им с другими, обеспечивает быстрое распространение мошеннической продукции в соцсетях и различных цифровых платформах. Таким образом, можно констатировать, что эксплуатация недостатков человеческого восприятия, поведения и мышления – одна из основ киберпреступности сегодня. Есть ли решение у этой проблемы?

Анализ текущего состояния киберпреступности показал, что проблема носит системный и масштабный характер. Киберпреступность стала неотъемлемым спутником цифровизации. Цифровизация сегодня – не только благо в виде, например, повышения эффективности процессов, качества жизни или снижения издержек производства, но и большой риск. Причем риск самого разного спектра: краткосрочный и долгосрочный; глобальный и локальный; на бытовом, корпоративном, государственном и межгосударственном уровне; восполнимый и невосполнимый. Риск для всех сфер общественной жизни, поскольку все они уже в той или иной степени

являются оцифрованными. Приведем несколько примеров из каждой сферы для понимания масштаба и глубины происходящих процессов. Для экономической сферы: роботизация и автоматизация производства, хранения и логистики; электронная коммерция, онлайн-банкинг. Политическая сфера: электронное правительство, онлайн-петиции, электронное голосование. Социальная сфера: социальные сети и мессенджеры, справочно-информационные порталы, виртуальные представительства. Духовная: онлайн-образование, искусство в онлайн, досуг в интернет-среде. Важно подчеркнуть, что подавляющее большинство этих процессов цифровизации являются необратимыми: их невозможно отменить или перейти на предыдущую ступень, поскольку это может повлечь как снижение уровня жизни и комфорта, так и деградацию всей сложившейся глобальной системы воспроизводства общественных отношений.

В рамках данного анализа необходимо отметить важный тренд**,** который напрямую влияет на характер распространения киберпреступности сегодня и глубину проблемы. Этот тренд заключается во все более тесной взаимосвязи всех сфер общественной жизни в процессе цифровизации, их унификации и стандартизации. Если раньше границы этих сфер были четко очерчены и разделены, то сейчас они все более тесно переплетены и включены в огромное количество связей и процессов друг с другом. Для наглядности проиллюстрируем это примером. Представим распорядок дня обычного гражданина еще 30 лет назад. Он собирается и едет на работу на завод, после работы у него занятия в университете. Он совершает покупки в магазине за наличные денежные средства. На выходные посещает театр и выставки с друзьями или смотрит телевизор. За справками обращается в госучреждения, а в день голосования ходит на выборы с паспортом и голосует на бумажном бланке. Сегодня жизнь этого гражданина кардинально изменилась. Телефон – его единый проводник ко всем благам и инструмент закрытия всех или практически всех потребностей. Наш гражданин работает,

учится, развлекается и удовлетворяет свои потребности в общении в одном месте – своей квартире, с использованием Интернета и электронного устройства. Цифровые технологии позволили гражданину серьезно сократить издержки, связанные с перемещением до работы или учебы и обратно, связанные с ожиданием в очередях, готовкой, поиском информации или исполнителей по бытовым вопросам. Также уже не требуется расплачиваться наличными в кассе, поскольку для этого у нашего гражданина есть единый электронный банковский счет. С одного устройства наш гражданин и учится, и работает, проводит досуг, взаимодействует с государственными органами и даже голосует на выборах. Причем делать все это можно, используя единую учетную запись и пароль, а сами эти сервисы могут быть разработаны по единой технологии с одинаковым уровнем безопасности, а порой одним и тем же самым поставщиком программного обеспечения. Какого уровня последствия могут наступить, если преступники смогут получить доступ, например, к устройству нашего гражданина или к аккаунту, который подтверждает личность нашего гражданина в цифровой среде? Эти последствия могут быть грандиозны по масштабам для всех сфер жизни нашего гражданина, а также распространяться на его окружение и те сервисы, к которым у него есть доступ. Например, доступ злоумышленников к конфиденциальной информации жертвы может повлечь за собой проникновение в корпоративный контур организации, где человек работает; к банковским счетам не только жертвы, но и всей его семьи; открывает возможности для преступных действий в отношении знакомых жертвы, особенно с использованием инструментов социальной инженерии, или незаконных действий в отношении государственных органов власти. То есть привести к проблемам на самых разных уровнях: индивидуальном, семейном, а в особых случаях на организационном, государственном и даже межгосударственном. Описанный выше пример иллюстрирует важную особенность сложившегося устройства глобальной цифровой системы: ее

проникновение во все сферы и на все уровни общественной жизни, от индивидуального до глобального. В таких условиях границы возможностей серьезно расширяются, а количество комбинаций и вариантов совершения различных операций возрастает. Например, варианты совершения денежных переводов, онлайн–покупок или получения услуги сейчас насчитывают десятки и сотни самых различных вариаций: от выбора онлайн-сервиса и заканчивая способом оплаты. Причем это касается не только горизонтальных, но и вертикальных связей, чему, например, способствует внедрение и развитие концепции электронного правительства. В таких системах информация оперативно передается на самые разные уровни системы: от частного до публичного, от государственного до корпоративного. Узлы информационной системы, имея установленные между собой каналы связи, передают, хранят и обрабатывают информацию самого разного свойства и ценности: от бытовых переписок граждан до денежных переводов в миллиарды долларов, от научных и военных разработок до секретных документов о принятии важных государственных решений. Цифровые системы и информация, циркулирующая в них, напрямую влияют на поддержание и функционирование глобального миропорядка, процессов и институтов. Инциденты глобального масштаба и вирусные атаки последних лет наглядно продемонстрировали, к каким последствиям могут привести сбои в этой системе на нескольких уровнях. Например, ущерб от атаки компьютерного вируса WannaCry в 2017 году проявился на государственном, организационном и индивидуальном уровне и затронул самые разные социальные сферы: от медицины и банковской сферы до производства и логистики. Такое масштабное и стремительное распространение вредоносной программы стало возможным благодаря тесной взаимосвязи узлов глобальной информационной системы. Безусловно, есть особо защищенные, обособленные узлы системы, будь то спецсвязь или

финансовый сектор, но даже их нельзя охарактеризовать как абсолютно защищенные и неуязвимые к кибератакам.

С чем можно сравнить глобальную цифровую систему? Можно провести аналогию со вселенной, которая включает в себя миллиарды галактик, звезд и планет, а информация передается посредством света. Причем эта галактика находится в постоянном движении: ее части непрерывно видоизменяются, появляются новые элементы и исчезают старые. Вместо звезд и галактик в нашей цифровой вселенной мы имеем дело с информационными системами и устройствами, начиная от глобальных и хорошо защищенных банковских экосистем и заканчивая персональными компьютерами и телефонными устройствами обычных пользователей. Такая система дуальна: она олицетворяет структуру и хаос одновременно. С одной стороны, цифровая система имеет структуру: определенные правила и нормы хранения, обработки и передачи информации, уровни доступа к системе и степени ее защищенности, требования к безопасности программного обеспечения. С другой стороны, распространение информации в цифровых системах порой принимает хаотичный, неконтролируемый характер. И здесь речь касается не только вредоносных вирусов, которые способны за считанные минуты распространяться по устройствам и цифровым системам в планетарном масштабе, но и довольно популярные сегодня мемы, фейковые новости или дипфейки. Такого рода информация, особенно резонансная и отвечающая текущей новостной повестке, хорошо чувствует себя в информационном поле и способна довольно стремительно распространяться среди населения отдельного региона или всей планеты. Резонансная информация, подобно вирусу с очень высокой степенью заразности, попадает в благодатную среду для распространения. Но что включает в себя эта среда? С одной стороны, это конечно же информационные технологии и устройства как средство коммуникации между индивидами, различными социальными группами, организациями, государственными органами. Но с другой

стороны, все эти технологии и цифровые системы – это всего лишь инструмент, среда, в которой происходит коммуникация и протекают различной степени важности и сложности процессы. И здесь мы подходим к рассмотрению важной в рамках данного анализа части системы – социальной.

Действительно, сама по себе цифровая система носит нейтральный характер, она выполняет лишь ту функцию или набор действий, который в нее заложил разработчик. Если технология способствует, например, повышению благосостояния населения, оптимизации производства или улучшению жизни без негативных последствий для других, то такие технологии можно назвать полезными. Как раз за счет их внедрения и использования совершаются переходы на качественно новые уровни общественного развития. Оборотная сторона медали – это технологии и системы, разрабатываемые и используемые в преступных целях. К ним можно отнести как исключительно вредные вымогатели, сетевые черви или программы для спама, так и технологии двойного назначения. Например, наряду с Интернетом существует Даркнет, а виртуальные частные сети (VPN) или криптовалюты могут использоваться для незаконных деяний. Подобно оружию, многие информационные технологии могут использоваться в двойном назначении: для совершения как законных, так и противозаконных деяний. С другой стороны, есть разработчики программного обеспечения, и это тоже отдельная социальная группа, где есть свои стандарты проектирования, производства и внедрения готовых решений. С третьей стороны есть потребители, у которых есть свои ожидания и потребности, которые они хотят удовлетворить за счет использования цифровых продуктов. Если ранее рассматривались сущностные характеристики технологической системы как совокупности связанных между собой устройств и цифровых алгоритмов, то теперь пришло

время рассмотреть не менее важную часть системы, которую можно охарактеризовать как социальную.

Что включает в себя социальная составляющая? Это все то, что выходит за рамки машинных алгоритмов и устройств. Сюда можно отнести людей как пользователей устройств и различных информационных сервисов. Это широкого спектра отношения и культурный контекст, который возникает между пользователями в цифровой среде: идентификация, восприятие, нормы, ожидания, ответственность, намерения, навыки, знания, опыт, модели поведения и так далее. По сути, все те отношения, которые существовали между людьми до появления информационных технологий и многие из которых в той или иной степени «оцифрованы» сегодня. Это все те нормы и подходы к проектированию и разработке программного обеспечения, которые используются экспертным ИТ-сообществом – разработчиками технологических систем. Это законы, акты, рекомендации и инструкции, регламентирующие поведение в цифровой среде. Это сфера образования, которая включает в себя нормы, ценности и подходы как в вопросах подготовки ИТ-специалистов, так и широких групп населения в вопросах грамотного и безопасного поведения в цифровой среде. Причем сегодня данная область находится в ведении не только государства, но и негосударственного сектора: рост коммерческого образовательного контента в данной области в России очень стремительный. Естественно, уровень образования и выпускаемых специалистов прямо влияет на степень безопасности и надежности разрабатываемых ими цифровых решений. Помимо этого, к социальной составляющей можно отнести те намерения, нормы и принципы, способы коммуникации, преступные схемы и правила конспирации, которые используются киберпреступными сообществами. Киберпреступные сообщества – это отдельный и довольно важный объект исследования со своими нормами и моделями поведения, традициями, правилами конспирации в цифровом и реальном мире. Одним словом, к

социальной составляющей можно отнести огромное количество отношений, которые возникают между людьми в цифровом пространстве и по поводу него. Все вместе в совокупности это и есть та социальная составляющая нашей социо-цифровой системы: отношения между людьми и социальными группами в цифровой среде.

Почему исследование возможностей и ограничений социальной подсистемы имеет важное значение в рамках анализа феномена киберпреступности? Рассмотрим этот вопрос далее.

Каждая система имеет свои возможности и ограничения, слабые места и уязвимости. Это относится в том числе и к цифровым системам, где нередко эксплуатация бага или бэкдора в преступных целях ведет к масштабным негативным последствиям. Киберпреступность сегодня – это прежде всего эксплуатация социальных, а не технических уязвимостей системы. Эксплуатация социальных уязвимостей – один из наиболее эффективных инструментов из арсенала киберпреступников, особенно популярный в последнее несколько лет. Например, это рост мошеннических действий с использованием инструментов социальной инженерии, то есть манипулятивных действий в отношении людей. Популярность таких схем обмана постоянно растет, потому что со все более высоким уровнем защищенности цифровых систем самым слабым звеном становится именно человек. Именно за человеком остается принятие финального решения, поскольку он является создателем любой цифровой системы или алгоритма, его администратором и центром принятия решений по ключевым вопросам. Современные системы безопасности и противодействия киберпреступности умеют успешно обнаруживать уязвимости и преступную активность. Они подобно массивным стенам зàмка, способны успешно держать оборону от различного рода киберугроз извне. Однако чтобы захватить зàмок, достаточно неосторожного поведения одного человека, который откроет двери и впустит неприятеля. И таким слабым звеном в хорошо защищенной

информационной системе сегодня все чаще становится человек. Действительно, зачем пытаться взломать прочную броню кибербезопасности банка, разработанную сильнейшими профессионалами в своей области и протестированную во многих реальных и гипотетических сценариях, когда можно использовать всего лишь одного сотрудника, имеющего доступ к секретным данным? Статистика последних лет показывает, что именно к такому способу и прибегают преступники, если речь касается особо защищенных систем, в частности, банковских. Волновой рост киберпреступлений с использованием человеческого фактора в последние годы – это серьезный вызов не только для специалистов в области информационной безопасности, но и для всего человечества в целом. Сегодня эта проблема касается каждого: любой человек является потенциальной жертвой. Масштаб возможных преступных схем поражает. Причем чем более жизнь человека связана с цифровым миром, тем больше вероятность наткнуться на противоправные действия в свой адрес: от пресловутых и очень популярных звонков от «сотрудников банков» до более продвинутых технологий голосовых и визуальных дипфейков. Это делает такого киберпреступного «троянского коня» все более незаметным в потоке повседневной информации с точки зрения человеческого восприятия. И вот почему.

Особенность большинства киберпреступных продуктов в том, что он никак не выделяется на фоне других цифровых артефактов, которыми оперирует человек в своей обычной жизни. Переписки с друзьями в соцсети, скачивание файлов с фильмами и музыкой, онлайн-покупки и прочие операции – обычная рутина современного продвинутого человека. С течением времени даже в самых экстремальных условиях бдительность человека притупляется, а боязнь опасности снижается. Но почему в целом человеку свойственны более неосторожное и вольное поведение в сети, нежели в реальном мире?

Важная особенность цифровой реальности в контексте исследования киберпреступности заключается в том, что человек в ней не чувствует физической опасности здоровью или жизни для себя или для своих родственников. Интернет – это поток информации, которая циркулирует между большим количеством участников. Общение в сети, игры, просмотр сериалов в онлайн-кинотеатре является более безопасным по сравнению с альтернативами в реальном мире: поход в тот же кинотеатр может закончиться травмой, нападением на улице, конфликтом с другими людьми, ДТП и даже смертью. Интернет выступает в роли точки доступа к большому количеству благ современного общества, который при этом значительно снижает издержки для конечного потребителя: временные, финансовые, психоэмоциональные. Такой эффект можно особенно ярко наблюдать у людей с низким уровнем социализации, для которых Интернет становится главным проводником в окружающий мир. При этом неминуемо образуется замкнутый круг: чем больше человек погружается в виртуальную реальность, тем больше теряет контакт с миром реальным, а социальные навыки деградируют. Как итог, Интернет выступает иллюзией безопасности и отстраненности по сравнению с миром реальным, происходит рутинизация действий, совершаемых в цифровой среде.

Для человека еще недавняя ноу-хау технология оказывает влияние на привычную жизнь, она становится массовой и обыденной: электронная коммерция, онлайн-образование, удаленная работа и многое другое. Событие массового перехода на удаленный формат работы во время пандемии показало, как быстро социум адаптируется к новым реалиям и новым цифровым технологиям в своей жизни. Общий тренд на более широкое внедрение дистанционной формы занятости в России, безусловно, сохранится: этот процесс носит глобальный характер и имеет глубинные объективные основания в цифровой трансформации, роботизации производственных процессов, которые неуклонно развиваются в сторону

безлюдных технологий, «отвязывая» человека от офиса, производственного цеха, торговой точки и т.д.[148]

Происходит рутинизация поведения человека в цифровой среде, снижение внимания, осмотрительности. И эти особенности поведения в цифровом мире активно эксплуатируются кибермошенниками. Их преступные схемы часто мимикруют под привычные действия, которые продвинутый пользователь совершает ежедневно. И в этом главная опасность киберпреступности – она вездесуща, и может ударить даже самых продвинутых пользователей в привычное место. Подстеречь там, где человек этого не ожидает, и застать человека врасплох. Важно помнить, что каждый выход в сеть – это не легкая беззаботная прогулка, а словно поездка на автомобиле по оживленной магистрали, где необходимо непрерывно отслеживать обстановку на дороге со всех сторон. Помимо этого, сегодня нередко эксплуатируются другие особенности, присущие человеческому мышлению, поведению и восприятию. Людям, даже самым образованным и осознанным, свойственно ошибаться и заблуждаться, проявлять неконтролируемые эмоции, совершать неосознанные или нелогичные поступки. Свойственно не брать на себя ответственность за совершаемые действия, а перекладывать ее на кого-то другого. Свойственно потреблять контент, пользоваться устройствами или сервисами, но при этом не задумываться о рисках, которые они влекут прежде всего для самого человека. На социальном масштабе такая модель поведения вытекает в риски, которые реализуются на практике в виде повышения активности киберпреступной деятельности. Киберпреступность идет по пути наименьшего сопротивления и бьет в самое слабое звено системы.

[148] 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 / Л.Г. Судас, А.А. Оносов, А.Ж. Бесланеев, Ю.В. Манкевич, М.Б. Пивоварова, В.А. Правосудова, Д.С. Рассадина, П.С. Швыряев // Государственное управление. Электронный вестник. – 2021. – № 86. – С. 284–306.

Но предпосылки и благодатная почва для повышения криминогенной обстановки формируются не за один день. Это длительный процесс, который может занимать годы или даже десятки лет, но который в конечном итоге формирует такое состояние системы, в которой киберпреступная деятельность принимает серьезные масштабы и даже ставит под угрозу само функционирование этой системы. Эксплуатация уязвимости может иметь характер взрыва, быстро распространяющегося по всей системе и вводящего ее в состоянию шока и дезорганизации. Яркий пример – атака вируса WannaCry в мае 2017 года. Или же более плавный, но непрерывный процесс, принимающий характер долгосрочного тренда, роста мошеннической активности, например, с использованием методов социальной инженерии в России. Но оба эти события имеют некоторые схожие черты. Первое – это огромный масштаб, который затрагивает все сферы общественной жизни на всех уровнях: от нарушения нормальной жизнедеятельности человека до сбоев в системе государственного управления. В особых случаях можно говорить о потере на некоторое время управляемости всей системой или отдельными ее узлами. Второе – система пришла к такому состоянию не за один день. Когда события о кибератаках наводняют новостную повестку, может сложиться ложное впечатление, что обстоятельства и условия для совершения таких громких преступлений сформировались если не молниеносно, то в относительно недавнее время. Однако зачастую это совершенно не так. Процесс формирования системы, к которой она пришла в момент атаки на нее, может занимать годы и даже десятки лет, а количество различных участников может насчитывать десятки, сотни и даже тысячи. Это череда неправильных решений, просчетов и упущений, которые были сделаны людьми и которые в итоге и сформировали уязвимое состояние системы. Почему так происходит? Для этого более подробно рассмотрим, под воздействием каких факторов и в каком контексте разрабатываются цифровые продукты.

Цифровые системы и устройства, будь то телефоны, онлайн-сервисы, сайты, операционные системы, программы и приложения – это вещи, которые не создаются в вакууме. Подобно предметам материального мира, они создаются конкретными людьми для других людей с целью выполнения определенных задач в конкретных обстоятельствах своего времени. Эти обстоятельства насчитывают огромное количество факторов, которые в конечном итоге формируют продукт, который представляется для конечного потребителя. Обзорно перечислим эти факторы на разных уровнях. Государственный: требования к стандартам информационной безопасности цифровых систем; санкции за нарушения предписаний и произошедшие инциденты; аудит и контроль со стороны государства; регулирование образовательного процесса с точки зрения подготовки будущих ИТ-специалистов и просветительской деятельности потребителей цифрового контента; борьба с преступностью в цифровой среде и деятельность по ее предупреждению в будущем. Общественный**:** обратная связь со стороны общественности как потребителя услуг, репутационные риски и воздействие со стороны гражданского общества, журналистские расследования. Профессиональный: принятые в профессиональной сфере подходы к проектированию, разработке и внедрению программного обеспечения, дискуссии и модные тренды со стороны сообщества. Организационный: принятые и поддерживаемые в данной организации подходы и стандарты к разработке программного обеспечения. Личностный: личностные и профессиональные особенности конкретного человека, которые влияют на разрабатываемый им продукт. Как итог, цифровой продукт, подобно произведениям искусства, отражает особенности той культурной и социальной эпохи, в которой он был произведен. Он становится продуктом своего времени и вбирает в себя результат работы людей, который базировался на принятии конкретных решений под воздействием большого количества факторов: опыта сотрудников как разработчиков системы,

принятые стандарты к разработке и информационной безопасности, ответственность со стороны государственных органов, профессионального сообщества и общественности. Любая цифровая система – это продукт культурный в наиболее общем смысле этого слова, как результат взаимодействия людей в определенном культурном контексте. С другой стороны, это продукт социально ориентированный: он создается для выполнения определенных задач и удовлетворения потребностей, явных и неявных. Цифровая система, произведенная людьми, начинает оказывать на них определенное влияние. Оказывается влияние и на процессы, которые раньше функционировали по иным правилам и в других обстоятельствах физического мира. Цифровые системы и технологии внедряются в привычный уклад жизни, качественно меняя ее, и меняя людей, их поведение и восприятие окружающей действительности и даже провоцируя различные психические расстройства. Как итог, сегодня неотъемлемой частью жизни становятся синдромы упущенной выгоды, технострессы, снижение концентрации внимания или депрессивные эпизоды на фоне чрезмерного или нездорового потребления цифрового контента. В наиболее общем смысле мы можем говорить о взаимном влиянии технологий и человека друг на друга: человек создает технологию с определенной целью и в определенном условиях, внедряет ее в жизнь, и далее технология начинает влиять на человека и менять его привычный уклад.

Данный тезис отражает одну из ключевых идей исследований науки и технологий (STS, Science and Technology Studies). Джон Ло, один из представителей данного направления, отмечал: «Базовая интуиция проста: научное знание и технологии развиваются не в вакууме. Скорее, они участвуют в социальном мире, формируются им и одновременно формируют его»[149]. Это важное утверждение, которое уберегает нас от скатывания к

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

идеям технократизма: это опасно не только в рамках исследования процесса цифровизации в целом, но и проблем киберпреступности в частности. Сегодня мы можем часто наблюдать, как предпринимаются попытки решить проблему киберпреступности с помощью технократического подхода: ответить на социальную проблему техническим решением. Практика показывает всю узость и ограниченность такого подхода, когда из зоны внимания выпадает само понимание феномена киберпреступности как социальной проблемы: незаконной деятельности, совершаемой людьми с использованием цифровых технологий и направленной на других людей. Киберпреступность – это прежде всего социальная проблема, которая возникает из социума и направлена в него. Киберпреступность и ее составляющие, которые включают людей, связи между ними, преступные схемы, инструменты и технологии – это все продукт социального мира. Конечная цель преступников – оказать воздействие на социальный мир и добиться своих незаконных целей. Результат совершения такого действия – изменение социального уклада, характера протекания социальных отношений, начиная от вмешательства в жизнь отдельного индивида и заканчивая глобальными сбоями планетарного масштаба.

Внутри направления STS можно выделить такое ответвление, как социальное конструирование технологий, или SCOT (social construction of technology). К ведущим представителям SCOT относят Вибе Бейкера и Тревора Пинча. Ключевая идея направления SCOT заключается в понимании технологических артефактов как социальных конструкций[150]. В своих работах исследователи рассматривают развитие технологий как непрерывный процесс обсуждения и поиска консенсусного варианта среди различных социальных групп. С позиций SCOT, может существовать множество вариантов реализации той или иной технологии, она может

[150] 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.

разрабатываться конкурирующими между собой научно–исследовательскими институтами или компаниями. До момента внедрения технология может проходить серию испытаний, доработок и улучшений, которые базируются на обратной связи различных социальных групп и акторов. Тот вариант, в котором технология в конечном итоге попадает в массовое использования, – это консенсус различных социальных групп и интересов. Несмотря на то, что в дальнейшем SCOT критиковались за игнорирование последствий выбора той или иной технологии[151], методология данного направления полезна для исследования как развития технологий в целом, так и киберпреступности в частности. К ключевой заслуге SCOT можно отнести исследование социальных переменных, которые оказывают влияние на конечные характеристики технологии и масштаб ее использования. Очевидно, что любая технология – это продукт взаимодействия большого количества людей, объединенных в социальные группы, которые имеют свои взгляды и интересы по поводу разрабатываемого продукта. Для анализа феномена киберпреступности идеи SCOT дают дальнейшую перспективу исследования того, в каких обстоятельствах и условиях развиваются те или иные социо-цифровые системы с позиции обеспечения информационной безопасности, надежности и отказоустойчивости. Ведь к эксплуатации незамеченной при разработке уязвимости или умышленно оставленного бэкдора привели конкретные человеческие действия, которые совершались в определенных обстоятельствах, которые включают в себя огромное количество факторов. Исследование этих факторов поможет нам сформировать более системный, комплексный взгляд на развитие и использования технологий, а также тех рисков и проблем, которые неразрывно с ними связаны и используются в преступных целях.

[151] Winner L. «Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology» *Science, Technology, & Human Values*, vol. 18, no. 3, 1993, pp. 362–378.

Существенным недостатком подхода SCOT, за который направление обоснованно критиковалось другими исследователями, является социальный редукционизм[152]. Критика идей SCOT подтолкнула к дальнейшему развитию исследований технологий, появлению концепции со-конструирования общества и технологий Пола Эдвардса. Концепция П. Эдвардса направлена на преодоление ограничений исследований предшественников. Ключевая идея концепции П. Эдвардса заключается в том, что «инфраструктуры одновременно формируют и формируются, то есть находятся в условиях со-конструирования»[153]. Одно из ключевых понятий концепции Эдвардса – инфраструктуры, которые не сводятся просто к оборудованию: в такой трактовке видится большое упущение. Пол Эдвардс рассматривает инфраструктуры как социотехнические системы, которые включают в себя не только физическое оборудование, но и большое количество артефактов, которые участвуют в процессе создания инфраструктур: организации, знания, коммуникацию, одобрение и доверие, нормы, знаки и символы, ценностные образцы. Социум создает различные инфраструктуры для поддержания стабильности, удовлетворения потребностей и защиты от агрессивной окружающей среды. Однако любая инфраструктура имеет свои ограничения, контроль и ограниченный список возможностей использования. Например, дорожные сети обеспечивают возможность комфортного перемещения на общественном или личном транспорте на определенных условиях: транспортное средство должно быть в приемлемом техническом состоянии, двигаться можно по определенным правилам и останавливаться по первому требованию дорожных служб. Цифровые продукты предлагают определенный интерфейс для взаимодействия по заранее определенным

[152] Судас Л.Г. Управленческие императивы Индустрии 4.0 / Л.Г. Судас, М.А. Юдина. – М.: Издательство Московского университета, 2021. – 152 с.
[153] 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.

пользовательским «маршрутам» при принятии соглашений. В любой инфраструктурной среде неминуемо есть набор ограничений и условий, которым индивид вынужден подчиняться, и все это является фундаментальной составляющей мировоззрения модернизма. Таким образом, инфраструктуры, формируемые социумом в определенную историческую эпоху, начинают оказывать влияние на сам социум на разных уровнях. Причем данный подход применим к исследованию развития не только инфраструктур, но и киберпреступности в частности, поскольку киберпреступность неразрывно связана с закономерностями развития цифровых инфраструктур и особенностями их взаимодействия с социумом. Не менее полезным в рамках данного исследования является метод рассмотрения инфраструктур одновременно на нескольких масштабах силы, времени и социальной организации. Выделяется три уровня масштаба: микро-масштаб, мезо-масштаб и макро-масштаб. Данный методологический подход позволяет нам проследить закономерности развития инфраструктур на различных масштабах и их влияние на частную и социальную жизнь, в том числе и в области исследования киберпреступности и информационной безопасности.

Еще одним важным направлением исследований в рамках проблематики развития технологий является акторно-сетевая теория. Бруно Латур, один из ведущих представителей АСТ, предложил вместо привычных понятий «актор» или «субъект» использовать термин «актант» , который «позволяет распространить область социального исследования на всех взаимодействующих, вступающих в ассоциации и обменивающихся своими свойствами существ»[154]. Эти «существа» – понятие более широкое, системное, оно выходит за пределы привычного понимания индивидов и социальных групп как объектов взаимодействия. Под актантом можно

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

понимать любой объект, который совершает действие или в отношении которого совершается какое-либо действие. И с этой позиции нам открываются перспективы перехода на новый уровень социологического анализа. Распространение цифровых технологий и устройств, появление автопилотов и использование искусственного интеллекта для выполнения повседневных задач расширяют ранее сложившиеся представления о субъектности. Коренной перелом заключается в передаче машинному алгоритму прав на совершения рутинных действий в самых разных областях человеческой деятельности: от установки будильника на смартфоне до трансграничных банковских переводов. Сегодня технологии – это не просто второстепенный фон социального взаимодействия, а полноценный его участник, который в одних случаях обеспечивает возможность этого взаимодействия, а в другом – устанавливает нормы и правила этого взаимодействия. Машинные алгоритмы принимают решение, будет ли заблокирован тот или иной пользователь соцсети за некорректное поведение. Или наступит ли блокировка пользователя за совершение подозрительных операций. С развитием антивирусной и антимошеннической инфраструктуры этот вопрос становится актуальным и для проблемы кибербезопасности. В вопросах киберпреступности актантом выступает не только специалист по информационной безопасности, но и защитные алгоритмы, которые вычисляют подозрительную активность и блокируют источник угрозы. И в этой связи возникает ряд важных вопросов, которые требуют ответа и на которых в том числе базируется подход к выстраиванию информационной безопасности на различных социальных уровнях. Каковы возможности и ограничения современных систем безопасности? Какова должна быть роль человека в этой системе? На какие моменты должно быть обращено внимание при совершенствовании существующих и разработке новых систем безопасности? Как минимизировать роль человеческого фактора в системах безопасности?

Концепция социальности объектов получила свое развитие в трудах австрийского социолога Карен Кнорр-Цетины, для которой социальность представляется объект-центричной, включающей и материальные объекты (но не ограничивающейся ими)[155]. Процесс по все большему участию объектов в социальном взаимодействии социолог определяет как «объектуализацию», а «новую социальность» – как «социальность с объектами». Такие объекты, под которыми можно понимать в том числе информационные технологии и цифровые устройства, становятся или посредниками в социальном взаимодействии между людьми, или полноценными участниками этого взаимодействия. И действительно, с развитием эпохи информационных технологий существует устойчивый тренд на передачу ответственности от человека к технологиям и машинам. В рутинных делах, не требующих высокой квалификации, человек заменяется автоматикой, а социальное взаимодействие переходит в цифровой формат и приобретает свои специфические черты. При совершении рутинных социальных действий человек все более зависит от программы и алгоритма, заложенного в него. От этого зависит результативность различных действий при совершении широкого спектра операций: от авторизации до банковских переводов. То, какие темпы приобретает цифровизация в последние несколько лет, говорит о том, что масштаб и глубина процесса «объектуализации» стабильно растет. Риски такого процесса очевидны: от локальных и глобальных сбоев до расцвета киберпреступности в масштабах всей планеты.

Рассмотренные выше концепции дают нам дальнейшую перспективу для более системного социологического исследования феномена киберпреступности: через понимание того, в каких условиях киберпреступность зарождается и прогрессирует, к выработке системного,

[155] Кнорр-Цетина К. Социальность и объекты. Социальные отношения в постсоциальных обществах знания // Социология вещей: Сб. статей / Под ред. В. Вахштайна. М.: ИД «Территория будущего». – 2006. – 392 с.

стратегического подхода по эффективной борьбе с ней, в основе которого – действия упреждающего характера. Очевидно, что полностью решить проблему киберпреступности невозможно, это неотъемлемый спутник цифровизации, однако снизить ее масштабы и уровень воздействия на социум через выработку и реализацию альтернативного подхода к технологическому развитию – задача сложная, но посильная.

В последние годы в России особенно популярными стали мошеннические действия с использованием методов социальной инженерии. Наиболее распространенной формой стали звонки гражданам под видом сотрудников банков или государственных органов. Ответом со стороны банковского сектора становится совершенствование технических систем и систем антифрода[156]. Это относительно быстрый и эффективный в моменте ответ на вызовы со стороны преступного мира, который, однако, не устраняет корневую причину высокой жизнестойкости такого незаконного метода. А причина лежит прежде всего не в технической плоскости, а в социальной. Первый человек совершает действие, которое делает его преступником, второй – которое делает его жертвой. Техническая система в виде Интернета или телефонной сети здесь выступает передаточным звеном, которое может сигнализировать о подозрительной активности, как, например, системы антифрода, но не может принять окончательное решение за человека. Здесь стоит подчеркнуть, что социальная инженерия успешно использовалась для совершения мошеннических действий еще задолго до появления Интернета и телефонной связи, но обрела повсеместную популярность только относительно недавно за счет относительно легкой возможности доступа к потенциальным жертвам, который обеспечивают цифровые технологии и средства связи. И это хороший пример того, как полезные свойства технологий могут использоваться во вред, при этом они

[156] ТАСС. Банки рассказали, что жертвой мошенников можно стать независимо от личных характеристик. [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/13625465 (дата обращения: 28.01.2023).

не могут гарантированно уберечь человека от мошеннических действий в отношении него. Практика показывает, что если человеку свойственно совершать необдуманные, нерациональные действия, то риск стать жертвой кибермошенников у такого человека велик. И это не зависит от уровня системы безопасности антивирусной системы его телефона или антифрода банков, где он обслуживается, поскольку корень проблемы в данном случае не в них, а в самом человеке, его восприятии мира, опыте, уровне цифровой грамотности и образования, доверия и большом количестве других факторов. Эти факторы формируются годами и в итоге влияют на то, какие решения принимает человек и в целом формируют его уникальную призму восприятия мира. В этом процессе участвует множество агентов: семья, школа, сверстники и друзья, СМИ, места работы и досуга, государственная политика, общественный дискурс. То есть окружение в настоящем и прошлом данного человека, а также его личностные особенности и характеристики, такие как уровень эмоциональной устойчивости, склонность к риску и совершению нерациональных поступков. Переходя с анализа индивидуального уровня на общественный, мы можем увидеть, как формируется определенный культурный и образовательный уровень, который можно проанализировать для конкретного, например, государства. Но почему при одинаковом уровне цифровизации одни страны оказываются более защищенными по отношению к киберугрозам? Или почему одни организации намного реже сталкиваются с утечками и инцидентами, чем другие, где проблемы возникают постоянно? Казалось бы, почему везде не использовать передовые технологии защиты данных и наиболее эффективное антивирусное программное обеспечение? Проблема заключается в том, что социальные проблемы не устраняются техническими решениями. Даже самые совершенные антифрод-системы не решают проблемы низкой цифровой грамотности населения, низкого уровня подготовки ИТ-специалистов, нежелания брать на себя ответственность за совершаемые

действия или желание заработать в условиях тяжелой экономической ситуации. Как итог, технический ответ на социальные проблемы, которые активно эксплуатируются киберпреступностью, не устраняет саму причину возникающей проблемы. Да, это, как правило, быстрый ответ на угрозу здесь и сейчас, который способен замедлить или приглушить проблему, но не устранить или вернуть ее в умеренное русло. А самое главное – создать такое состояние системы, в котором вероятность эксплуатации уязвимости минимальна, а порог проникновения сквозь защитный барьер системы высок и сложен. К сожалению, в России по состоянию на 2023 год в этом вопросе нельзя отметить существенных изменений и перелома тренда. Меняются преступные схемы и подходы в зависимости от новостной повестки и условий, но базовый сценарий остается одним и тем же: раздобыть данные потенциальный жертвы, с помощью манипуляций войти в доверие и усыпить бдительность, получить доступ к счетам или аккаунтам и совершить кражу средств. Стоит признать, что население России сегодня, несмотря на непростую экономическую ситуацию, остается все еще желанным объектом совершения киберпреступлений, что подтверждают актуальные данные статистики. Киберпреступность постоянно бьет новые рекорды и остается острой и дорогой проблемой для всех: государства, бизнеса, населения. Как, исходя из всего вышеизложенного, подходить к обсуждению вопроса эффективной и стратегически верной борьбы с киберпреступностью?

Накопленный опыт дает возможность понять, что комплексная по своей сути проблема требует комплексного решения. Наивно надеяться на волшебное «чудо-оружие», которое разом обратит злоумышленников в бегство и заставит свернуть свою преступную деятельность. Такие системы, будь то с применением искусственного интеллекта, больших данных или иных «модных» сегодня технологий, могут помочь в этой борьбе, но не внести решающего вклада. Технократический подход к пониманию киберпреступности и борьбе с ней сегодня устарел. Его ограничение связано

прежде всего с тем, что он упускает из виду ключевую составляющую любой цифровой системы – социальную. Без понимания того, в каких условиях создается цифровой продукт; каким образом он внедряется и масштабируется; кем, как и в каких обстоятельствах используется, анализ возможных рисков использования такого продукта будет ограниченным и неполным. Поднимаясь на ступень выше, можно в целом говорить о необходимости формирования комплексного подхода к созданию и развитию цифровых продуктов, который учитывает риски и возможности обеих составляющих системы: цифровую и социальную. Игнорирование одной из них ведет к нарушению целостности восприятия и анализа происходящих процессов, упущению из вида системных уязвимостей. Например, занижение внимания к человеческому фактору при проектировании системы информационной безопасности приводит к тому, что самым слабым элементом системы становится человек. В таком случае фокус атак смещается с попытки взломать защищенный внутренний контур системы в сторону попытки проникновения за счет пользователя или администратора этой системы. Такие примеры мы часто можем видеть в банковском секторе: гораздо проще подкупить или обмануть банковского сотрудника, которых может насчитываться тысячи или даже десятки тысяч в рамках организации, нежели попытаться пробить укрепленный рубеж информационной защиты банка. Аналогичную проблему мы наблюдаем и в более широком секторе: обмане населения за счет эксплуатации цифровой безграмотности, доверчивости, страхов или убеждений, новостной повестки. Вместе с тем все образовательные и информационные активности, нацеленные на повышение грамотности населения, бессмысленны без постоянного улучшения отказоустойчивости цифровых систем. В процессе непрерывной разработки новых и улучшения существующих цифровых продуктов, новые уязвимости и ошибки появляются на регулярной основе. Это требует постоянного улучшения и тестирования безопасности таких систем в самых разных

обстоятельствах и сценариях. Любая программа, сайт, приложение или любой иной цифровой продукт быстро устаревает без регулярной технической поддержки, и, что самое важное, становится потенциально опасным для пользователей. Это объясняет тот факт, что разработчики программного обеспечения настоятельно не рекомендуют использовать старые, неподдерживаемые версии своего продукта, а переходить на наиболее свежие версии. Как итог, даже самый продвинутый пользователь, который хорошо разбирается в вопросах информационной безопасности, может стать жертвой киберпреступников, если защитный контур системы достаточно низкий и содержит в себе уязвимости, которые могут быть использованы для незаконных действий. Но как обеспечить так, чтобы защита цифровых систем была на высоком уровне? Здесь мы опять выходим на уровень социальный. Высокое качество выпускаемой продукции обеспечивается за счет профессионализма разработчиков, которые работают в благоприятных для этого условиях. Какие это условия? Это прежде всего образование: независимые, богатые университеты, которые способны проводить свою автономную образовательную политику и привлекать лучших специалистов в своей области, использовать свои стандарты и программы подготовки специалистов, обмениваться опытом с ведущими мировыми институтами и организациями. Это заинтересованность со стороны государства и общества: создание условий для развития цифровых технологий и новых продуктов через инвестиции в образование и технологии, создания ИТ-кластеров с привлечением лучших специалистов и преподавателей со всего мира, выстраивание ИТ-бренда страны на международной арене. Это возможности международной кооперации и обмена опытом: изоляционистская политика в этом вопросе не способствует созданию успешных продуктов. Рыночные условия конкуренции: государственная монополия и стандартизация убивают дух борьбы и мотивацию создать продукт лучше, чем у твоих конкурентов. И здесь мы

снова вступаем на поле социальное, как неразрывно связанное с полем цифровым: социальное порождает цифровое, а цифровое воздействует на социальное. Тесная взаимосвязь двух систем и постоянный поиск баланса – своего рода смена цифровых эпох.

Это регулярные и бесконечные циклы: телефонов и компьютеров, приложений, сайтов, технологий, подходов к разработке и безопасности цифровых систем, законодательства в области информационных технологий, инструментов влияния и контроля со стороны гражданского общества, возможностей для развития и масштабирования новых технологий, алгоритмов совершения преступных действий и сохранения анонимности, моделей использования и потребления цифрового контента и устройств. И можно проследить, как всплеск активности киберпреступности нередко приходится на смену эпох цифрового развития. Эта активность связана с эксплуатацией уязвимости нового состояния системы: зыбкого, неустойчивого, постоянно меняющегося. Сегодня новые технологии можно сравнить со стихией, которая неожиданно и стремительно накрывает привычный ландшафт и меняет его, причем характер изменений довольно сложно прогнозировать. Бумы персональных компьютеров и телефонов, распространения интернета, соцсетей, появление криптовалют или онлайн–банкинга, электронной коммерции показывают, что вместе с очевидной пользой они несут и существенные риски за счет эксплуатации возникающих при этом уязвимостей нового состояния системы. Например, бум онлайн-банкинга в России повлек за собой рост мошеннических действий в отношении счетов и вкладов граждан. Бум криптовалют повлек за собой волну мошеннических действий на этапе ICO, взлом кошельков и криптобирж. Важно понимать, что новая технология или продукт – это всегда зона повышенного риска, и, следовательно, объект повышенного внимания. Иногда необходимо пройти несколько десятков или даже сотен итераций продукта, чтобы подготовить относительно стабильную и

надежную версию цифрового продукта. Но проблема в том, что за счет развития СМИ, мессенджеров и горизонтальных связей, привычная схема жизненного цикла принятия инновационных продуктов трансформируется. Сегодня Интернет, персональный компьютер и телефон – это не предметы роскоши и не показатели статуса. Если еще 30 лет назад персональный компьютер был доступен, как правило, высшему классу с хорошим достатком и уровнем образования, то сегодня дешевые смартфоны доступны даже в самых бедных странах мира. Если раньше новаторами технологий могло быть ограниченное меньшинство общества, то сейчас случайным новатором и распространителем новой технологии может оказаться практически любой пользователь интернета, просто потому что он где–то прочитал об этом или узнал от знакомых. Новатором может быть практически каждый. Из этого вытекает другая проблема – это не постепенное и плавное, а лавинообразное распространение новой технологии. Сегодня большую роль в этом играют и средства массовой информации. Достаточно написать одну новость о новом, необычном продукте, и в течение нескольких дней можно наблюдать кратный рост новых пользователей. Яркий пример последних лет – это ажиотаж вокруг криптовалют и активный прилив новых пользователей, который спустя некоторое время обернулся рядом инцидентов с хакерскими атаками на криптобиржи. Бум криптовалют – хрестоматийный пример социального заражения, когда желание прибыли и эмоции затуманивает сознание человека, его рациональную составляющую. А за счет эффекта виральности в интернет-среде информация о продукте активно распространяется среди большого количества пользователей. И вот уже человек, слабо осознающий риски покупки криптовалют и плохо понимающий принцип работы технологии блокчейн, криптобирж, горячих и холодных кошельков, уже готов покупать и хранить криптовалюту на свои или даже заемные средства. И все это происходило в условиях, когда криптовалюты еще никак не были

урегулированы на законодательном уровне, не говоря уже о компенсациях за кражу активов. Более свежий пример – взрывной рост популярности социальной сети Clubhouse, пик которой пришелся на период пандемии COVID–19 в 2020–2021 годах. И тут мы снова можем наблюдать тесное переплетение цифрового и социального. Существующая инфраструктура позволила разработать и распространить новый цифровой продукт, а социальное – привлечь к нему интерес и новых пользователей. Однако появление чего-то нового ведет за собой изменения системы: полностью или какой-то ее части. Это новое может быть враждебно для системы, вступать с ней в противоречие на первых этапах включения. Сама система может быть не готова к появлению в ней нового, пока еще чужеродного элемента. Причем это касается как цифровой, так и социальной части системы. И тут мы подходим к вопросу выработки комплексного подхода к устойчивому цифровому развитию. Но что мы вкладываем в это понятие?

Устойчивое цифровое развитие – это такой подход к проектированию, внедрению и масштабированию цифровых продуктов и устройств, который обеспечивает минимальные риски зарождения и распространения в ней незаконной, преступной деятельности в рамках как всей социо-цифровой системы, так и отдельных ее частей. Это прежде всего изменение самого целеполагания при разработке и использовании цифровых продуктов и устройств. Цифровые инциденты, все более глубокие и масштабные по своей природе, все отчетливее показывают необходимость пересмотра сформировавшегося ценностного подхода к технологиям. История показывает, что такие переломы сложны и многоступенчаты, продолжительны по времени, но возможны и необходимы. Примеры из экологии или атомной энергетики это подтверждают. Необходимость подобного перехода назрела и в сфере цифровых технологий: от хаоса к порядку и структуре, от максимизации прибыли к минимизации рисков и уязвимостей, от безграмотности к массовому просвещению.

Данные цели соотносятся с целями в области устойчивого развития ООН, принятыми в 2015 году до 2030 года. В рамках девятой цели «Создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям» выделяются задачи по развитию «качественной, надежной, устойчивой и стойкой инфраструктуры»[157]. Сегодня в мировой повестке, на уровне международных организаций отпадает вопрос о необходимости технического прогресса: «инновации имеют ключевое значение для поиска долгосрочных решений как экономических, так и экологических проблем, таких как повышение эффективности использования ресурсов и энергоэффективности»[158]. Однако характер протекания технологического развития крайне важен, что и отмечается в документах ООН: приоритет отдается безопасности и стойкости инфраструктуры, которая является одной из основ для развития и процветания всего человечества. Без надежной и отказоустойчивой технологической инфраструктуры невозможно достижение целей в области устойчивого развития. В связи с этим концепцию устойчивого цифрового развития можно рассматривать как важный шаг на пути к реализации целей устойчивого развития ООН как «плана действий в интересах людей, планеты и процветания»[159].

В рамках первой главы были было проанализировано актуальное состояния киберпреступности в России и динамика развития проблемы в стране в последние 5 лет. Результаты проведенного анализа дали

[157] Официальный сайт ООН. Цель 9: Создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям [Электронный ресурс]. Режим доступа: https://www.un.org/sustainabledevelopment/ru/infrastructure–industrialization/ (дата обращения: 09.07.2023).

[158] Официальный сайт ООН. Цель 9: Создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям [Электронный ресурс]. Режим доступа: https://www.un.org/sustainabledevelopment/ru/infrastructure–industrialization/ (дата обращения: 09.07.2023).

[159] Резолюция, принятая Генеральной Ассамблеей ООН 6 июля 2017 года [Электронный ресурс]. Режим доступа: https://ggim.un.org/documents/A_Res_71_313_r.pdf (дата обращения: 09.07.2023).

перспективу более глубокой теоретической проработки данного феномена и определения тех факторов прежде всего социальной природы, которые лежат в основе проблемы киберпреступности. Второй параграф направлен на раскрытие социальной природы киберпреступности как непрерывной криминальной деятельности по поиску и эксплуатации социальных уязвимостей социо-цифровой системы. Полученное понимание социальной природы киберпреступности позволяет перейти к разработке новой, долгосрочной и более эффективной стратегии противодействия киберпреступности, что будет сделано в рамках второй главы исследования.

Глава 2. Стратегия противодействия киберпреступности в парадигме устойчивого цифрового развития

По результатам первой главы были проанализированы ключевые тенденции развития проблемы киберпреступности в последние 5 лет и показана их социальная природа, что делает киберпреступность прежде всего социальной проблемой. Данное заключение важно с позиции как понимания происходящих процессов и закономерностей развития проблемы, так и выработки эффективных стратегий противодействия. Выработке такой стратегии посвящена вторая глава диссертационного исследования.

§ 2.1 Проблема киберпреступности в России в оценке экспертов[160]

В первой главе была показана сложная социальная природа киберпреступности как эксплуатация социальных уязвимостей, вызванных дисбалансом между технологической и социальной подсистема единой социо–цифровой системы. Для эффективного решения проблемы важно глубокое понимание причин сложившейся ситуации. Есть ли это осознание в профессиональном сообществе: среди экспертов, исследователей, практиков? В какой степени экспертное сообщество осознает риски новых цифровых технологий? Понимают ли эксперты сложную социальную природу киберпреступности? Есть ли понимание выхода из сложившейся ситуации через прогнозирование рисков и принятие превентивных действий? Происходит ли осознание данной проблемы среди населения России – массового сегмента потребителей цифровых товаров и услуг, одного из главных объектов киберпреступного воздействия?

[160] При подготовке данного раздела использованы следующие публикации, выполненные автором лично, в которых отражены основные результаты, положения и выводы исследования: Швыряев П.С. Проблема киберпреступности в России: актуальное состояние и перспективы решения / П.С. Швыряев // Уровень жизни населения регионов России. – 2023. – Том 19. – № 4. – С. 616–629.

Для ответа на поставленные вопросы обратимся к результатам исследования[161], проведенного в рамках проекта «Концепт «цифрового рая» как пространство общественных ожиданий и страхов». Исследование проведено в 2023 году рабочей группой, в которую вошли эксперты Центра СИТИ НИУ ВШЭ и Фонда «Петербургская политика» под руководством Елены Джибиловой (Центр СИТИ НИУ ВШЭ), на базе Института научной информации по общественным наукам РАН по итогам отбора научных проектов, поддержанных Министерством науки и высшего образования РФ и Экспертным институтом социальных исследований.

Согласно данным проведенного исследования, по состоянию на 2023 год около 60% россиян можно назвать технооптимистами: они положительно оценивают роль цифровых технологий в будущем. Такая высокая позитивная оценка выглядит диссонансом на фоне того колоссального всплеска киберпреступности, который наблюдался в России и в мире во время пандемии. От этой деятельности, по результатам исследований, мог пострадать каждый шестой россиянин[162], что дает внушительную цифру в миллионы пострадавших граждан страны.

Не проявляется высокий уровень осознания важности и серьезности проблемы киберпреступности и при перечислении минусов цифровизации. Несмотря на то, что проблема киберпреступности сегодня касается каждого гражданина страны, на первом месте идут 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.

Далее будут представлены результаты авторского экспертного опроса.

---

[161] HSE daily. Между раем и адом: как россияне относятся к цифровизации [Электронный ресурс]. Режим доступа: https://daily.hse.ru/post/976 (дата обращения: 21.08.2023).

[162] РБК. Каждый шестой россиянин пострадал из–за телефонных мошенников. [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/02/10/2021/6156e99a9a794778904993ed (дата обращения: 12.06.2023).

Цель исследования: на основании результатов экспертного опроса выявить ключевые факторы, которые, по мнению опрошенных экспертов, оказывают влияние на состояние киберпреступности в России, а также определить их оценку стратегий противодействия киберпреступности.

Достижение поставленной цели потребовало решения следующих задач:

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

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

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

Объект исследования – киберпреступность в России.

Предмет исследования – экспертные оценки факторов, оказывающих влияние на состояние киберпреступности в России.

Обратимся к результатам экспертного опроса, который был проведен в формате дистанционного интервью в июле-августе 2023 года[163]. В рамках данного исследования было проведено 17 экспертных интервью с представителями следующих организаций (в скобках указаны должности экспертов):

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

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

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

[163] Швыряев П.С. Проблема киберпреступности в России: актуальное состояние и перспективы решения // Уровень жизни населения регионов России. 2023. Том 19. № 4. С. 616–629.

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

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

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

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

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

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

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

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

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

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

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

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

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

Экспертная выборка включает как исследователей-теоретиков проблемы киберпреступности, так и практиков: бывших следователей, которые непосредственно работали в сфере расследования киберпреступлений, а также в образовательных учреждениях по подготовке специалистов для расследования в том числе и преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

В рамках подготовительного этапа была разработана дорожная карта глубинного интервью (Приложение 1), которое включает 4 блока вопросов по следующим темам:

1. Экспертная оценка состояния киберпреступности в России.
2. Экспертная оценка причин сложившейся ситуации.
3. Экспертная оценка стратегий решения проблемы.
4. Заключительный блок.

Блоки вопросов выстроены в логическом порядке.

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

Вопросы второго блока направлены на определение позиции эксперта по поводу причин сложившейся ситуации: ключевые факторы усугубления проблемы, эффективность государственной политики и правоохранительных

органов, оценка влияния санкционного давления с 2022 года и прочих факторов.

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

Четвертый блок направлен на то, чтобы предоставить возможность эксперту в свободной форме изложить свое мнение по тем вопросам, которые не прозвучали ранее в ходе интервью.

Первый вопрос был направлен на определение позиции экспертов относительно актуального состояния киберпреступности в России. Практически все эксперты отмечают актуальность данной проблемы, ее рост в последние годы и фиксацию показателей на высоких уровнях по состоянию на 2023 год. Один из экспертов отметил, что в России фактически упустили нарастающую проблему, которая активно формировалась в течение последних нескольких лет. Другой эксперт на основании большого опыта работы в правоохранительных органах заявил, что, по его мнению, официальная статистика лишь отчасти отражает действительность, но не передает фактического масштаба проблемы. Это объясняется как особенностями классификации преступлений внутри российской правоохранительной системы, так и латентностью как характерной чертой такого рода преступлений. Жертва далеко не всегда может осознавать факт совершенного в отношении нее преступления, либо не заявлять об этом в полицию[164]. Тем не менее, даже с учетом некоторых сложностей с систематизацией и классификацией преступлений, эксперты отмечают отчетливый тренд на стабильное увеличение количества киберпреступлений в России. Отмечается и возросшее количество кибератак, в том числе и на критическую инфраструктуру России, которые совершаются из-за рубежа.

[164] Ведомости. Киберпреступность в домашних тапочках [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/opinion/articles/2018/10/17/783976–kiberprestupnost (дата обращения: 24.07.2023).

Стоит отметить, что повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования – одно из основных направлений обеспечения информационной безопасности страны, провозглашенное в Доктрине информационной безопасности Российской Федерации[165].

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

Далее экспертам был задан вопрос о том, в чем они видят главную опасность киберпреступности. Наиболее популярный ответ – это латентный характер киберпреступности. В качестве серьезной опасности киберпреступности эксперты отмечают и все более заметный экономический

[165] Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 30.07.2023).

и социальный ущерб, который за последние 4 года вырос более чем втрое[166]. Снижающийся порог входа в преступную индустрию – еще одна важная проблема, которую отметили эксперты. Один из экспертов отметил, что если еще 30 лет назад киберпреступность была занятием наиболее талантливых и продвинутых знатоков в области информационных технологий (так называемых «хакеров»), то в настоящее время, в век высокой доступности интернета и устройств связи, порог входа в преступную индустрию сильно снижен. Как отметил один из экспертов, для совершения преступных деяний в социальных сетях или звонков потенциальным жертвам не требуется каких–либо специальных знаний или умений: это по сути классические мошеннические операции одних людей в отношении других, совершаемые с использованием цифровых инструментов коммуникации. Низкий порог входа приводит к формированию полноценной индустрии, на что обратил внимание один из экспертов. Существуют полноценные нелегальные компании со своими офисами, оборудованием, системами найма и мотивации, которые занимаются незаконной киберпреступной деятельностью. Эксперт отметил, что развитие данной индустрии – повод обратить на нее пристальное внимание как со стороны правоохранителей, так и общественности.

Еще одна проблема, которую отметили эксперты, – это низкая эффективность расследования киберпреступлений. И если в расследовании относительно простых преступлений, не требующих высокой технической и исследовательской подготовки, эксперты отмечают положительную динамику, то в расследовании преступлений, совершенных злоумышленниками среднего и высокого уровня, ситуация складывается негативно. В процессе интервью эксперты, которые имеют непосредственный опыт работы в правоохранительных органах, перечислили

[166] Ведомости. Интернет несет потери [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/importsubstitution/new_technologies/articles/2023/03/14/966290–internet–neset–poteri (дата обращения: 06.08.2023).

целый ряд проблем, которые, по их мнению, не позволяют российским правоохранительным органам эффективно бороться с новыми вызовами со стороны киберпреступного сообщества. К ключевым причинам низкой эффективности российской правоохранительной системы эксперты отнесли низкую мотивацию сотрудников, прежде всего материальную; низкий уровень подготовки слушателей академий, проблемы с повышением квалификации действующих сотрудников; отсутствие стандартизированного формата коммуникации правоохранительных органов с операторами мобильной связи и банками по обмену информацией; административно-территориальные барьеры при обмене информацией между регионами; проблемы в материально-техническом обеспечении; недоукомплектованность профильными ИТ-специалистами, которые должны работать в тесной связке со следователями.

Помимо низкой эффективности правоохранительной системы, эксперты отметили быстроту реакции и принятия решений со стороны преступного сообщества: происходит постоянный процесс тестирования новых преступных схем и их масштабирование на большое количество потенциальных жертв. Эксперты отметили, что таких условиях как правоохранительные органы, так и законодательная база и инструменты информирования населения не всегда успевают за появлением новых способов мошенничества.

По мнению экспертов, принципиально не изменит ситуацию и ужесточение законодательства в отношении правонарушителей. Один из экспертов емко сформулировала бесперспективность данного направления. *На мой взгляд, важно не ужесточение наказания в законодательстве, а неотвратимость ответственности. Тогда, когда за киберпреступления неизбежно будет следовать наказание, даже не самое жестокое, это будет более эффективной мерой, чем повышение санкций за него*.

Среди ключевых трендов последних лет в области киберпреступлений наиболее популярный ответ экспертов – рост доли социальной инженерии. Один из экспертов подчеркнул, что эффективное средство решения данной проблемы до сих пор не найдено, поскольку для абсолютно любого человека свойственны ошибки, когнитивные искажения или проявления эмоций.

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

На вопрос о том, уделяется ли проблеме киберпреступности достаточное внимание со стороны органов государственной власти, ряд экспертов отметили низкую способность системы работать на опережение и предупреждать потенциальные киберугрозы. Эксперты подчеркивают, что несмотря на довольно широкую законодательную базу, которая включает в себя Доктрину информационной безопасности Российской Федерации[167], федеральные законы «Об информации, информационных технологиях и о

[167] Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 30.07.2023).

защите информации»[168], «О персональных данных»[169], Федеральный закон «О техническом регулировании»[170] и другие, заявления официальных лиц различного уровня о важности проблемы, реализуемая в настоящий момент политика борьбы с киберпреступностью имеет значительный потенциал к росту, что отметили несколько экспертов. И реализовать этот потенциал можно через повышение эффективности раскрытия киберпреступлений правоохранительными органами, а также через повышение профилактики киберпреступлений: в ряде случаев киберпреступление целесообразнее предупредить, чем ликвидировать последствия. Сотрудники академий МВД подчеркнули, что несмотря на то, что проблему низкой раскрываемости киберпреступлений констатировали еще в 2020 году, более трех лет назад, каких–либо фундаментальных изменений в данном вопросе до сих пор нет: проблема обучения следователей и привлечения квалифицированных ИТ-специалистов в правоохранительные органы остается острой.

На вопрос об эффективности российских правоохранительных органов в борьбе с киберпреступностью 11 из 17 экспертов отметили неэффективность или низкую степень эффективности. Один из экспертов прямо отметил, что сегодня «правоохранительные органы практически ничем не могут помочь гражданам». Другой эксперт выразил слабую надежду на сформированное в сентябре 2022 года управление по борьбе с киберпреступностью[171]. Несколько экспертов также подчеркнули, что при

---

[168] Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149–ФЗ (последняя редакция) [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.07.2023).

[169] Федеральный закон "О персональных данных" от 27.07.2006 N 152–ФЗ (последняя редакция) [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 30.07.2023).

[170] Федеральный закон "О техническом регулировании" от 27.12.2002 N 184–ФЗ (последняя редакция) [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_40241/ (дата обращения: 30.07.2023).

[171] КоммерсантЪ. В МВД создано управление по борьбе с киберпреступностью [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/5592758 (дата обращения: 30.07.2023).

анализе эффективности правоохранительных органов важно ранжировать киберпреступников по уровню и степени их профессионализма: если в вопросе расследования условно простых преступлений, совершенных не профессиональными злоумышленниками без специальных средств связи и программного обеспечения, можно отметить положительную динамику, то в вопросах расследования киберпреступлений, совершенных профессионалами высокого уровня, сохраняются серьезные сложности.

Каким образом могут повлиять отмеченные экспертами проблемы на дальнейший характер развития киберпреступности в стране на горизонте 2-3 лет? 11 из 17 экспертов прогнозируют дальнейшее усугубление проблемы: рост числа киберпреступлений на фоне сохраняющейся низкой раскрываемости. Один из экспертов прогнозирует ежегодный рост числа совершаемых киберпреступлений на 15-20 процентов; рост количества приостанавливаемых производством дел по причине неустановления лиц, подлежащих привлечению к уголовной ответственности; снижение количества преступников, привлекаемых к уголовной ответственности; использование технологий DeepFake для совершения преступлений. Другой эксперт также отмечает, что ситуация с проблемой киберпреступности будет усугубляться на фоне сохраняющейся замедленной реакции со стороны органов безопасности, которые и дальше не будут успевать за новыми трендами и схемами совершения преступлений в цифровой среде. Третий эксперт отметил, что в ближайшие 2-3 года общее количество кибератак увеличится минимум на 30 процентов, при этом атаки все чаще будут хорошо организованы группировками или отдельными хакерами. Один из экспертов при ответе на этот вопрос отметил важность характера развития технологий, в том числе искусственного интеллекта: *все более активное внедрение ИИ в преступную деятельность, в частности, Chat GPT уже сейчас позволяет маскировать безграмотность некоторых «компьютерных преступников».* Внимание на проблему искусственного интеллекта обратил и

другой эксперт, подчеркнув, что преступники уже сейчас активно осваивают ИИ и продолжат это делать для совершения противозаконных деяний. Учитывая, что предугадать развитие искусственного интеллекта и последствия этого развития сложно, проблеме использования искусственного интеллекта в преступных целях должно быть уделено важное внимание со стороны исследователей, практиков-разработчиков, лиц принимающих решения. Таким образом, киберпреступления с использованием искусственного интеллекта – еще одно важное направления для исследования в рамках общей проблемы киберпреступности.

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

ответственности должностных лиц за определенные сферы экономической, в том числе хозяйственной, а также общественной жизни конкретных государственных и общественных институтов.

Исходя из описанных выше причин, экспертам был задан вопрос о том, какие ключевые решения должны были быть предприняты для недопущения столь стремительного ухудшения ситуации в последние несколько лет. Предлагаемые экспертами решения можно разбить на несколько ключевых блоков.

1. Более масштабная, глубокая и системная работа с населением по повышению осведомленности, цифровой грамотности и образованности. Один из экспертов предложил введение специальных курсов по информационной гигиене на уровне общего, специального и высшего образования. Другие эксперты отметили важность постоянной работы с населением как одной из базовых составляющих профилактики предупреждения киберпреступлений. Еще один эксперт описал высокую грамотность населения как «прививку от киберпосягальств». *Сформированная на необходимом уровне цифровая грамотность станет не только одним из столпов эффективного противодействия, но и особой «вакциной», не позволяющей развиваться вирусу. Когда сам организм борется с вирусом. Я бы назвала это «прививкой от киберпосягательств».*

2. Модернизация правоохранительных органов, которые оказались не готовы к быстрому переходу преступности в цифровой сектор. Один из экспертов отметил ряд шагов, которые могли бы повысить эффективность правоохранителей в расследовании киберпреступлений: *увеличение штатной численности подразделений Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России, введение специализации в следственных подразделениях и районных судах по данному направлению, установление данным сотрудникам дополнительных надбавок к должностным окладам*

«за сложность и напряженность», повышение квалификации сотрудников органов предварительного расследования по данному направлению на системной основе. Отсутствие централизованного процесса обучения и повышения квалификации сотрудников правоохранительных органов отметил и другой эксперт, непосредственно работающий в академии МВД. Также эксперты отметили и сохраняющиеся проблемы с кадрами: российская правоохранительная система испытывает кадровый голод, особенно в области высококвалифицированных ИТ-специалистов, ключевой задачей которых и должна быть борьба с киберпреступностью на стороне государственной власти.

3. Более тесное международное сотрудничество, необходимость которого вытекает из трансграничной сущности киберпреступности. Один из экспертов, имеющий опыт работы в правоохранительных органах, отметил, что тесное взаимодействие российских правоохранителей с их коллегами из других стран по линии Интерпола для расследования киберпреступлений так и не было установлено. Если в вопросах традиционных преступлений, совершаемых в физическом мире, обмен информацией активно происходил, то в вопросах расследования киберпреступлений взаимодействие было минимально. Несмотря на то, что в 2022 году Россия не была исключена из Интерпола, наложенные ограничения могут еще сильнее затруднить взаимодействие между спецслужбами, в том числе и по расследованию киберпреступлений. Санкционное давление и накладываемые ограничения со стороны «недружественных» стран характеризуются экспертами как неблагоприятные в вопросе решения проблемы киберпреступности в стране. Один из экспертов подчеркнул, что *международное сотрудничество играет важную роль не только для обмена опытом противодействия киберпреступлениям, но и для принятия совместных мер, в том числе правовых, преследующих указанные цели. Тем более, как уже отмечалось, такие преступления выходят за пределы границ отдельного государства, а*

значит и вопрос юрисдикции может быть не решен или вызывать проблемы при отсутствии договоренностей между странами, отраженных в международных документах.

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. Несколько экспертов подчеркнули, что в решении проблемы киберпреступности кадры имеют ключевое, основополагающее значение, и в этом вопросе у России сохраняются серьезные проблемы. Один из экспертов подчеркнул серьезность проблемы оттока квалифицированных ИТ-кадров не только в моменте, но и на долгосрочную перспективу, что может внести свой негативный вклад в перспективные технические разработки в области кибербезопасности.

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

6. Эффективное и оперативное взаимодействие правоохранительных органов, банков и операторов связи для блокировки мошеннических ресурсов и номеров. Эксперты подчеркивают, что положительные решения в данном вопросе были приняты с сильным запозданием: лишь в 2021 году на эту проблему обратил внимание президент страны[172]. Тем не менее, один из экспертов в ходе интервью отметил

[172] Ведомости. Путин поручил МВД наладить взаимодействие с банками для борьбы с мошенничеством [Электронный ресурс]. Режим доступа:

сохранение проблемы по состоянию на середину 2023 года: в регионах формат взаимодействия между правоохранительными органами и операторами связи может строиться не на формальных предписаниях, а на основании личных знакомств и предпочтений, что имеет свои негативные последствия, которые приобретают системный характер.

7. Совершенствование российского законодательства в сфере информационных технологий. Один из экспертов отметил необходимость *«полного обновления норм, регулирующих сеть «Интернет».*

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

Но реализуются ли указанные экспертами решения? Лишь один из 17 опрошенных экспертов дал полностью утвердительный ответ на этот вопрос. Эксперты отметили, что в некоторых вопросах можно выделить отдельные эффективные решения, которые могут иметь положительный, но ограниченный эффект. И которые не способствуют изменению ситуации в целом. Такие меры, по мнению экспертов, имеют запоздалый характер и не способны в корне переломить ситуацию. Один из экспертов отметил, что киберпреступность, в отличие от государственной машины, хаотична: она не имеет четких процедур и регламентов, распространяется молниеносно и может принимать самые разные формы, зачастую сложно прогнозируемые. Для государства, которое более инертно и функционирует по своим законам и нормам, такой противник является весьма проблематичным. В такой ситуации остается открытым вопрос: готово ли государство перестраиваться под новые условия для конкурентной борьбы с новым серьезным

---

https://www.vedomosti.ru/finance/news/2021/03/03/860016–putin–poruchil–mvd–naladit–vzaimodeistvie–s–bankami–dlya–borbi–s–moshennichestvom (дата обращения: 01.08.2023).

противником, либо готово продолжать сохранять отстающую, проигрышную позицию?

Для четкого ответа на этот вопрос экспертом был задан прямой вопрос: является ли реализуемая в России в настоящий момент политика в области борьбы с киберпреступностью результативной и эффективной? Ни один из опрошенных 17 экспертов не дал четкий утвердительный ответ. 9 экспертов отметили некоторые положительные решения, но которых недостаточно для принципиального изменения ситуации. 2 эксперта отметили, что российская политика в области противодействия киберпреступности в настоящий момент полностью неэффективна. Остальные эксперты четкую позицию по данному вопросу не высказали.

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

непоследовательных мер недостаточно для стабилизации ситуации в моменте, а тем более решения проблемы в перспективе.

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

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

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

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

4. Коррупция.

5. Недостаточное финансирование в сфере противодействия киберпреступности.

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

Описанные выше проблемы один из экспертов суммировала таким образом. *Отсутствие комплексного реагирования на проблему. В одном направлении работа ведется, в других нет. Но только комплексное противодействие будет высоко эффективно. Это и право, и профилактика, и кадры, и наука. Еще и международный аспект, и отток кадров.*

Есть ли решения у данных проблем? Здесь ряд экспертов снова обратили внимание на отсутствие системного подхода к решению проблемы киберпреступности. Усугубление проблемы киберпреступности в мире и России приходится на экстраординарные события планетарного масштаба: пандемию COVID-19 в 2020-2021 годах и усиление международной

напряженности начиная с 2022 года. В таких условиях фокус внимания ключевых лиц может смещаться на более приоритетные, как им кажется, проблемы. Однако это ошибочная позиция. Очевидно, что информационные технологии и цифровой мир – это новая реальность, неотъемлемая черта образа человечества настоящего и будущего. А киберпреступность – неразрывный спутник этой новой реальности. Не замечать эту проблему или занижать ее значимость, не предпринимать решительные действия по борьбе с киберпреступностью – стратегия не только проигрышная, но и опасная для благополучия населения и развития страны.

Общение с экспертами и исследователями киберпреступности подтвердило гипотезу о том, что в России не были предприняты необходимые меры для недопущения ухудшения ситуации. На данных официальной статистики было подробно проанализировано, как за последние несколько лет на фоне высоких темпов цифровизации происходил переход преступности в цифровую реальность. Было бы наивно надеяться, что с массовым распространением электронной коммерции, онлайн-банкинга, удаленной работы и прочего широкого круга активностей в цифровой среде и с использованием информационных технологий этим новым трендом не воспользуются преступники. А возможности технологий по сохранению анонимности, сокрытию следов преступлений, подделке голоса или изображений лишь только способствуют повышению вероятности совершения деяния без последствий для злоумышленника.

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

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

Общение с экспертами показало, что эффективная стратегия противодействия киберпреступности требует более глубокого и комплексного взгляда на проблему, в основе которого – понимание социальной природы феномена киберпреступности. Важно подчеркнуть, что предлагаемые экспертами меры носят социально ориентированный характер: просвещение населения, реформа правоохранительных органов, создание условий для подготовки и удержания ИТ-специалистов и так далее. Но как объединить все эти меры в единую стратегию по противодействию киберпреступности? Этому вопросу посвящен следующий параграф диссертационного исследования.

§ 2.2 Устойчивое цифровое развитие как основа альтернативной стратегии борьбы с киберпреступностью[173]

Одной из ключевых задач в рамках данного исследования было показать сложную, многогранную сущность феномена киберпреступности. *Киберпреступность – это не просто незаконная деятельность с использованием цифровых технологий, а производная социо-цифровой*

[173] При подготовке данного раздела использованы следующие публикации, выполненные автором лично, в которых отражены основные результаты, положения и выводы исследования: Швыряев П.С. Проблема киберпреступности в России: актуальное состояние и перспективы решения / П.С. Швыряев // Уровень жизни населения регионов России. – 2023. – Том 19. – № 4. – С. 616–629.

реальности, эксплуатация уязвимостей самой этой системы с целью совершения противозаконных деяний в отношении людей. Киберпреступность можно рассматривать как индикатор состояния системы, ее структуры и процессов, протекающих в ней и во взаимодействии с окружающей средой. По характеру развития и распространения киберпреступности в системе можно оценивать ее текущее состояние, степень защищенности системы, ее готовности к изменениям и угрозам в будущем. По характеру ответа на угрозы и свершившиеся инциденты можно судить о восприятии киберпреступности в данной системе, степени ее защищенности в настоящий момент и готовности к потенциальным киберугрозам в будущем.

Исходя из анализа киберпреступности последних лет, можно заключить, что несмотря на комплексы шагов, предпринимаемых на самых разных уровнях различными акторами со стороны международных и государственных институтов, коммерческих и общественных организаций, о решении проблемы киберпреступности на всех этих уровнях пока говорить не приходится. В настоящее время проблема киберпреступности не находится под полным контролем, а современный процесс цифровизации можно сравнить с передвижением по минному полю: никогда не знаешь, когда и в каком месте произойдет взрыв. Причем масштабы таких инцидентов порой сложно смоделировать: последствия наносят гораздо более серьезный и глубокий ущерб, чем может казаться на первый взгляд. Как итог, проблема киберпреступности остается актуальной сейчас и важной в долгосрочной перспективе: в том числе от этого зависит устойчивость социальной и цифровой систем в будущем. Будет ли оно безопасным для всех пользователей или же киберинциденты различного масштаба станут обыденностью подобно тому, как сейчас стал рядовым поток новостей об утечках конфиденциальных данных?

В глобальном смысле необходимо поставить вопрос о выработке такого подхода к развитию общества и технологий, который обеспечивает максимальную пользу и минимизирует реальный и потенциальный вред. События последних лет показывают, что киберпреступность как опасность для человечества играет все более значимую роль. В период пандемии киберпреступные сообщества оказались одними из главных выгодоприобретателей очередной волны цифровизации. Объем суммарного ущерба от киберпреступности растет из года в год: к 2030 году прогнозируется уровень ущерба, сопоставимый с текущим уровнем мирового ВВП, а киберпреступность рассматривается как одна из возможных причин глобального кризиса[174]. В этой связи вопрос о выработке эффективного подхода к борьбе с киберпреступностью крайне актуален. Такой подход должен быть обращен прежде всего на сами причины, которые позволяют киберпреступности весьма эффективно существовать в нынешней реальности. Попытка бороться с последствиями без анализа причин, как показывает опыт, неэффективна: такие меры имеют ограниченный, фрагментарный характер и не могут привести к долгосрочному решению проблемы.

В этой связи подробно проанализируем одну из важных особенностей киберпреступности – это использование одних и тех же системных уязвимостей разными способами. Рассмотрим это на примере.

В последние годы в России особенно участились звонки гражданам под видом сотрудников органов правопорядка, банков или государственных структур. Ключевая цель – с использованием психологического давления заставить человека совершить перевод средств со счета потенциальной жертвы на счет мошенников. Анализ динамики похищенных денежных средств говорит о том, что данный способ мошенничества показывает свою

[174] Вести.ru. Потери мировой экономики от кибератак к 2030 году оценены в $90 трлн. [Электронный ресурс]. Режим доступа: https://www.vesti.ru/finance/article/2481467 (дата обращения: 24.02.2023).

высокую эффективность в течение нескольких лет. При этом с течением времени усложняется сценарий совершения преступления. Так, после того, как эффективность звонков под видом банковских сотрудников начала падать, появились новые сценарии с использованием подменных номеров, технологий изменения голоса или звонков под видом сотрудников государственных структур. Однако сам вид мошенничества, несмотря на огромное количество разнообразных схем, остается единым – использование методов социальной инженерии. Каковы возможные стратегии борьбы с такого рода мошенническими действиями?

Первый из них – тактический. Это сиюминутный ответ на новую угрозу. Например, с началом роста мошеннических звонков по всей стране можно было наблюдать кампании по массовому информированию граждан: призывы к ужесточению законодательства, освещение в СМИ, работа с населением по повышению осведомленности, технологические защитники от мошеннических звонков. Ответом стало падение эффективности старой схемы и быстрая переориентация на новую, с использованием легенд про представителей правоохранительных органов и государственных структур. По мере исчерпания потенциала очередной преступной схемы, мошенники переключились на использование продвинутых DeepFake-технологий синтеза речи. Особенность новой схемы мошенничества – это высокая схожесть синтезированной речи с оригиналом, что снижает бдительность жертвы и повышает потенциальную эффективность совершения противозаконных действий в отношении нее. Ответом на новый вызов стала разработка антифрод-систем по борьбе со спам-звонками, которые отслеживают и блокируют подозрительные банковские операции, совершаемые пользователями, до выяснения всех подробностей транзакции.

В чем проблема такого подхода к борьбе с киберпреступностью? Первый и самый очевидный – это отстающая позиция и наличие временного лага. Сегодня на постоянной основе тестируется огромное количество новых

схем мошеннических действий, цель которых – найти и масштабировать уязвимости системы для максимизации прибыли, полученной незаконной деятельностью. Находиться в отстающей позиции в такой гонке – заведомо проигрышная стратегия, поскольку технологии позволяют масштабировать новую преступную схему за дни, часы или даже минуты. И тут проявляется оборотная стороны технологической системы: она позволяет одинаково быстро масштабировать как позитивные, так и негативные процессы. Подобно волне, новая киберпреступная схема после апробации «накрывает» пользователей по заранее подготовленным каналам. Современные технологии, как, например, спам-рассылка по номерам или в соцсетях, или голосовые помощники, позволяют совершать массовые, масштабные атаки на население. Если речь идет о новой схеме мошенничества, то потенциальная жертва может быть не подготовлена как информационно, так и психологически: к разговору на другом конце провода могут подключаться довольно профессиональные психологи и манипуляторы. Новостные события, вызывающие эмоциональный отклик у больших групп населения, также могут способствовать повышению эффективности мошеннической схемы: потенциальная жертва на фоне страха и тревоги, неопределенности будущего способна совершать нелогичные действия, продиктованные эмоциями, а не здравым смыслом. Это и обуславливает высокую эффективность методов социальной инженерии: управлять человеком в эмоционально нестабильном состоянии гораздо проще и легче.

На социальном уровне противодействие методам социальной инженерии требует долгосрочной и постоянной работы по просвещению населения и повышению его осведомленности в данном вопросе в связке с улучшением антифрод-систем. Финальная цель этих мероприятий – это выработка социального «иммунитета» у всей системы к подобного рода противоправным действиям. Сравнение с иммунитетом здесь не случайно, поскольку такой подход имеет целью обезопасить потенциальный объект

нападения от определенного рода угроз, «вируса», как в моменте, так и в долгосрочной перспективе. В отличие от тактического подхода, такой подход к борьбе с киберпреступностью можно назвать стратегическим.

События последних лет, связанные с ростом киберпреступности и отсутствием системного, эффективного подхода борьбы с ним, поднимают вопрос о пересмотре существующих методов противодействия киберпреступности. Как уже было подробно рассмотрено ранее, сложившаяся ситуация вызывает тревогу и опасность по поводу образа цифрового будущего: с необратимым процессом цифровизации вероятность глобальных киберинцидентов увеличивается. Ответом на подобного рода вызовы и ограниченную эффективность существующих инструментов становится разработка и внедрение новых подходов к обеспечению безопасности систем. Одним из наиболее популярных в последние годы становится кибериммунитет, который определяется как ключевой элемент безопасных умных IT-систем будущего[175], а важность разработки подобных систем отмечается на уровне первых лиц российского государства[176].

Кибериммунитет – это принципиально новый подход к проектированию, разработке и эксплуатации информационных систем, который становится ответом на вызовы со стороны киберпреступного сообщества. Индустрия информационной безопасности существует уже более сорока лет, потребность в пересмотре существующих подходов к обеспечению защиты цифровых систем назрела довольно давно. Ранее в рамках данного параграфа была подробно рассмотрена ограниченность тактического подхода к обеспечению информационной безопасности: отстающий в цифровой гонке всегда проиграет. Вместо этого предлагается

[175] KasperskyOS. Кибериммунитет [Электронный ресурс]. Режим доступа: https://os.kaspersky.ru/technologies/cyber–immunity/ (дата обращения: 06.12.2022).

[176] Рамблер. Мишустин предложил Kaspersky работу над кибериммунитетом в промышленности. [Электронный ресурс]. Режим доступа: https://news.rambler.ru/tech/46756871/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 05.03.2023).

кардинально иной подход, названный кибериммунитетом, который обеспечивает «встроенную» защиту от кибератак[177]. В первую очередь такой подход требует пересмотра сложившихся ценностей, целеполагания, норм и фокуса внимания при разработке новых систем: на первом месте идет безопасность, и только затем ожидаемая польза или выгода от использования технологии. Такой подход существенно отличается от доминирующего сегодня, где потенциальные выгоды нередко имеют первостепенный приоритет.

Технологии остаются мощным драйвером развития бизнеса в самых разных нишах. Сегодня ежегодно запускается большое количество цифровых проектов в образовании, здравоохранении, индустрии развлечений, логистике, финансах, производстве и доставке еды. Отдельно стоит отметить популярную венчурную индустрию, где ключевая задача заключается в запуске и масштабировании своего бизнес-проекта для максимизации прибыли. Немалую роль вносят и ИТ-гиганты: большие корпорации, занимающие доминирующее положение на рынке и предлагающие свои услуги и продукты с использованием мощной системы маркетинга и продаж. Все это создает ложное представление о цифровых продуктах как безопасном инструменте удовлетворения потребностей, однако вся история развития и использования технологий говорит о том, что это совсем не так. Появление новых подходов к разработке цифровых систем – это ответная реакция на сложившееся цифровое мироустройство, которое становится все более рискогенным и опасным. Это план по переустройству сложившегося цифрового ландшафта с фокусом на эффективное противодействие новым, серьезным вызовам со стороны киберпреступного сообщества, минимизации рисков возникновения широкого спектра киберугроз.

---

[177] KasperskyOS. Кибериммунитет [Электронный ресурс]. Режим доступа: https://os.kaspersky.ru/technologies/ (дата обращения: 31.12.2023).

В более глобальном смысле можно говорить о выработке и реализации в долгосрочной перспективе нового подхода к развитию социо-цифровых систем, в котором доминирующую позицию будет занимать минимизация вероятности возникновения и масштабирования реальных и потенциальных киберугроз. Это социально ориентированное развитие цифровых технологий, где приоритет отдается надежности и устойчивости системы, а не попыткам извлечь максимальную пользу. Такой подход можно обозначить как устойчивое цифровое развитие. Аналогии с программой 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.

Устойчивое цифровое развитие – мировой тренд и тема, набирающая актуальность в России. Это отметил[178] директор Российской ассоциации электронных коммуникаций Сергей Плуготаренко во время запуска исследования устойчивого цифрового развития в 2020 году. Возросший интерес к исследованию проблем цифровизации через призму целей устойчивого развития – закономерная и ожидаемая реакция со стороны научного и экспертного сообщества. Цифровые технологии занимают все более значимое место в общественных отношениях, что постепенно трансформирует и способы достижения целей устойчивого развития. И именно цифровые технологии рассматриваются как один из наиболее эффективных инструментов достижения этих целей. Например, достижения исследователей больших данных или искусственного интеллекта находят свое применение в решении проблем изменения климата, ликвидации мирового голода или повышения доступности образования, что напрямую связано с целями устойчивого развития. А пандемия 2020 года поспособствовала росту интереса научного сообщества к исследованию

[178] РАЭК. Запущено исследование устойчивости цифрового развития [Электронный ресурс]. Режим доступа: https://raec.ru/live/raec–news/11462/ (дата обращения: 08.08.2023).

места, возможностей и ограничений цифровых технологий в развитии медицины и сохранения здоровья населения планеты. Помимо глобальных целей ООН, цифровизация и технологии как фактор устойчивого развития исследуются и на уровне организаций и бизнеса. Интерес к данному направлению исследования можно отметить и со стороны российских исследователей[179].

Цели устойчивого развития ООН масштабны и наукоемки по своим характеристикам, что вызывает интерес со стороны научного сообщества и исследователей-практиков. Однако в вопросе применения цифровых технологий для достижения целей устойчивого развития неизбежно возникает вопрос: как интегрировать технологии в процесс достижения целей устойчивого развития таким образом, чтобы максимизировать их пользу и минимизировать вред, не придать всей системе излишнюю хрупкость и рискогенность?

Появление концепции устойчивого цифрового развития – это попытка переосмыслить развитие технологий за последние десятки лет: глобальные кибератаки, угрозы для критической инфраструктуры, рост киберпреступности и ее оформление в полноценную индустрию, проблемы искусственного интеллекта и многое другое. Это привлечение внимания к проблеме дуальности технологий как мощного инструмента достижения целей устойчивого развития и одновременно источника большой опасности для всего населения планеты. Как при такой природе технологий обеспечить безопасное развитие технологий на уровне личности, государства, планеты? Возможно ли это в принципе?

В российском исследовательском сообществе внимание на проблему устойчивого цифрового развития обратили эксперты РАЭК в 2020 году.

[179] Гудкова Т.В., Синицын С.А. Цифровизация как фактор устойчивого развития компании / Т.В. Гудкова, С.А. Синицын // Государственное управление. Электронный вестник. – 2022. – №93. – С. 121 – 132.

Эксперты РАЭК отмечают[180], что 103 из 169 задач целей устойчивого развития достижимы с помощью цифровых технологий, среди которых: хорошее здоровье и благополучие; качественное образование; индустриализация, инновации и инфраструктура; устойчивые города и населенные пункты; борьба с изменением климата; мир, правосудие и эффективные институты.

В своем аналитическом отчете[181] эксперты подчеркивают важность взвешенного, адекватного подхода к цифровизации и информационным технологиям: восторг должен смениться на осознание всех рисков и проблем, в том числе и социальных, которые неразрывно связаны с процессом цифровизации. На пути устойчивого развития общества авторы выделяют следующие группы вызовов цифровой трансформации:

1. Снижение психологического комфорта человека в цифровой среде.
2. Делегирование ответственных решений алгоритмам (ИИ).
3. Потеря гражданами контроля над приватностью.
4. Растущий урон от взлома или отказа цифровых систем ввиду развития связности.
5. Цифровое неравенство.
6. Увеличивающийся экологический след цифровизации.

В качестве плана действий эксперты предлагают решения на трех уровнях: пользователя, компании и государства. Такой многоуровневый план действий – это следствие системности проблемы, для решения которой нужны масштабные и эффективные решения на всех уровнях системы.

Какие ключевые группы решений, по мнению экспертов, способны повысить устойчивость цифрового развития страны?

---

[180] РАЭК. Запущено исследование устойчивости цифрового развития [Электронный ресурс]. Режим доступа: https://raec.ru/live/raec–news/11462/ (дата обращения: 08.08.2023).

[181] РАЭК. Запущено исследование устойчивости цифрового развития [Электронный ресурс]. Режим доступа: https://raec.ru/live/raec–news/11462/ (дата обращения: 08.08.2023).

1. Работа с населением: повышение цифровой грамотности, осведомленности, внедрение практик кибербезопасности, развитие цифровых навыков.

2. Соблюдение компаниями этических норм при разработке и использовании информационных технологий: ответственное и открытое взаимоотношение с клиентами, приоритизация безопасности и учет интересов пользователей.

3. Государство как гарант прав и свобод граждан и главный «архитектор» на пути к устойчивому цифровому развитию: установление правил обращения с персональными данными, международное сотрудничество по обеспечению кибербезопасности, развитие образования и госпрограмм.

Что объединяет все эти решения? Это социально ориентированные действия с конкретным смысловым и ценностным контекстом, которые направлены на всех участников технологического процесса. Это действия, которые для коррекции всей системы предполагают поддержание на длительном промежутке времени общественного взаимодействия с фокусом на технологическую безопасность и устойчивое развитие, на устранение тех проблем, о которых было заявлено ранее. Здесь не перечислены какие–то конкретные шаги и решения, которые могли бы улучшить ситуацию в моменте. Очевидно, что если такие решения и существуют, то они недостаточны. Сама проблема системна, поскольку именно текущее, несовершенное, рискогенное состояние системы породило те вызовы, которые подробно рассматриваются экспертами. Вместо работы с частностями, эксперты в своем исследовании поднялись на более высокий уровень анализа для констатации проблем на макроуровне. Однако помимо конкретного плана и направления действий, важен пересмотр и ценностной составляющей. Крайне важно полностью избавиться от опасной очарованности информационными технологиями: восторг должен смениться

холодным и взвешенным подходом. Технология словно оружие, которое может использоваться как во благо, так и во вред. Причем важно это понимать как конечному пользователю, который является непосредственным объектом негативного воздействия, так и компаниям и государству как реализаторам политики по регулированию развития информационных технологий. Именно на эти важные аспекты обращают внимание эксперты РАЭК в своем докладе.

Переход к устойчивому цифровому развитию – это длительный процесс, который требует серьезного пересмотра сложившегося миропорядка на всех уровнях: международном, государственном, общественном, организационном, личностном. Поскольку в разработку и потребление цифровых продуктов вовлечено большое количество действующих лиц, выпадение какой-либо одной группы сильно снижает конечную эффективность. Например, низкая защищенность программного обеспечения может стать причиной совершения преступных действий даже в отношении самых продвинутых пользователей. С другой стороны, даже самая надежная система может не уберечь неопытного в цифровой среде пользователя, который не отдает отчет совершаемым действиям. Единство проводимой политики по достижению общей цели – одно из ключевых преимуществ устойчивого цифрового развития по сравнению с мерами отдельных субъектов: государства, организаций, гражданских инициатив. Опыт показывает, что последние имеют локальный, ограниченный характер, и в большинстве случаев не приводят к улучшению ситуации в долгосрочной перспективе.

Стоит отдельно отметить, что устойчивое цифровое развитие – это прежде всего пересмотр существующих социальных отношений в процессе производства, распространения и потребления цифровых продуктов. Цифровая технология или устройство – продукт социального взаимодействия, который разрабатывается как инструмент для дальнейшего

использования в общественных отношениях. Вокруг производства и потребления технологического контента возникает большое количество социальных связей и групп интересов: со стороны государства и коммерческого сектора, профессиональных сообществ и гражданского общества, лоббирование со стороны заинтересованных групп. То, какие характеристики примет продукт в своей конечной модификации – это, как правило, результат влияния большого количества групп интересов и результат консенсуса между десятками, сотнями акторов. Это касается и информационной безопасности цифровых систем. Степень защищенности цифрового продукта и уровень его уязвимости – это не случайность, а результат последовательной цепочки социальных действий.

В контексте развития технологий можно выделить три ключевые составляющие, которые стоит подробно рассмотреть в рамках нашего анализа: производители технологий, потребители технологий и контекст их взаимодействия. Рассмотрим каждую составляющую более подробно.

Потребители технологий – ключевой элемент в системе. Именно на них направлена деятельность широкого круга производителей цифровых продуктов и государства. Это огромная масса людей, которые ежедневно пользуются благами прогресса: развлекаются в соцсетях, ищут информацию в поисковиках, совершают покупки в онлайн-магазинах. Сегодня технология – это продукт массового потребления, задача которой – удовлетворение утилитарных потребностей. Цифровые продукты, подобно кино, музыке или искусству, приобретают черты произведения массовой культуры для развлечения и удовлетворения интересов широких масс. Большие ИТ-компании сегодня задают ценности и образцы поведения, характер потребления медиаконтента для выражения своего статуса и положения в обществе, формируют привычки и подталкивают пользователей к закреплению определенных моделей поведения. Многие технологии и продукты прочно укоренились в жизнь современного человека, а отказ от них

воспринимается как серьезный урон качеству жизни, нередко с проявлением синдрома отмены. В такой реальности человек нередко теряет свою субъектность, выступает аморфной целью для производителей цифровых продуктов, которого необходимо «накормить» своей продукцией или услугами. Жизнь современного человека нередко напоминает бесконечную погоню за мнимыми ценностями для подтверждения своего статуса: покупка продукции компании Apple, просмотр и обсуждение с друзьями популярных сериалов в Netflix, создание личного бренда в соцсетях. Компании-производители предлагают широкий выбор однотипных по своей сути способов удовлетворения потребностей в статусности, одобрении со стороны общества, досуга. Человек принимает пользование такими услугами как что-то должное, зачастую перекладывая ответственность с себя на других, в том числе и за свою безопасность. Современный человек готов совершать действия, потреблять, но не нести за это ответственность, отстраняться при возникновении вопроса об обязанностях за совершаемые действия. В этой связи неудивительно, например, что при высоком уровне цифровизации в России сохраняется довольно низкий уровень цифровой грамотности[182]. Такой подход деструктивен, в том числе и с позиций информационной безопасности. Отсутствие критического мышления, осмотрительности, образованности и грамотности в области цифровых технологий создают благоприятные условия для манипулирования пользователем с целью совершения в отношении него противоправных деяний. Отказ от субъектности и отстаивания собственных интересов в угоду удовлетворения навязанных потребностей – опасная черта современного развитого общества. Но если раньше, в эпоху массовой культуры кино, искусства, спорта, данная проблема носила ограниченный характер и интересовала в основном профессиональное сообщество, то теперь, в эпоху массовых технологий,

[182] НАФИ. Уровень цифровой грамотности в России и Беларуси. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/uroven–tsifrovoy–gramotnosti–v–rossii–i–belarusi/ (дата обращения: 07.03.2023).

такая проблема касается каждого, кто имеет доступ в Интернет: киберпреступность вездесуща, и ее инструменты направлены на массового потребителя.

Какими могут быть шаги по решению данной проблемы для перехода к устойчивому цифровому развитию? Прежде всего – это обретение и осознание субъектности потребителями цифровых услуг. Гармоничное развитие невозможно без проявления обратной связи и ее учета при совершении последующих действий. На примере больших социальных систем, будь то государства или корпорации, можно проследить, к чему приводит игнорирование или замалчивание обратной связи со стороны значимой части системы. Подобное правило применимо и к цифровому развитию: сбалансированное, устойчивое развитие невозможно без выражения потребителями технологий обратной связи и учета этой связи производителями. Дисбаланс в этом взаимодействии технологического и социального довольно часто приводит к негативным последствиям: новые технологии или продукты, неадаптированные под возможности пользователей, несут опасность возникновения и развития киберинцидентов. Одна из ключевых задач концепции устойчивого цифрового развития и заключается в создании таких благоприятных долгосрочных условий, которые обеспечат баланс между социальным и технологическим для максимизации полезности и минимизации возможных рисков. Но как обеспечить максимальную подготовленность социальной составляющей социо-цифровой системы?

Здесь важно еще раз подчеркнуть, что проблема киберпреступности носит системный, массовый характер. Любая незамкнутая система, имеющая какое-либо взаимодействие с внешним миром, является потенциальной целью киберпреступного сообщества. На основании этого был сделан важный вывод о том, что с системной проблемой можно бороться только системными, комплексными мерами, используя стратегический подход к

решению проблемы киберпреступности. Но какие меры в долгосрочной перспективе способны установить и поддерживать баланс между технологическим и социальным?

Ключевую роль на пути к становлению устойчивого цифрового развития играет массовое и профессиональное образование. Уровень образования и человеческий капитал становятся важными факторами не только с точки зрения экономического, но и технологического благополучия. В вопросе развития человеческого капитала с позиций устойчивого цифрового развития рассмотрим два направления: массовое и профессиональное образование.

Профессиональное образование направлено на подготовку кадров высшей категории – лидеров цифровых трансформаций будущего и настоящего. Этот процесс включает в себя отбор и развитие наиболее талантливой молодежи для государственного и коммерческого сектора, науки и образования. В последние десятки лет можно отчетливо наблюдать глобальный тренд на создание благоприятных условий для молодых и перспективных ИТ-специалистов. За высококвалифицированные кадры борьба происходит сразу на нескольких уровнях: на уровне государств, компаний, вузов, исследовательских центров. Проигрыш в такой гонке может быть опасен как с точки зрения зависимости от иностранной продукции, так и технологической деградации существующей инфраструктуры, что нередко ведет к повышению ее уязвимости с точки зрения киберугроз.

В контексте подготовки и удержания талантливых специалистов, создания благоприятных условий для их дальнейшей деятельности в интересах внутренней экономики, события 2022 года в России вызывают особую озабоченность. С точки зрения миграционного оттока 2022 год

оказался одним из наиболее заметных в истории современной России[183]. Так, по официальным заявлениям российских властей только за 2022 год страну могли покинуть до 10 процентов ИТ-специалистов[184]. Негативные последствия данного события имеют отложенный эффект. Покидают страну или увольняются из российских компаний наиболее квалифицированные кадры, которые без особых сложностей находят работу на зарубежные компании, тем самым инвестируя свои таланты на экономику других стран. Такие специалисты – это и есть экспертная и профессиональная основа для будущего технологического развития нашей страны, которая в настоящий момент активно теряется и переориентируется на другие страны в силу происходящих с февраля 2022 года обстоятельств. Это не означает кризис на рынке подбора ИТ-специалистов в моменте, однако формирует устойчивый негативный тренд: высококвалифицированные кадры нередко заменяются начинающими специалистами. В долгосрочной перспективе такие процессы способны оказывать серьезное деструктивное влияние на технологическое развитие государства, поскольку серьезно нарушается преемственность поколений специалистов: хорошие специалисты редко являются самоучками, для их подготовки требуется серьезная образовательная база.

Российская образовательная база испытывает сложности и в связи с уходом западных компаний и санкций в отношении российской науки. Здесь важно отметить, что современный мир построен на глобальной кооперации, разделении труда и сотрудничестве. Исключение из глобальных процессов неминуемо ведет к изоляции и технологическому отставанию: этот процесс можно наблюдать на примере стран, долгие годы находящихся под санкциями. Отсутствие возможности использовать мировые достижения и

[183] Швыряев П.С. Кадровая обеспеченность в сфере информационных технологий в России: проблемы и перспективы / П.С. Швыряев // Государственное управление. Электронный вестник. – 2023. – № 97. – С. 231–240.

[184] ТАСС. Шадаев заявил, что порядка 100 тыс. IT–специалистов покинули Россию с начала года. [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/16639651 (дата обращения: 08.03.2023).

опыт, привлекать лучших преподавателей и специалистов ведет к технологической деградации: упрощаются технологические процессы и выпускаемая продукция, уровень надежности и защищенности систем падает.

В этой связи неминуемо страдает и качество подготовки новых специалистов. В сфере подготовки российских ИТ-специалистов сложился тренд на все большую коммерциализацию данного вида образовательной деятельности: профессиональные учебные заведения заменяются онлайн-школами, использующими агрессивный маркетинг для продажи своих услуг. Большинство таких курсов – низкокачественный продукт из-за невозможности на потоке находить хороших преподавателей, а зачастую и отсутствия цели сделать обучение более качественным[185]. Как итог, на рынок выходит большое количество плохо подготовленных, низкоквалифицированных соискателей, которые заменяют собой опытных специалистов.

Власти России, понимая сложность ситуации, готовят целые программы по возвращению уехавших специалистов[186]. Однако общий тренд очевиден: отток квалифицированных кадров в сфере информационных технологий сегодня приобретает угрожающие черты не столько для настоящего, сколько для будущего нашей страны. События 2022 года – лишь сконцентрированный, яркий отрезок того процесса, который протекает уже десятки лет в российском государстве. Стоит отметить, что предпринимаемые российскими властями меры имеют ограниченный эффект. Их можно охарактеризовать скорее как адаптацию под новые вызовы и возникающие проблемы, а не план по изменению тренда и переориентации

[185] Газета.ru. «Отсрочка от реальной работы»: можно ли заработать в IT после онлайн–курсов. [Электронный ресурс]. Режим доступа: https://www.gazeta.ru/tech/2021/07/31/13815866/it_courses.shtml (дата обращения: 09.03.2023).

[186] Forbes. Метод кнута и пряника: как вернуть IT–специалистов в Россию. [Электронный ресурс]. Режим доступа: https://www.forbes.ru/tekhnologii/481417–metod–knuta–i–pranika–kak–vernut–it–specialistov–v–rossiu (дата обращения: 08.03.2023).

его в выгодном для страны направлении. Такие инструменты можно рассматривать как попытку улучшить ситуацию в моменте, но не как долгосрочный план по выращиванию и удержанию талантливых специалистов внутри страны для их плодотворной и эффективной работы на благо отечественной экономики. Естественно, в течение всей истории современной России такие планы провозглашались и в той или иной мере реализовывались в нашей стране, однако к 2023 году с точки зрения обеспеченности ИТ-кадрами мы подходим в весьма тревожном положении: по заявлениям властей, российской экономике не хватает до 1 миллиона ИТ-специалистов[187]. Решать сложившуюся проблему власти собираются в том числе через реформы в сфере высшего образования, однако и тут есть немало важных нюансов.

Высшие учебные заведения и исследовательские центры – важная составляющая на пути к устойчивому цифровому развитию. На протяжении многих столетий университеты остаются центром притяжения и развития талантливой молодежи, кузницей идей и научных прорывов, местом подготовки профессиональных кадров. В вопросах обеспечения технологического благополучия важно создавать условия для развития и масштабирования научно-образовательных центров. Согласно актуальным рейтингам, ведущими университетами мира остаются западные учебные заведения, прежде всего США и Европы. Ключевыми качествами таких университетов можно назвать автономность в проводимой политике; определенную степень независимости от государства; развитые системы связи и обмена опытом с другими университетами, коммерческими компаниями; создание условий для работы лучших специалистов и преподавателей; большие бюджеты на НИОКР.

[187] РБК. Дефицит ИТ–мозгов: как Россия решает проблему кадрового голода в отрасли // РБК [Электронный ресурс]. Режим доступа: https://www.rbc.ru/economics/28/07/2022/62e12c929a794747597da279 (дата обращения: 04.05.2023).

Усиление тренда на практикоориентированность образовательных программ высшего образования – это одновременно институциональная реакция на запрос работодателей, рынка труда[188]. Российская система высшего образования в сфере подготовки ИТ-кадров остается консервативной, недостаточно мобильна и гибка, работает не на рынок труда[189]. Свой негативный вклад в развитие российского профессионального образования внесут и события 2022 года. Международные санкции, введенные в отношении российской науки и образования, способны негативным образом повлиять на уровень подготовки профессиональных кадров на долгосрочном горизонте. Здесь важно подчеркнуть, что наука и образование – это те области человеческой деятельности, в которых особое значение имеют кооперация и сотрудничество, обмен опытом, знаниями и технологиями, в том числе и на международном уровне. Отказ от сотрудничества с наиболее прогрессивными технологическими странами и переориентация на «дружественные» страны могут иметь свои долгосрочные негативные последствия, весь масштаб и глубину которых можно оценить только с течением времени. Тем не менее, такой процесс переориентации уже сейчас вызывает особую озабоченность.

Теперь рассмотрим массовое образование и просвещение населения в области цифровой грамотности и безопасности – еще один важный пункт на пути к устойчивому цифровому развитию. Уровень цифровой грамотности населения самым прямым образом связан с уровнем киберпреступности[190]. Потребители цифровых продуктов и услуг зачастую и оказываются наименее

---

[188] Зубок Ю. А., Селиверстова Н. А. Представления молодежи о будущем страны в проекции культуры / Ю.А. Зубок, Н.А. Селиверстова // Наука. Культура. Общество. 2023. Т. 29, № 3. С. 39–52.

[189] Климова Ю.О. Проблемы подготовки кадров в сфере информационных технологий / Ю.О. Климова// Проблемы развития территории. – 2020. – №6 (110). – С. 86–105.

[190] Forbes. Эксперты назвали низкую цифровую грамотность россиян причиной роста киберпреступности. [Электронный ресурс]. Режим доступа: https://www.forbes.ru/tekhnologii/455881–eksperty–sprognozirovali–rost–userba–ot–kiberprestupnosti–v–rossii–do–165–mlrd–rublej (дата обращения: 06.05.2023).

защищенным элементом системы, целью для кибермошенников. Интернет-пользователи – наиболее массовый сегмент всей цифровой системы, по состоянию на апрель 2022 года преодолевший отметку в 5 миллиардов человек[191]. Состояние данного сегмента в контексте цифровой грамотности как уровень подготовленности и противостояния возможным киберугрозам – еще одна важная составляющая устойчивого цифрового развития. Здесь еще раз важно подчеркнуть, что создание цифровых продуктов – прерогатива лишь малой, наиболее продвинутой части населения. Однако использование этих продуктов доступно подавляющей части населения. Аудитории наиболее популярных интернет-сервисов неуклонно растут и переваливают за миллиард пользователей. Такие сервисы уже давно имеют межгосударственный, планетарный масштаб, а их пользователи имеют самый разный социальный статус, образование, в том числе и уровень цифровой грамотности. Высокий уровень цифровой грамотности населения – одна из ключевых основ устойчивого цифрового развития. По аналогии со всеобщим обязательным образованием, программа по повышению цифровой грамотности и образованности населения должна быть одной из ключевых задач современного, технологически развитого государства. Данный постулат отражен и в обновленной Концепции внешней политики РФ от 31 марта 2023 года: одним из национальных интересов РФ провозглашено содействие устойчивому развитию российской экономики на новой технологической основе[192]. Несмотря на очевидную важность данного вопроса для технологического развития и процветания страны, многочисленные заявления экспертов и государственных лиц, в России цифровая грамотность населения остается все еще на невысоком уровне.

[191] DataReportal. Digital 2022 April Global Statshot. [Электронный ресурс]. Режим доступа: https://datareportal.com/reports/digital–2022–april–global–statshot (дата обращения: 06.05.2023).

[192] Указ Президента РФ от 31 марта 2023 г. N 229 «Об утверждении Концепции внешней политики Российской Федерации". [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_443540/ (дата обращения: 18.06.2023).

Ежегодные исследования НАФИ показывают, что цифровая грамотность населения России растет в последние 4 года довольно медленными темпами[193] относительно общего уровня цифровизации. Особое внимание заслуживает вывод исследователей о том, что россияне до сих пор не осознают важность умения защищать свои персональные данные. А персональные данные сегодня – ключевая информация для киберпреступников, которая позволяет найти более грамотный и тонкий подход к потенциальной жертве и повысить эффективность мошеннической схемы. Результаты исследования также подсвечивают и слабые стороны в общем уровне цифровой грамотности населения страны. Так, к наименее защищенным слоям населения можно отнести россиян старшего возраста (55 лет и старше), неработающих пенсионеров, жителей небольших городов и сел[194]. Суммарно данная аудитория насчитывает десятки миллионов граждан страны. Это значительная часть населения, которая особенно сильно может быть подвержена атакам со стороны киберпреступников.

Но могут ли себя ощущать в безопасности остальные категории граждан? Например, технологически продвинутая молодежь или люди средних лет? Как показывают результаты исследований, нет. Так, согласно исследованию банка ВТБ[195], чаще всего жертвами мошенников становятся мужчины в возрасте от 35 до 39 лет. И это вполне ожидаемо: деятельность мошенников направлена прежде всего на социально активных граждан со средним и высоким уровнем достатка. Несмотря на то, что мужчины

[193] НАФИ. В России выросла доля людей с продвинутым уровнем цифровой грамотности. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/v–rossii–vyrosla–dolya–lyudey–s–prodvinutym–urovnem–tsifrovoy–gramotnosti/ (дата обращения: 06.05.2023).
[194] НАФИ. В России выросла доля людей с продвинутым уровнем цифровой грамотности. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/v–rossii–vyrosla–dolya–lyudey–s–prodvinutym–urovnem–tsifrovoy–gramotnosti/ (дата обращения: 06.05.2023).
[195] РБК. ВТБ описал типичную жертву финансовых мошенников. [Электронный ресурс]. Режим доступа: https://www.rbc.ru/society/23/06/2021/60d1cd2c9a7947cd10c61ba3 (дата обращения: 07.05.2023).

демонстрируют более высокий уровень цифровой грамотности[196], это не мешает им оказываться в числе наиболее частых жертв мошенников. Приведенные выше результаты наталкивают на выводы о том, что, во-первых, никто не может ощущать себя в полной мере защищенным от киберпреступников. Установка продвинутого антивируса или прохождение спецкурсов по информационной безопасности не должны создавать ложных иллюзий о полной и долгосрочной защищенности от мошенников. Даже самые продвинутые системы не спасают от банальной человеческой глупости или невнимательности под воздействием психологического давления или нестабильного внешнего информационного фона.

Все эти размышления наталкивают на мысль о том, что в вопросах цифровой грамотности и образованности российскому государству и населению предстоит проделать еще немало работы. Ключевая задача здесь видится в построении образовательных систем с ориентацией на новый технологический уклад. Причем как для детей, так и для взрослого населения. Сегодня необходимо решать проблему защищенности не только взрослого населения, на которое в основной своей массе направлена деятельность киберпреступников, но и подрастающего поколения, которое спустя некоторое время станет основной целью мошенников. Опросы населения показывают, что запрос на повышение цифровой грамотности среди россиян есть и он существенный: 74% россиян выражают готовность повышать свои знания в областях, связанных с цифровыми финансовыми услугами и их безопасным использованием[197]. Но каковы возможности для претворения этой готовности в реальные действия?

---

[196] НАФИ. В России выросла доля людей с продвинутым уровнем цифровой грамотности. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/v–rossii–vyrosla–dolya–lyudey–s–prodvinutym–urovnem–tsifrovoy–gramotnosti/ (дата обращения: 06.05.2023).

[197] НАФИ. НАФИ провел первый замер Индекса цифровой финансовой грамотности жителей России. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/nafi–provel–pervyy–zamer–indeksa–tsifrovoy–finansovoy–gramotnosti–zhiteley–rossii/ (дата обращения: 08.05.2023).

На наш взгляд, главным проводником на пути к построению устойчивого цифрового развития должно оставаться государство. Именно оно, имея серьезный административный и финансовый ресурс, способно реализовывать проекты в масштабах всей страны, нацеленные на большие группы граждан. В рамках российского государства задача по повышению информированности и кибербезопасности россиян реализуется в рамках федерального проекта «Информационная безопасность». Так, начиная с 2022 года, на реализацию программы по повышению цифровой грамотности россиян будет ежегодно выделяться по 200 миллионов рублей[198]. Стоит отметить, что для страны, население которой составляет более 140 миллионов человек, такие суммы, выделенные на просветительскую и образовательную деятельность, выглядят более чем скромными. Если допустить, что объектом данной программы является население России старше 14 лет, то на каждого потенциального адресата данной просветительской деятельности заложено меньше 2 рублей. Это малые суммы, которые исключают возможность проведение рекламной кампании в масштабах всей страны. События 2022-2023 годов с активной рекламной кампанией службы по контракту показывают, что необходимые возможности у российского государства есть, вопрос лишь в приоритетах.

Особое внимание вызывают планы по сокращению бюджета по нацпроекту «Цифровая экономика» в 2023 году на треть[199]. С одной стороны, здесь отчетливо прослеживается влияние санкционного давления, с которым и связывается сокращение финансирования в ряде федпроектов[200]. Вызывают обеспокоенность и планы по сокращению таких важных направлений

---

[198] Официальный сайт Правительства РФ. Правительство поддержит разработку программы для повышения цифровой грамотности. [Электронный ресурс]. Режим доступа: http://government.ru/news/44479/ (дата обращения: 08.05.2023).

[199] Ведомости. Расходы на «Цифровую экономику» и «Международную кооперацию» снизят почти на треть в 2023 году. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/economics/articles/2022/09/27/942639–rashodi–na–tsifrovuyu–ekonomiku (дата обращения: 08.05.2023).

[200] Там же.

цифрового развития страны, как «инфраструктура», «цифровые технологии», «искусственный интеллект», «кадры для цифровой экономики»[201]. Увеличение бюджета федпроекта «Информационная безопасность» на 7,2%, до 7,9 млрд рублей, может быть недостаточным и несопоставимым с тем масштабом проблемы, которая сложилась в России в последние годы. Важность информирования граждан по данному вопросу подчеркивается и Президентом страны[202], однако финансирование данной программы и масштаб ее реализации все еще имеют серьезный потенциал к росту как с точки зрения охвата аудитории, так и качества и глубины проработки материала, его адаптации к постоянно меняющимся преступным схемам.

Особую роль в противодействии киберпреступности в России занимает банковский сектор. В последние годы банковская инфраструктура и ее пользователи стали одним из главных объектов атак. Банки, аккумулируя в себе огромные финансовые ресурсы, а также конфиденциальную информацию граждан и организаций, находятся под постоянным давлением и проверкой на прочность со стороны преступного мира. В России банковский сектор в лице прежде всего крупнейших банков страны сформировал уникальный и разносторонний опыт противодействия мошенническим действиям. С целью повышения уровня защиты критической инфраструктуры на постоянной основе проводятся масштабные киберучения, которые охватывают всех сотрудниках на всех уровнях управления[203]. Помимо внутренних учений, нельзя не отметить растущую популярность межведомственных киберполигонов. Это, безусловно,

---

[201] Интерфакс. Бюджет нацпрограммы "Цифровая экономика" в 2023 году предложено сократить на 35%. [Электронный ресурс]. Режим доступа: https://www.interfax.ru/business/865340 (дата обращения: 22.05.2023).

[202] РИА Новости. Путин прокомментировал рост киберпреступности. [Электронный ресурс]. Режим доступа: https://ria.ru/20230320/kiber–1859136636.html (дата обращения: 22.05.2023).

[203] Ведомости. Банки активизировали проведение киберучений в прошлом году. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/finance/articles/2023/02/16/963166–banki–aktivizirovali–provedenie–kiberuchenii (дата обращения: 29.05.2023).

позитивный тренд, направленный на укрепление взаимодействия между различными организациями в вопросах информационной безопасности. Таким образом, российский банковский сектор сегодня выступает флагманом в борьбе с киберпреступностью, одним из ведущих центров экспертизы по противодействию незаконным действиям с использованием информационных технологий. Столкнувшись с масштабным ростом кибератак за последние несколько лет, банковскому сектору удалось достойно ответить на новый вызов технологической эпохи и адаптироваться к новым экстремальным условиям. Такая экспертиза может быть полезна в том числе и в других областях и сферах как коммерческой, так и некоммерческой деятельности. В этой связи совместные учения и обмен знаниями между организациями можно только поддержать и надеяться на дальнейшее развитие данного сотрудничества не только в пределах страны, но и с коллегами по информационной безопасности из «дружественных» стран.

Лидирующую роль в процессе укрепления банковской инфраструктуры и просвещения граждан сегодня занимает Банк России. Именно со стороны этого органа власти исходят предписания для банковского сектора по повышению уровня информационной безопасности и оповещению граждан. Вместе с тем важно подчеркнуть, что противодействие киберпреступности – это комплексная, всесторонняя работа, которая требует полной вовлеченности всех участников. Попытки перекладывания ответственности или отстранения в данном вопросе контрпродуктивны. На наш взгляд, как уже неоднократно подчеркивалось ранее, государство в построении устойчивого цифрового развития занимает лидирующую, смыслообразующую роль. Только через глубокое понимание феномена киберпреступности, технологических и информационных рисков, особенностей взаимодействия человека и цифровых объектов, социальной и технической части, возможен переход к устойчивому цифровому развитию.

Можно ли сегодня говорить о том, что в нашей стране на уровне общественности и власти сформировалось правильное, рациональное восприятие технологического развития с фокусом на безопасность и защищенность всей социо-цифровой системы? Можно ли говорить о том, что российский технологический сектор взял полноценный курс на устойчивое цифровое развитие? На наш взгляд, говорить об этом еще рано. Безусловно, нельзя не отметить рациональные, эффективные шаги в данном направлении, которые в последнее время особенно часто исходят от банковского сектора. Однако в целом ситуация на текущий момент все еще остается неразрешенной.

В настоящее время в России реализуются сложные, масштабные проекты по цифровизации самых разных областей общественной жизни. Безусловно, это важные и нужные шаги по переходу к новому технологическому укладу нашего общества. Однако прошлый опыт показывает, что спешка и необдуманные решения в этом вопросе губительны. Например, вектор на разработку единых цифровых баз граждан содержит в себе не только потенциальные бонусы, но и огромные риски. Проектирование и реализация таких сложных цифровых систем могут быть небезопасными в условиях сжатых сроков и внешнего давления. Зачастую именно в таких условиях вопросы безопасности и кибериммунитета всей системы отходят на второй план или вовсе упрощаются. Плохо протестированные, ненадежные и необкатанные системы – это огромный риск для всей глобальной социо-цифровой системы. Так, уязвимости в единой базе данных граждан могут быть использованы как для компрометации данных граждан и их дальнейшего использования в преступных целях, так и для несанкционированного доступа к другим базам и системам. Такая уязвимость в рамках одного узла системы способна вызвать цепную реакцию, эффект которой был подробно рассмотрен в рамках данного параграфа.

Большую опасность таит и принудительная цифровизация, которая зачастуют и создает тот самый дисбаланс между темпами технологического развития и возможностями социальной системы к со-конструированию в новых реалиях. Одним из направлений восстановления нарушенного баланса может стать процесс децифровизации, предложения о которой высказываются ведущими специалистами в области информационной безопасности России[204].

Не менее важной проблемой остается низкий уровень цифровой грамотности населения. Глобально можно говорить о становлении новой формы неравенства и поляризации на основе цифровой грамотности и образованности, которая чревата разного уровня рисками. По всей видимости, данная проблема постепенно вытеснит «классическую» проблему цифрового неравенства, связанную с доступностью сети: уровень проникновения Интернета постоянно растет, как и количество пользователей по всему земному шару. Такие пользователи сталкиваются со все более усложняющимся технологическим миром, который представляют особую опасность для такого сегмента пользователей. На другом «полюсе» мы имеем продвинутое меньшинство – производителей технологических решений и наиболее прогрессивных пользователей цифровых систем. Как адаптировать и подготовить постоянно отстающее большинство к непрерывно меняющимся условиям технологического уклада – вопрос актуальный и открытый.

Таким образом, стратегия устойчивого цифрового развития включает следующие основные направления, которые имеют прежде всего социальную, а не техническую ориентацию, и направлены на формирование в интересах общества, бизнеса и государства отсутствующего в настоящий

[204] Интерфакс. Наталья Касперская заявила о необходимости децифровизации предприятий для защиты от кибератак [Электронный ресурс]. Режим доступа: https://www.interfax.ru/digital/872493 (дата обращения: 17.12.2023).

момент динамического баланса между темпами технологического развития и возможностями социальной системы.

1. Ценностная переориентация на новый 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.

Схема эффективной стратегии противодействия киберпреступности должна включать следующие пункты[205]:

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.

6. Ресурсы, которые необходимы для выполнения этих задач.

7. Ожидаемые результаты и инструменты оценки.

Рост киберпреступности в России и мире в последние несколько лет послужил поводом обратить внимание на проблему киберпреступности. Сегодня опасность и важность проблемы киберпреступности подчеркивается на самом высоком уровне[206]. Осознание серьезности ситуации среди первых лиц государства – начальная точка для стабилизации ситуации.

В сентябре 2022 указом президента РФ в структуре МВД было создано управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий. Среди основных задач Управления выделены: предупреждение, выявление, пресечение и раскрытие преступлений и иных правонарушений в сфере IT-технологий, а также координация этой деятельности в системе МВД России; анализ данных,

[205] Управление 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).

[206] РИА Новости. Путин прокомментировал рост киберпреступности. [Электронный ресурс]. Режим доступа: https://ria.ru/20230320/kiber–1859136636.html (дата обращения: 12.06.2023).

содержащихся в информационно-телекоммуникационных сетях, в целях выявления запрещенного контента и противодействия преступности; организация взаимодействия подразделений органов внутренних дел РФ с государственными органами, органами государственной власти субъектов, учреждениями финансово-кредитной системы, организациями информационно-коммуникационной сферы, иными участниками и информационного обмена, включая агрегаторы больших данных[207].

Противодействии киберпреступности – важное направление государственной деятельности не только в России, но и в западных странах. В указе[208] президента США от 30 октября 2023 года провозглашается новый подход к разработке и использованию искусственного интеллекта, основанный на приоритете безопасности и надежности. Данный документ представляет собой долгосрочный план по содействию исследований и разработок в области искусственного интеллекта с фокусом на интересы общества с лидирующей ролью государства как гаранта интересов граждан.

Вопросами безопасного технологического развития озабочены европейские и развивающиеся страны. О необходимости консолидации международных усилий по изучению искусственного интеллекта и построению безопасного цифрового будущего было заявлено в Декларации Блэтчли, опубликованной по итогам саммита по проблемам безопасного использования искусственного интеллекта в ноябре 2023 и поддержанной несколькими десятками наиболее развитых и развивающихся стран мира[209].

---

[207] Интерфакс. В МВД РФ создадут Управление по организации борьбы с киберпреступлениями [Электронный ресурс]. Режим доступа:https://www.interfax.ru/russia/865726 (дата обращения: 24.12.2023).

[208] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence [Электронный ресурс]. Режим доступа: https://www.whitehouse.gov/briefing–room/presidential–actions/2023/10/30/executive–order–on–the–safe–secure–and–trustworthy–development–and–use–of–artificial–intelligence/ (дата обращения: 06.01.2024).

[209] The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 November 2023 [Электронный ресурс]. Режим доступа: https://www.gov.uk/government/publications/ai–safety–summit–2023–the–bletchley–declaration/the–bletchley–declaration–by–countries–attending–the–ai–safety–summit–1–2–november–2023 (дата обращения: 06.01.2024).

Успехи в области противодействия онлайн-мошенничеству можно отметить у Центрального Банка России. В ЦБ РФ разработана собственная система мониторинга, которая в 2022 году выявила 4964 субъекта с признаками нелегальной деятельности, в том числе с признаками финансовых пирамид, что на 85% больше по сравнению с 2021 годом[210]. Большинство таких субъектов действовало в сети Интернет.

Также важной мерой на пути противодействия кибермошенникам стала введенная с 1 октября 2022 года возможность добровольно ограничить или наложить полный запрет на онлайн-операции в банке, в котором обслуживается гражданин[211]. Помимо этого, для дополнительной защиты клиентов от действий кибермошенников с 1 октября 2022 года банки обязаны проводить идентификацию всех устройств, с которых граждане совершают онлайн-операции, подтверждать их телефонные номера и адреса электронной почты[212].

Масштабная работа ведется и в рамках Стратегии повышения финансовой грамотности[213] на 2017-2023 гг., которая включает в том числе меры по противодействию мошенникам в Интернет-среде за счет повышения финансовой грамотности населения и формирования финансовой культуры. В Банке России отмечают[214], что благодаря реализации Стратегии удалось сформировать по всей стране методологическую базу и образовательную

---

[210] Банк России.Противодействие нелегальной деятельности на финансовом рынке [Электронный ресурс]. Режим доступа: https://www.cbr.ru/analytics/inside/2022/ (дата обращения: 24.12.2023).

[211] Банк России. Клиенты банков смогут добровольно ограничивать онлайн–операции для защиты от мошенников [Электронный ресурс]. Режим доступа: https://cbr.ru/press/event/?id=13971 (дата обращения: 24.12.2023).

[212] Интерфакс. Клиенты банков с 1 октября могут ограничивать онлайн–операции для защиты от мошенников [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/15927795 (дата обращения: 24.12.2023).

[213] Банк России. Распоряжение от 25 сентября 2017 г. № 2039–р. [Электронный ресурс]. Режим доступа: https://cbr.ru/Content/Document/File/59796/Inf_note_dec_2718.pdf (дата обращения: 24.12.2023).

[214] Банк России. Правительство России утвердило Стратегию повышения финансовой грамотности и формирования финансовой культуры до 2030 года [Электронный ресурс]. Режим доступа: https://www.cbr.ru/press/event/?id=17155 (дата обращения: 24.12.2023).

инфраструктуру, создать специальные информационные ресурсы. В 2023 году была утверждена новая Стратегия до 2030 года, которая включает в себя дальнейшие меры по развитию финансовой культуры жителей России, в том числе для формирования иммунитета и противодействию кибермошенничеству: внедрение новых образовательных программ и продуктов для разных аудиторий, обучение финграмотности всех школьников и студентов среднего профессионального образования, создание центров финансовой грамотности во всех регионах страны, дальнейшее развитие волонтерских движений и иные меры[215].

Таким образом, нельзя не отметить конкретные шаги в нужном направлении по борьбе с киберпреступностью в России. Однако предстоит проделать еще много работы для выработки и последующей реализации системной, долгосрочной стратегии противодействию киберпреступности.

[215] Банк России. Правительство России утвердило Стратегию повышения финансовой грамотности и формирования финансовой культуры до 2030 года [Электронный ресурс]. Режим доступа: https://www.cbr.ru/press/event/?id=17155 (дата обращения: 24.12.2023).

Заключение

В разработанной в диссертационном исследовании методологической перспективе предложена постановка вопроса о принципиально новой стратегии противодействия киберпреступности на основе решения более широкой задачи – перехода к устойчивому цифровому развитию как основе комплексного и долговременного решения проблемы киберпреступности.

Устойчивое цифровое развитие может стать ответом на запрос со стороны общества на приоритет безопасности и надежности цифровизацизационных процессов, ориентацию прежде всего на социальную ответственность в вопросах технологического 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 – установления нарушенного в настоящий момент баланса между технологическим и социальным и его дальнейшее поддержание за счет мер упреждающего, стратегического характера.

Однако существуют 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.

События пандемии и нарастания геополитической напряженности показали жизненную необходимость поиска, обретения и поддержания баланса между технологическим и социальным. Перекос в одну из сторон грозит нарастанием напряженности в цифровом пространстве, повышением технологических рисков и ростом киберпреступной активности. Гармоничное технологическое развитие, где киберпреступность не является угрозой планетарного масштаба, видится в установлении этого баланса. Однако важно это понимать не только на уровне экспертного и научного сообщества, но и на уровне лиц, принимающих решения, политического руководства стран и международных объединений. Безопасность сегодня должна быть безусловным приоритетом в процессе технологического развития, и важно это не только провозглашать, но и реализовывать на практике. Дальнейшее исследование проблемы киберпреступности и выработки эффективных подходов противодействия, проведение регулярных, мониторинговых исследований – один из приоритетов социальных наук на ближайшие десятилетия.

Список литературы

Нормативно-правовые акты

1. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями.
2. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 30.07.2023).
3. Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно–коммуникационных технологий в преступных целях от 29.06.2021 [Электронный ресурс]. Режим доступа: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_–_R.pdf (дата обращения: 17.07.2023).
4. Проект Концепции стратегии кибербезопасности Российской Федерации [Электронный ресурс]. Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 30.11.2023).
5. Резолюция, принятая Генеральной Ассамблеей ООН 6 июля 2017 года [Электронный ресурс]. Режим доступа: https://ggim.un.org/documents/A_Res_71_313_r.pdf (дата обращения: 09.07.2023).
6. Указ о национальных целях развития России до 2030 года [Электронный ресурс]. Режим доступа: http://kremlin.ru/events/president/news/63728 (дата обращения: 09.07.2023).
7. Указ Президента РФ от 31 марта 2023 г. N 229 «Об утверждении Концепции внешней политики Российской Федерации". [Электронный ресурс]. Режим доступа:

https://www.consultant.ru/document/cons_doc_LAW_443540/ (дата обращения: 18.06.2023).

8. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149–ФЗ (последняя редакция) [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.07.2023).

9. Федеральный закон "О персональных данных" от 27.07.2006 N 152–ФЗ (последняя редакция) [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 30.07.2023).

10. Федеральный закон "О техническом регулировании" от 27.12.2002 N 184–ФЗ (последняя редакция) [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_40241/ (дата обращения: 30.07.2023).

11. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence [Электронный ресурс]. Режим доступа: https://www.whitehouse.gov/briefing–room/presidential–actions/2023/10/30/executive–order–on–the–safe–secure–and–trustworthy–development–and–use–of–artificial–intelligence/ (дата обращения: 06.01.2024).

Монографии и коллективные источники

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

13. Кнорр–Цетина К. Социальность и объекты. Социальные отношения в постсоциальных обществах знания // Социология вещей: Сб. статей / Под ред. В. Вахштайна. М.: ИД «Территория будущего». – 2006. – 392 с.

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

15. Оценка цифровой готовности населения России [Текст] : докл. к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / Н. Е. Дмитриева (рук. авт. кол.), А. Б. Жулин, Р. Е. Артамонов, Э. А. Титов; Нац. исслед. ун–т «Высшая школа экономики». – М. : Изд. дом Высшей школы экономики, 2021. – 86 С.

16. Судас Л.Г. Управленческие императивы Индустрии 4.0 / Л.Г. Судас, М.А. Юдина. – М.: Издательство Московского университета, 2021. – 152 с.

17. Alshalan A. (2006). Cyber–crime fear and victimization: An analysis of a national survey. PhD Dissertation submitted to Mississippi State University.

18. Casey, E. (2011). Digital Evidence and Computer Crime :Forensic Science, Computers and the Internet (3rd ed.). Academic Press.

19. Decker M., Ladikas M. Bridges between science, society and policy. Technology assessment – methods and impacts // Berlin: Springer. – 2004. – P. 252.

20. Ely A., van Zwanenberg P., Stirling A. New Models of Technology Assessment for Development // Brighton: STEPS Centre. – 2011. – P. 47.

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

22. Ladikas M., Chaturvedi S., Zhao Y., Stemerding D. Science and Technology Governance and Ethics. A Global Perspective from Europe, India and China // Springer International Publishing. – 2015. – P. 173.

Статьи в научных журналах

23. 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.

24. Аккаева Х.А. Международный кибертерроризм как политический феномен / Х.А. Аккаева // Социально–политические науки. – 2018. – № 1. – С. 138–140.

25. 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.

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

27. Антонян Е.А., Клещина Е.Н. Киберпреступность на современном этапе: тенденции и направления противодействия / Е.А. Антонян, Е.Н. Клещина // Вестник экономической безопасности. – 2022. – № 5. – С. 11–15.

28. Арипшев А.М. Кибертерроризм: проблемы в понимании и способы противодействия / А.М. Арипшев // Журнал прикладных исследований. – 2023. – №4. – С. 109–112.

29. Атнашев В.Р., Яхъеева С.Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом / В.Р. Атнашев, С.Н. Яхъеева // Евразийская интеграция: экономика, право, политика. – 2019. – №3 (29). – С. 37–42.

30. Басова Е.А. Цифровое неравенство российских регионов: современные проблемы и пути преодоления / Е.А. Басова // Вопросы территориального развития. – 2021. – №4.– С.1–17.

31. Батюкова В.Е. Предупреждение кибермошенничества в период COVID–19 / В.Е. Батюкова // Образование и право. – 2020. – №11. – С. 347 – 349.

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

33. Бураева Л.А. Кибертерроризм в молодежной среде / Л.А. Бураева // Проблемы экономики и юридической практики. – 2016. – №2. – С. 271–274.

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

35. Бычкова А.М., Суходолов А.П. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции / А.М. Бычкова, А.П. Суходолов // Всероссийский криминологический журнал. – 2018. – № 6. – С.753–766.

36. Ватутина Л.А., Злобина Е.Ю., Хоменко Е.Б. Цифровизация и цифровая трансформация бизнеса: современные вызовы и тенденции / Л.А. Ватутина, Е.Ю. Злобина, Е.Б. Хоменко // Вестник Удмуртского университета. Серия «Экономика и право». – 2021. – №4. – С. 545 – 551.

37. Веденин Д. В. Общая характеристика лиц, совершающих преступления с использованием информационно–телекоммуникационных технологий или в сфере компьютерной информации / Д.В. Веденин // Вестник Уральского юридического института МВД России. – 2023. – № 2. – С. 127–131.

38. Вертакова Ю.В., Крыжановская О.А. Особенности развития организаций в условиях цифровой трансформации / Ю.В. Вертакова и О.А. Крыжановская // Вестник университета. – 2020. – № 10. – С. 33–39.

39. 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.

40. Вершинская О.Н. Информационное неравенство как социологическая проблема / О.Н. Вершинская // Информационное общество. – 2001. – № 4. – С. 45–50.

41. Вехов В.Б., Ковалев С.А. Проблемы борьбы с кибертерроризмом / В.Б. Вехов, С.А. Ковалев // Правопорядок: история, теория, практика. – 2018. – №1 (16). – С. 89–93.

42. 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.

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

44. 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.

45. Воронин Г.Л., Курячьева М.М. Интернет–пространство старшего поколения: анализ проблемы вхождения в цифровую эпоху / Г.Л. Воронин, М.М. Курячьева // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Социальные науки. – 2018. – №3 (51). – С. 55–65.

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

47. Галушкин А.А. К вопросу о кибертерроризме и киберпреступности / А.А. Галушкин // Вестник РУДН. Серия: Юридические науки. – 2014. – №2. – С. 44 – 49.

48. Геляхова Л.А. Международно–правовые основы противодействия кибертерроризму / Л.А. Геляхова // Пробелы в российском законодательстве. – 2017. – № 3. – С. 65–67.

49. Горохов В.Г. Оценка техники как прикладная философия техники и новая научно–техническая дисциплина / В.Г. Горохов // Гений Шухова и современная эпоха. Материалы Международного конгресса. М.: Изд–во МБГТУ им. Н.Э. Баумана, 2015. С. 241–249.

50. Гудкова Т.В., Синицын С.А. Цифровизация как фактор устойчивого развития компании / Т.В. Гудкова, С.А. Синицын // Государственное управление. Электронный вестник. – 2022. – №93. – С. 121–132.

51. Даринская Л.А., Молодцова Г.И., Москвичева Н.Л. Пожилой человек и цифровое пространство: точки соприкосновения / Л.А. Даринская, Г.И. Молодцова, Н.Л. Москвичева // Человек и образование. – 2016. – №3 (48). – С. 151–157.

52. 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.

53. 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.

54. Дубень А.К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению / А.К. Дубень // Международное право и международные организации. – 2022. – №1. – С. 24–33.

55. 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

56. Дяксул О.Ю., Фещенко Н.В. Влияние интернета на современную молодежь / О.Ю. Дяксул, Н.В. Фещенко // Научно–техническое и экономическое сотрудничество стран АТР в XXI веке. – 2017. – Т. 1. – С. 263–266.

57. Евдокимов К.Н., Хобонкова К.В. К проблеме совершенствования международного сотрудничества в сфере противодействия

киберпреступности / К.Н. Евдокимов, К.В. Хобонкова // Сибирский юридический вестник. – 2022. – №3 (98). – С. 90–95.

58. Жмуров Д.В. Кибервиктимология: методы и метрика / Д.В. Жмуров // Baikal Research Journal. – 2022. – Т.13, №1. – С. 1–29.

59. Зубок Ю. А., Селиверстова Н. А. Представления молодежи о будущем страны в проекции культуры / Ю.А. Зубок, Н.А. Селиверстова // Наука. Культура. Общество. 2023. Т. 29, № 3. С. 39–52.

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

61. Игнатов А.Н., Соловьев В.С. Информационно–когнитивные технологии в механизме цифровой виктимизации / А.Н. Игнатов и В.С. Соловьев // Вестник Казанского юридического института МВД России. – 2023. – Т. 14. № 1 (51). – С. 59 – 66.

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

63. Ищенко Е.П. О криминалистическом обеспечении раскрытия и расследования киберпреступлений / Е.П. Ищенко // Деятельность правоохранительных органов в современных условиях: сборник материалов 20–й международной научно–практической конференции. В 2 томах. – 2015. – Т. 1. – С. 336–337.

64. Кабанов П.А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021–2022 гг. / П.А. Кабанов // Виктимология. – 2023. – Т. 10, №1. – С. 17–28.

65. Карпова Д.Н.: Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 46–50.

66. 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.

67. Кибакин М.В., Гришаева С.А. Актуальные проблемы рефлексии цифровой социальной реальности: переосмысление научных концепций / М.В. Кибакин, С.А. Гришаева / Цифровая социология. – 2019. – №2(1). – С. 4–9.

68. Кибальник А.Г., Волосюк П.В. Искусственный интеллект: вопросы уголовно-правовой доктрины, ожидающие ответов / А.Г. Кибальник, П.В. Волосюк // Юридическая наука и практика. Вестник Нижегородской академии МВД России. – 2018. – № 3 (44). – С.173-178.

69. Кириленко В.П. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы / В.П. Кириленко, Г.В. Алексеев // Всероссийский криминологический журнал. – 2020. – Т. 14, № 6. – С. 898–913.

70. Клевцов К.К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам / К.К. Клевцов // Вестник Санкт–Петербургского университета. – 2022. – Т. 13. Вып. 3. – С. 678–695.

71. Климова Ю.О. Проблемы подготовки кадров в сфере информационных технологий / Ю.О. Климова// Проблемы развития территории. – 2020. – №6 (110). – С. 86–105.

72. 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.

73. Кобец П.Н. Совершенствование межгосударственного сотрудничества в сфере информационной безопасности: основа противодействия

международной киберпреступности / П.Н. Кобец // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2023. – № 1. – С. 83–89.

74. Комлев Ю.Ю. От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии / Ю.Ю. Комлев // Российский девиантологический журнал. – 2022. – №2(1). – С. 17–26.

75. Комлев Ю.Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии / Ю.Ю. Комлев // Вестник Казанского юридического института МВД России. – 2020. – №1 (39). – С. 31–40.

76. Корнилова М.В. Интернет как адаптационный ресурс пожилых пользователей / М.В. Корнилова // Изв. Сарат. ун–та Нов. сер. Сер. Социология. Политология. – 2018. – №3. – С. 250–259.

77. Коробеев А.И., Жмуров Д.В. Кибервиктимология фейка: первичное досье / А.И. Коробеев, Д.В. Жмуров // Вестн. Том. гос. ун–та. – 2021. – №471. – С. 250–257.

78. Коротков А.В. Цифровое неравенство в процессах стратификации информационного общества / А.В. Коротков // Информационное общество. – 2003. – № 5. – С. 24–35.

79. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника / Косенков А.Н., Черный Г.А. // Всероссийский криминологический журнал. – 2012. – №3. – С. 87–94.

80. Костомолова М.В. Цифровая девиация как феномен новой социальной реальности: методологические основания и концептуализация понятия / М.В. Костомолова // Социологическая наука и социальная практика. – 2020. – Т. 8. № 2. – С. 41–53.

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

82. Красовская Н.Р., Гуляев А.А. К вопросу о кибермошенничестве / Н.Р. Красовская, А.А. Гуляев // Вестн. Удм. ун–та. Социология. Политология. Международные отношения. – 2022. – Т. 6, вып. 1. – С. 133–138.

83. 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.

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

85. Максимов С.В., Васин Ю.Г., Утаров К.А. Цифровая криминология как инструмент борьбы с организованной преступностью / С.В. Максимов, Ю.Г. Васин, К.А. Утаров // Всероссийский криминологический журнал. – 2018. – №4. – С. 476–484.

86. Мартышенко С.Н. Влияние интернета на формирование коммуникационной среды современной молодежи / С.Н. Мартышенко // АНИ: педагогика и психология. – 2020. – №1 (30). – С. 185–189.

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

88. 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.

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

90. Мороз Н.О. Особенности международно–правового сотрудничества в борьбе с киберпреступностью в рамках ЕС / Н.О. Мороз // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». – 2018. – №4 (16). – С. 87–94.

91. Мосечкин И.Н. Уголовная ответственность за организацию устойчивой группы лиц, созданной для совершения преступлений в сфере компьютерной информации» / И.Н. Мосечкин // Вестник Санкт–Петербургского университета. – 2022. – Право 1. – С. 28–45.

92. Назаров В.Л., Жердев Д.В., Буйначева А.В. Актуальные проблемы цифровой трансформации среднего образования / В.Л. Назаров, Д.В. Жердев, А.В. Буйначева // Образование и наука. – 2023. – № 25(4). – С. 109–166.

93. Никитин Е. В. Обеспечение виктимологической безопасности и профилактики преступлений с использованием информационных технологий / Е.В. Никитин // Виктимология. – 2022. – Т. 9, № 2. – С. 204–212.

94. 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.

95. Никульченкова Е.В. О необходимости введения дефиниции «киберпреступление» в уголовный закон Российской Федерации / Е.В. Никульченкова // Вестник ОмГУ. Серия. Право. – 2022. №3. – С. 98 – 107.

96. Номоконов В.А., Тропина Т.Л.. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012 – № 24. – С. 45–55.

97. Перина А.С. Использование компьютерных технологий против личности: подходы к криминализации в странах СНГ / А.С. Перина // Мониторинг правоприменения. – 2023. №1 (46). – С. 59 – 68.

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

99. Плотникова Т.В., Котельникова О.В. Феномен киберпреступности в условиях XXI века / Т.В. Плотникова, О.В. Котельникова // Право: история и современность. – 2020. – № 3(12). – С. 141 – 150.

100. Поляков В.В., Попов Л.А. Особенности личности компьютерных преступников / В.В. Поляков, Л.А. Попов // Известия АлтГУ. – 2018. – №6 (104). – С. 256–259.

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

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

103. Прокофьева Т.В. О мерах по совершенствованию борьбы с киберпреступностью в Российской Федерации / Т.В. Прокофьева // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. – 2022. – Вып. 1(842). – С. 142–146.

104. Пучков О.А. Мотивация действий хакеров в современной цифровой среде: междисциплинарный подход / О.А. Пучков // Проблемы современного педагогического образования. – 2020. – №67–3. – С. 306–308.

105. Ревенков П.В., Бердюгин А.А.. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания / П.В. Ревенков, А.А. Бердюгин // Национальные интересы: приоритеты и безопасность. – 2017. – Т. 13, № 9. – С. 1747–1760.

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

107. Рыжова Н.И., Громова О.Н. Киберугрозы цифрового социума и их профилактика в рамках виктимологической деятельности / Н.И. Рыжова, О.Н. Громова // Вестник РУДН. Серия: Информатизация образования. – 2020. – №3. – С. 254–268.

108. Сергеев А.Ю., Широкова О.В. Мошенничество в цифровом обществе в условиях социальных изменений / А.Ю. Сергеев, О.В. Широкова // Цифровая социология. – 2023. – №1. – С. 59 – 71.

109. Серебренникова А.В. Криминологические проблемы цифрового мира (цифровая криминология) / А.В. Серебренникова // Всероссийский криминологический журнал. – 2020. – №3. – С. 423–430.

110. Ситков А.С. Международное сотрудничество полиции в рамках Интерпола по противодействию киберпреступности и обеспечению кибербезопасности / А.С. Ситков // Вестник Московского университета МВД России. – 2022. – № 5. – С. 238–242.

111. Скляров С.В., Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации / С.В. Скляров, К.Н. Евдокимов // Всероссийский криминологический журнал. – 2016. – №2 (Т. 10). – С. 322 – 330.

112. Созаев С.С., Кунашев Д.А. Социальная инженерия, ее техники и методы ее противодействия / С. С. Созаев, Д. А. Кунашев // Международный журнал «Вестник науки». – 2020. – № 2 (23). – Т. 1. – С. 85–88.

113. Старостенко О.А. Виктимологические проблемы обеспечения безопасности личности в сети интернет / О.А. Старостенко // Вестник Сибирского юридического института МВД России. – 2022. – №2 (47). – С. 157–161.

114. 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.

115. Стырин Е.М., Родионова Ю.Д. Единая информационная система в сфере закупок как государственная цифровая платформа: современное состояние и перспективы / Е.М. Стырин, Ю.Д. Родионова // Вопросы государственного и муниципального управления. – 2020. – № 3. – С. 49 – 70.

116. Стяжкина С.А. Виктимологическая профилактика кибермошенничества / С.А. Стяжкина // Вестник Удмуртского университета. Серия «Экономика и право». – 2022. – №3. – С. 546–552.

117. 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 / Л.Г. Судас, А.А. Оносов, А.Ж. Бесланеев, Ю.В. Манкевич, М.Б. Пивоварова, В.А. Правосудова, Д.С. Рассадина, П.С. Швыряев // Государственное управление. Электронный вестник. – 2021. – № 86. – С. 284–306.

118. Суходолов А.П., Иванцов С.В., Молчанова Т.В., Спасенников Б.А., Калужина М.А. Цифровая криминология: математические методы прогнозирования (часть 1) / А.П. Суходолов, С.В. Иванцов., Т.В. Молчанова, Б.А. Спасенников, М.А. Калужина // Всероссийский криминологический журнал. – 2018. – №2. – С. 230–236.

119. Тамбиев С.А., Кочесокова З.Х. Международный опыт противодействия кибертерроризму / С.А. Тамбиев, З.Х. Кочесокова // Право и управление. – 2023. – №2. – С. 160–164.

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

121. Тарчоков Б.А. К вопросу о понятии кибертерроризма и некоторых способах противодействия / Б.А. Тарчоков // Право и управление. – 2023. – №2. – С. 170–174.

122. Термелева А.Е. Цифровая трансформация на современном этапе и ее влияние на инновационную деятельность / А.Е. Термелева // Вестник Самарского университета. Экономика и управление. 2022. Т. 13, № 3. С. 50–58.

123. 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.

124. Тирранен В. А. Искусственный интеллект и нейронные сети как инструмент современной киберпреступности // Уголовное право: стратегия развития в XXI веке : материалы XVI Междунар. науч.-практ. конф. (24—25 янв. 2019 г.) М. : РГ-Пресс, 2019. – С. 135—140.

125. Трахтенберг А.Д. Идеологический концепт электронного правительства: как работает риторика разрыва? / Д.А. Трахтенберг // Научный ежегодник Института философии и права Уральского отделения Российской академии наук. – 2017. – Т. 17. Вып. 2. – С. 41–58.

126. Унукович А.С. Социальная инженерия и кибербезопасность: виктимологический аспект / А.С. Унукович // Психопедагогика в правоохранительных органах. – 2021. – №3 (86). – С. 346–351.

127. Федосеева О.И. Психологические особенности формирования личности несовершеннолетнего киберпреступника / О.И. Федосеева // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2022. – № 4 (60). – С. 174–178.

128. 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.

129. 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.

130. Чимаров С.Ю., Бялт В.С. Зарубежный опыт противодействия киберпреступности: в контексте опоры полиции на потенциал общественности / С.Ю. Чимаров, В.С. Бялт// Международный журнал гуманитарных и естественных наук. – 2023. – №1–3 (76). – С. 147–149.

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

132. Швыряев П.С. Кадровая обеспеченность в сфере информационных технологий в России: проблемы и перспективы / П.С. Швыряев // Государственное управление. Электронный вестник. – 2023. – № 97. – С. 231–240.

133. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства / П.С. Швыряев // Государственное управление. Электронный вестник. – 2021. – № 89. – С. 184–196.

134. Швыряев П.С. Проблема киберпреступности в России: актуальное состояние и перспективы решения / П.С. Швыряев // Уровень жизни населения регионов России. – 2023. – Том 19. – № 4. – С. 616–629.

135. Швыряев П.С. Утечки конфиденциальных данных: главный враг внутри / П.С. Швыряев // Государственное управление. Электронный вестник. – 2022. – № 91. – С. 226–241.

136. Янгаева М.О. Методы (техники) социальной инженерии, используемые при совершении преступлений в сфере компьютерной информации / М.О. Янгаева // Криминалистика: вчера, сегодня, завтра. – 2021. – Т. 18. – № 2. – С. 145–151.

137. Ajayi E. F. G. (2016). Challenges to Enforcement of Cyber–crimes Laws and Policy. Journal of Internet and Information Systems, 6(1), 1–12.

138. Albahar M. (2019). Cyber attacks and terrorism: a twenty–first century conundrum. Science and Engineering Ethics 25(4), 993–1006.

139. Almutairi B. S., & Alghamdi A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. Journal of Information Security, 13(04), 363–379.

140. Amankwah–Amoah J., Khan Z., Wood G., Knight G. 2021. COVID–19 and digitalization: The great acceleration // Journal of Business Research, Elsevier, vol. 136(C), pages 602–611.

141. Apau R., Koranteng F. N. (2019). Impact of cybercrime and trust on the use of ecommerce technologies: An application of the theory of planned behavior. International Journal of Cyber Criminology, 13(2).

142. Backhaus S et al. (2020) A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. Cyberpsychology, Behavior, and Social Networking 23(9), 595–603.

143. Brenner S (2007) At light speed: attribution and response to cybercrime/terrorism/warfare. J Crim Law Criminol 97:379.

144. Brenner S. (2004). Toward a criminal law for cyberspace: Distributed security. Boston University Journal of Science & Technology Law, 10(2), pp. 1–105.

145. Carter, D. (1995). Computer crime categories: How techno–criminals operate. FBI Law Enforcement Bulletin, 64(7), 21.

146. 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.

147. Clarke RA (2016) The risk of cyber war and cyber terrorism. Journal of International Affairs 70(1), 179–181.

148. Conteh N.Y., (2021). The dynamics of social engineering and cybercrime in the digital age. In Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 144–149).

149. Curran D. (2018). Risk, innovation, and democracy in the digital economy, European Journal of Social Theory, Vol. 21 No. 2, pp. 207-226.

150. Darawong C. (2018). Dynamic capabilities of new product development teams in performing radical innovation projects. International Journal of Innovation Science, 10 (3), 333–349.

151. David Buil–Gil, Fernando Miró–Llinares, Asier Moneva, Steven Kemp & Nacho Díaz–Castaño (2021) Cybercrime and shifts in opportunities during

COVID–19: a preliminary analysis in the UK, European Societies, 23:sup1, S47–S59.

152. De Bruyne, E., and Gerritse, D. (2018). Exploring the future workplace: results of the futures forum study. Journal of Corporate Real Estate, 20(3), 196–213.

153. 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.

154. Di Nicola, A. Towards digital organized crime and digital sociology of organized crime. Trends Organ Crim (2022).

155. 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.

156. Frank, A.G., Dalenogare, L.S. and Ayala, N.F. (2019), Industry 4.0 technologies: implementation patterns in manufacturing companies, International Journal of Production Economics, Vol. 210, pp. 15-26.

157. Gartzke E (2013) The myth of cyberwar: bringing war in cyberspace back down to earth. International Security 38(2), 41–73.

158. Gross ML, Canetti D and Vashdi DR (2016) The psychological effects of cyber terrorism. Bulletin of the Atomic Scientists 72(5), 284–291.

159. 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.

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

161. Halder, D., & Jaishankar, K. (2015). Irrational coping theory and Positive Criminology: A frame work to protect victims of cyber crime. In N. Ronel and D. Segev (eds.), Positive Criminology (pp. 276–291).

162. Hamadi H, Manzo C (2021) Corporate digital responsibility – a study on managerial challenges for AI integration in business. Lund University, Lund.

163. Heavin, C. and Power, D.J. (2018), Challenges for digital transformation – towards a conceptual decision support guide for managers, Journal of Decision Systems, Vol. 27 No. 1, pp. 38-45.

162. Hennen L., Nierling L. A next wave of Technology Assessment? Barriers and opportunities for establishing TA in seven European countries // Science and Public Policy. – 2015. – vol. 42. – P. 44–58.

163. Herzog S (2011) Revisiting the Estonian cyber attacks: digital threats and multinational responses. Journal of Strategic Security 4(2), 49–60.

164. Hinduja, S., & Patchin, J. W. (2007). Offline consequences of online victimization: School violence and delinquency. Journal of School Violence, 6(3), 89–112.

165. Kozlowski, S. W., Chao, G. T., & Van Fossen, J. (2021). Leading virtual teams. Organizational Dynamics, 50(1), 1–11.

166. Lastowka F.G., & Hunter D. (2004). Virtual crimes. New York Law School Law Review, 49, 293–316.

167. Li Q. (2007). Bullying in the new playground: Research into cyberbullying and cyber victimisation. Australasian Journal of Educational Technology, 23(4), 435–454.

168. Lipton J. D. (2011). Combating cyber–victimization. Berkeley Technology Law Journal, 26, 1103–1156.

169. Mueller, B. Corporate Digital Responsibility. Bus Inf Syst Eng 64, 689–700 (2022).

170. Ngo F. T., Paternoster R. (2011). Cybercrime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5(1), 773–793.

171. Paiola, M. (2018), Digitalization and servitization: opportunities and challenges for Italian SMES, Sinergie Italian Journal of Management, Vol. 36 No. 107, pp. 11-22.

172. 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.

173. Radha R., K. Mahalakshmi, V. Sathish Kumar, A. R. Saravanakumar, ELearning during Lockdown of Covid–19 Pandemic: A Global Perspective, IJCA, vol. 13, no. 4, pp. 1088–1099, Jun. 2020.

174. Roberts L. (2008). Cyber–victimisation in Australia: Extent, impact on individuals and responses. TILES Briefing Paper No. 6.

175. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

176. 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.

177. Sinha R. (2018). Social Impact of Cyber Crime: A Sociological Analysis, International Journal of Management, IT & Engineering Vol. 8 Issue 10(1).

178. Tekic, Z. and Koroteev, D. (2019), From disruptively digital to proudly analog: a holistic typology of digital transformation strategies, Business Horizons, Vol. 62, pp. 683-693.

179. Varghese Gr. (2016). A sociological study of different types of cyber crime, International Journal of Social Science and Humanities Research, Vol. 4, Issue 4, pp: (599-607).

180. Weißenberger BE, Marrocco A (2022) Corporate Digital Responsibility und Ihre Integration in die Unternehmensfu¨hrung. In: RothS, Corsten H (eds) Handbuch Digitalisierung. Vahlen, Berilin, pp 41–58.

181. Winner L. «Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology.» *Science, Technology, & Human Values*, vol. 18, no. 3, 1993, pp. 362–378.

182. Yar M. (2012) E–Crime 2.0: the criminological landscape of new social media. Information & Communications Technology Law, 21(3), 207–219.

Электронные ресурсы

183. Банк России. Правительство России утвердило Стратегию повышения финансовой грамотности и формирования финансовой культуры до 2030 года [Электронный ресурс]. Режим доступа: https://www.cbr.ru/press/event/?id=17155 (дата обращения: 24.12.2023).

184. Банк России. Распоряжение от 25 сентября 2017 г. № 2039–р. [Электронный ресурс]. Режим доступа: https://cbr.ru/Content/Document/File/59796/Inf_note_dec_2718.pdf (дата обращения: 24.12.2023).

185. Банк России. Клиенты банков смогут добровольно ограничивать онлайн–операции для защиты от мошенников [Электронный ресурс]. Режим доступа: https://cbr.ru/press/event/?id=13971 (дата обращения: 24.12.2023).

186. Банк России. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/statistics/ib/review_1q_2023/ (дата обращения: 12.06.2023).

187. Банк России. Обзор операций, совершенных без согласия клиентов финансовых организаций. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 13.06.2023).

188. Банк России. Противодействие нелегальной деятельности на финансовом рынке [Электронный ресурс]. Режим доступа: https://www.cbr.ru/analytics/inside/2022/ (дата обращения: 24.12.2023).

189. Ведомости. Банки активизировали проведение киберучений в прошлом году. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/finance/articles/2023/02/16/963166–banki–aktivizirovali–provedenie–kiberuchenii (дата обращения: 29.05.2023).

190. Ведомости. Доля безналичных платежей в России достигла 70%. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/finance/news/2021/02/12/857761–dolya–beznalichnih–platezhei–v–rossii–dostigla–70 (дата обращения: 18.12.2021).

191. Ведомости. Интернет несет потери [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/importsubstitution/new_technologies/articles/2023/03/14/966290–internet–neset–poteri (дата обращения: 06.08.2023).

192. Ведомости. Киберпреступность в домашних тапочках [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/opinion/articles/2018/10/17/783976–kiberprestupnost (дата обращения: 24.07.2023).

193. Ведомости. Путин поручил разобраться с оборотными штрафами за утечки данных к июлю. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/technology/articles/2023/01/13/959007–putin–oborotnimi–shtrafami (дата обращения: 16.06.2023).

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

195. Ведомости. Расходы на «Цифровую экономику» и «Международную кооперацию» снизят почти на треть в 2023 году. [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/economics/articles/2022/09/27/942639–rashodi–na–tsifrovuyu–ekonomiku (дата обращения: 08.05.2023).

196. Ведомости. ЦБ заявил о росте доли безналичных платежей до 75%. [Электронный ресурс]. Режим доступа:

https://www.vedomosti.ru/finance/news/2021/10/15/891393–o–roste–doli–beznalichnih–platezhei–do–75 (дата обращения: 20.12.2021).

197. Вести.ru. Потери мировой экономики от кибератак к 2030 году оценены в $90 трлн. [Электронный ресурс]. Режим доступа: https://www.vesti.ru/finance/article/2481467 (дата обращения: 24.02.2023).

198. ВЦИОМ. Россия – страна технооптимистов [Электронный ресурс]. Режим доступа: https://wciom.ru/analytical–reviews/analiticheskii–obzor/rossiya–strana–tekhnooptimistov (дата обращения: 17.07.2023).

199. ВЦИОМ. Сохранность персональных данных [Электронный ресурс]. Режим доступа: https://wciom.ru/analytical–reviews/analiticheskii–obzor/sokhrannost–personalnykh–dannykh (дата обращения: 23.09.2023).

200. Газета.ru. «Отсрочка от реальной работы»: можно ли заработать в IT после онлайн–курсов. [Электронный ресурс]. Режим доступа: https://www.gazeta.ru/tech/2021/07/31/13815866/it_courses.shtml (дата обращения: 09.03.2023).

201. Известия. Их слишком много: почему киберпреступления остаются нераскрытыми. [Электронный ресурс]. Режим доступа: https://iz.ru/1166840/mariia–nemtceva/ikh–slishkom–mnogo–pochemu–kiberprestupleniia–ostaiutsia–neraskrytymi (дата обращения: 12.06.2023).

202. Известия. ФСБ сообщила об участии Пентагона в кибератаках против России [Электронный ресурс]. Режим доступа: https://iz.ru/1497823/2023–04–13/fsb–soobshchilo–ob–uchastii–pentagona–v–kiberatakakh–protiv–rossii (дата обращения: 16.07.2023).

203. Интерфакс. Бюджет нацпрограммы "Цифровая экономика" в 2023 году предложено сократить на 35%. [Электронный ресурс]. Режим доступа: https://www.interfax.ru/business/865340 (дата обращения: 22.05.2023).

204. Интерфакс. В МВД РФ создадут Управление по организации борьбы с киберпреступлениями [Электронный ресурс]. Режим доступа:https://www.interfax.ru/russia/865726 (дата обращения: 24.12.2023).

205. Интерфакс. Генпрокурор РФ заявил о бессилии правоохранительных органов перед киберпреступниками. [Электронный ресурс]. Режим доступа: https://www.interfax.ru/russia/699548 (дата обращения: 12.06.2023).

206. Интерфакс. Клиенты банков с 1 октября могут ограничивать онлайн–операции для защиты от мошенников [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/15927795 (дата обращения: 24.12.2023).

207. Интерфакс. Наталья Касперская заявила о необходимости децифровизации предприятий для защиты от кибератак [Электронный ресурс]. Режим доступа: https://www.interfax.ru/digital/872493 (дата обращения: 17.12.2023).

208. Интерфакс. Президент подписал закон о конфискации имущества у киберпреступников [Электронный ресурс]. Режим доступа: https://www.interfax.ru/russia/906019 (дата обращения: 16.07.2023).

209. КоммерсантЪ. В МВД создано управление по борьбе с киберпреступностью [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/5592758 (дата обращения: 30.07.2023).

210. Международный Конгресс по кибербезопасности [Электронный ресурс]. Режим доступа: https://icc.moscow/ru/ (дата обращения: 28.03.2024).

211. Министерство внутренних дел РФ. Состояние преступности [Электронный ресурс]. Режим доступа: https://мвд.рф/reports/ (дата обращения: 18.06.2023).

212. НАФИ. В России выросла доля людей с продвинутым уровнем цифровой грамотности. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/v–rossii–vyrosla–dolya–lyudey–s–prodvinutym–urovnem–tsifrovoy–gramotnosti/ (дата обращения: 06.05.2023).

213. НАФИ. Каждый четвертый россиянин имеет высокий уровень цифровой грамотности. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/tsifrovaya–gramotnost/ (дата обращения: 16.06.2023).

214. НАФИ. НАФИ провел первый замер Индекса цифровой финансовой грамотности жителей России. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/nafi–provel–pervyy–zamer–indeksa–tsifrovoy–finansovoy–gramotnosti–zhiteley–rossii/ (дата обращения: 08.05.2023).

215. НАФИ. Уровень цифровой грамотности в России и Беларуси. [Электронный ресурс]. Режим доступа: https://nafi.ru/analytics/uroven–tsifrovoy–gramotnosti–v–rossii–i–belarusi/ (дата обращения: 07.03.2023).

216. Новости ООН. В Вене проходят переговоры по разработке конвенции о борьбе с киберпреступностью [Электронный ресурс]. Режим доступа: https://news.un.org/ru/story/2023/01/1436692 (дата обращения: 16.07.2023).

217. ООО «Журнал «КО». Более 80% россиян готовы повысить свои знания в области цифровых прав [Электронный ресурс]. Режим доступа: https://ko.ru/news/bolee–80–rossiyan–gotovy–povysit–svoi–znaniya–v–oblasti–tsifrovykh–prav/ (дата обращения: 17.07.2023).

218. Официальный сайт ООН. Цель 9: Создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям [Электронный ресурс]. Режим доступа: https://www.un.org/sustainabledevelopment/ru/infrastructure–industrialization/ (дата обращения: 09.07.2023).

219. РАЭК. Запущено исследование устойчивости цифрового развития [Электронный ресурс]. Режим доступа: https://raec.ru/live/raec–news/11462/ (дата обращения: 08.08.2023).

220. РБК. Аналитики оценили уровень цифровой грамотности россиян. [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/20/06/2018/5b29331c9a79477930b03101 (дата обращения: 12.06.2023).

221. РБК. ВТБ описал типичную жертву финансовых мошенников. [Электронный ресурс]. Режим доступа:

a. https://www.rbc.ru/society/23/06/2021/60d1cd2c9a7947cd10c61ba3 (дата обращения: 07.05.2023).

222. РБК. Дефицит ИТ–мозгов: как Россия решает проблему кадрового голода в отрасли // РБК [Электронный ресурс]. Режим доступа:

a. https://www.rbc.ru/economics/28/07/2022/62e12c929a794747597da279 (дата обращения: 04.05.2023).

223. РБК. Интерпол решил не исключать Россию из организации [Электронный ресурс]. Режим доступа:

a. https://www.rbc.ru/politics/11/03/2022/622a58609a794796f4c3dbe1 (дата обращения: 16.07.2023).

224. РБК. Каждый шестой россиянин пострадал из–за телефонных мошенников. [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/02/10/2021/6156e99a9a794778904993ed (дата обращения: 12.06.2023).

225. РБК Plus. Соцсети наращивают клиентуру. [Электронный ресурс]. Режим доступа: https://plus.rbc.ru/news/5f8f18687a8aa9229962eb78 (дата обращения: 11.02.2022).

226. Рамблер. Мишустин предложил Kaspersky работу над кибериммунитетом в промышленности. [Электронный ресурс]. Режим доступа:

https://news.rambler.ru/tech/46756871/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 05.03.2023).

227. РИА Новости. Путин прокомментировал рост киберпреступности. [Электронный ресурс]. Режим доступа: https://ria.ru/20230320/kiber–1859136636.html (дата обращения: 12.06.2023).

228. Российская Газета. Крона уходит в сеть? [Электронный ресурс]. Режим доступа: https://rg.ru/2020/12/13/v–shvecii–otkazhutsia–ot–nalichnyh–deneg.html (дата обращения: 20.12.2021).

229. Российская Газета. Необходимо ужесточить ответственность за киберпреступления – эксперты [Электронный ресурс]. Режим доступа: https://rg.ru/2021/08/05/neobhodimo–uzhestochit–otvetstvennost–za–kiberprestupleniia–eksperty.html (дата обращения: 16.07.2023).

230. Российская Газета. Путин и Байден обсудили борьбу с киберпреступностью. [Электронный ресурс]. Режим доступа: https://rg.ru/2021/12/07/putin–i–bajden–obsudili–borbu–s–kiberprestupnostiu.html (дата обращения: 11.02.2022).

231. ТАСС. Банки рассказали, что жертвой мошенников можно стать независимо от личных характеристик. [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/13625465 (дата обращения: 28.01.2023).

232. ТАСС. ГП: правоохранительные органы отстают в технических возможностях от киберпреступников. [Электронный ресурс]. Режим доступа: https://tass.ru/politika/8915711 (дата обращения: 16.06.2023).

233. ТАСС. У киберпреступников будут конфисковывать незаконно полученное имущество [Электронный ресурс]. Режим доступа: https://tass.ru/obschestvo/17995469 (дата обращения: 08.08.2023).

234. ТАСС. Шадаев заявил, что порядка 100 тыс. IT–специалистов покинули Россию с начала года. [Электронный ресурс]. Режим доступа: https://tass.ru/ekonomika/16639651 (дата обращения: 08.03.2023).

235. Управление 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).

236. Цифровая устойчивость и информационная безопасность России 2024 [Электронный ресурс]. Режим доступа: https://ib-bank.ru/secural/program (дата обращения: 28.03.2024).

237. Bloomberg. The ‘New Normal’ for Many Older Adults Is on the Internet. [Электронный ресурс]. Режим доступа: https://www.bloomberg.com/news/features/2020–05–06/in–lockdown–seniors–are–becoming–more–tech–savvy (дата обращения: 19.12.2021).

238. Cybercrime Magazine. Cybercrime To Cost The World 8 Trillion Annually In 2023 [Электронный ресурс]. Режим доступа: https://cybersecurityventures.com/cybercrime–to–cost–the–world–8–trillion–annually–in–2023/ (дата обращения: 10.12.2023).

239. DataReportal. Digital 2022 April Global Statshot. [Электронный ресурс]. Режим доступа: https://datareportal.com/reports/digital–2022–april–global–statshot (дата обращения: 06.05.2023).

240. DoubleVerify. Four Fundamental Shifts in Media & Advertising During 2020. [Электронный ресурс]. Режим доступа: https://doubleverify.com/four–fundamental–shifts–in–media–and–advertising–during–2020/ (дата обращения: 17.12.2021).

241. EDELMAN TRUST BAROMETER 2022 [Электронный ресурс]. Режим доступа: https://www.edelman.com/sites/g/files/aatuss191/files/2022-10/2022%20Trust%20Barometer%20Special%20Report_Trust%20in%20Technology%20Final_10-19.pdf (дата обращения: 04.02.2024).

242. EDELMAN TRUST BAROMETER 2024 [Электронный ресурс]. Режим доступа: https://www.edelman.com/sites/g/files/aatuss191/files/2024-01/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL_1.pdf (дата обращения: 04.02.2024).

243. Forbes. Метод кнута и пряника: как вернуть IT–специалистов в Россию. [Электронный ресурс]. Режим доступа: https://www.forbes.ru/tekhnologii/481417–metod–knuta–i–pranika–kak–vernut–it–specialistov–v–rossiu (дата обращения: 08.03.2023).

244. Forbes. Роскомнадзор насчитал около 150 крупных утечек личных данных в 2022 году. [Электронный ресурс]. Режим доступа:

https://www.forbes.ru/tekhnologii/484301–roskomnadzor–nascital–okolo–150–krupnyh–utecek–licnyh–dannyh–v–2022–godu (дата обращения: 16.06.2023).

245. Forbes. Повестка дня: во сколько может обойтись создание электронного реестра военнообязанных. [Электронный ресурс]. Режим доступа: https://www.forbes.ru/tekhnologii/487484–povestka–dna–vo–skol–ko–mozet–obojtis–sozdanie–elektronnogo–reestra–voennoobazannyh (дата обращения: 15.06.2023).

246. Gartner. 7 Top Trends in Cybersecurity for 2022 [Электронный ресурс]. Режим доступа: https://www.gartner.com/en/articles/7–top–trends–in–cybersecurity–for–2022 (дата обращения: 10.12.2023).

247. Hootsuite. The Global State of Digital 2021. [Электронный ресурс]. Режим доступа: https://www.hootsuite.com/pages/digital–trends–2021#c–274407 (дата обращения: 16.12.2021).

248. HSE daily. Между раем и адом: как россияне относятся к цифровизации [Электронный ресурс]. Режим доступа: https://daily.hse.ru/post/976 (дата обращения: 21.08.2023).

249. InfoWatch. Россия: утечки информации ограниченного доступа в 2022 г. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki–informatsii–ogranichennogo–dostupa–v–rossii–za–2022–god.pdf (дата обращения: 15.06.2023).

250. KasperskyOS. Кибериммунитет [Электронный ресурс]. Режим доступа: https://os.kaspersky.ru/technologies/ (дата обращения: 31.12.2023).

251. Lenta.ru. Илон Маск объявил о запуске Starlink. Зачем миллиардеру проект спутникового интернета и как он изменит мир? [Электронный ресурс]. Режим доступа: https://lenta.ru/brief/2021/09/23/starlink/ (дата обращения: 17.12.2021).

252. McKinsey & Company. US digital payments: Achieving the next phase of consumer engagement. [Электронный ресурс]. Режим доступа:

https://www.mckinsey.com/industries/financial–services/our–insights/banking–matters/us–digital–payments–achieving–the–next–phase–of–consumer–engagement (дата обращения: 18.12.2021).

253. Kremlin.ru. Инвестиционный форум «Россия зовет!» [Электронный ресурс]. Режим доступа: http://kremlin.ru/events/president/transcripts/67241 (дата обращения: 17.07.2023).

254. Pew Research Center. About three–in–ten U.S. adults say they are ‘almost constantly’ online. [Электронный ресурс]. Режим доступа:: https://www.pewresearch.org/fact–tank/2021/03/26/about–three–in–ten–u–s–adults–say–they–are–almost–constantly–online/ (дата обращения: 11.02.2022).

255. Pew Research Center. Internet/Broadband Fact Sheet. [Электронный ресурс]. Режим доступа: https://www.pewresearch.org/internet/fact–sheet/internet–broadband/ (дата обращения: 17.12.2021).

256. Positive Technologies. Актуальные киберугрозы: итоги 2022 года. [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru–ru/research/analytics/cybersecurity–threatscape–2022/#id9 (дата обращения: 12.06.2023).

257. Reuters. White House plans 30–country meeting on cyber crime and ransomware – official. [Электронный ресурс]. Режим доступа: https://www.reuters.com/world/us/white–house–plans–30–country–meeting–cyber–crime–ransomware–official–2021–10–01/ (дата обращения: 11.02.2022).

258. SberProTech [Электронный ресурс]. Режим доступа: https://sber.pro/digital/sberprotech/ (дата обращения: 28.03.2024).

259. SEON. Global Cybercrime Report: Which Countries Are Most at Risk in 2023? [Электронный ресурс]. Режим доступа: https://seon.io/resources/global–cybercrime–report/ (дата обращения: 10.12.2023).

260. Surfshark. Cybercrime statistics [Электронный ресурс]. Режим доступа: https://surfshark.com/research/data–breach–impact/statistics (дата обращения: 10.12.2023).

261. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 November 2023 [Электронный ресурс]. Режим доступа: https://www.gov.uk/government/publications/ai–safety–summit–2023–the–bletchley–declaration/the–bletchley–declaration–by–countries–attending–the–ai–safety–summit–1–2–november–2023 (дата обращения: 06.01.2024).

262. Upwork. Economist Report: Future Workforce [Электронный ресурс]. Режим доступа: https://www.upwork.com/press/releases/economist–report–future–workforce (дата обращения: 18.12.2021).

263. World Economic Forum. State of the Connected World 2023 Edition [Электронный ресурс]. Режим доступа: https://www3.weforum.org/docs/WEF_State_of_the_Connected_World_2023_Edition.pdf (дата обращения: 10.12.2023).

264. World Economic Forum. The Global Risks Report 2023 18th Edition [Электронный ресурс]. Режим доступа: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (дата обращения: 09.12.2023).

Приложение 1. Гайд экспертного опроса

№	Тема	№	Вопрос	Ответ
1.	Состояние киберпреступности в России	1	Как бы Вы охарактеризовали актуальное состояние киберпреступности в России в 2023 году?	
		2	Можно ли говорить о том, что сегодня проблема киберпреступности – угроза национальной безопасности России?	
		3	В чем, на Ваш взгляд, главная опасность киберпреступности?	
		4	Какие ключевые тренды за последние несколько лет в сфере киберпреступлений в России Вы бы отметили?	
		5	Как Вы считаете, оказалась ли система безопасности России готова к росту количества киберпреступлений в период пандемии и после ее окончания? Или же ситуация вышла из–под контроля?	
		6	Как Вы считаете, в настоящий момент проблеме киберпреступности в России уделяется достаточное внимание со стороны государственной власти?	
		7	В какой степени, на Ваш взгляд, эффективны российские правоохранительные органы в борьбе с киберпреступностью?	
		8	Как Вы считаете, кто сегодня в России главный объект киберпреступного воздействия: общество, государство, бизнес?	
		9	А кто в России в настоящее время несет наиболее серьезные потери от киберпреступной деятельности: бизнес, государство, общество?	

		10	А кто сейчас в России наименее защищен перед угрозой киберпреступности: общество, бизнес, государство?	
		11	Можно ли спрогнозировать дальнейшее развитие проблемы киберпреступности в России? Если да, каким Вам представляется состояние киберпреступности в России на горизонте ближайших 2–3 лет?	
2.	Причины сложившейся ситуации	1	Как Вы считаете, каковы ключевые причины роста количества киберпреступлений в России в последние годы?	
		2	Какие ключевые факторы влияют на состояние киберпреступности в России, на Ваш взгляд?	
		3	На Ваш взгляд, какие ключевые решения должны были быть предприняты для недопущения ухудшения ситуации с киберпреступностью в России в последние годы?	
		4	Были ли они предприняты? Если нет, то по какой причине, на Ваш взгляд?	
		5	Как Вы считаете, в какой степени российская законодательная база отвечает вызовам со стороны киберпреступной угрозы? Актуальна ли она и эффективна в борьбе с киберпреступностью?	
		6	Как Вы считаете, в России реализуемая сегодня политика по борьбе с киберпреступностью является результативной и эффективной?	
		7	Какие эффективные решения в борьбе с киберпреступностью в России Вы бы отметили? Если таковые имели место быть, на Ваш взгляд.	

		8	Как Вы считаете, влияет ли уровень цифровой грамотности населения на состояние киберпреступности в государстве? Как бы вы оценили уровень цифровой грамотности населения в России?	
		9	Как Вы считаете, каким образом мог повлиять отток высококвалифицированных ИТ–кадров в 2022 году на состояние киберпреступности в стране? А влияет ли «утечка мозгов», которая наблюдается в течение многих лет в России?	
		10	Как Вы считаете, каким образом санкционное давление и курс на импортозамещение могли повлиять и повлияют на состояние киберпреступности в России?	
3.	Стратегии решения проблемы	1	Какие, на Ваш взгляд, препятствия встают перед Россией на пути решения проблемы киберпреступности?	
		2	Есть ли решения у этих проблем? Если да, какими Вы видите эти решения?	
		3	В последние несколько лет набирает популярность кибериммунный подход к разработке и внедрению цифровых систем, где первостепенный приоритет отдается безопасности и отказоустойчивости системы. Как Вы считаете, сегодня уже назрел пересмотр сложившегося подхода к разработке цифровых систем? Должен ли принцип безопасности лежать в основе цифровых систем будущего?	
		4	На ваш взгляд, ужесточение законодательства за киберпреступную деятельность и халатность в отношении конфиденциальных данных эффективно в борьбе с киберпреступностью?	

		5	Эффективна ли работа с населением в рамках борьбы с киберпреступностью? Сегодня в России проводятся массовые кампании по информированию граждан, повышению их цифровой грамотности. На Ваш взгляд, есть ли смысл в такой деятельности? И если да, как можно повысить эффективность и результативность таких кампаний?	
		6	Как Вы считаете, какое место занимает международное сотрудничество в решении проблемы киберпреступности? Какое влияние в данном контексте может оказать курс России на разрыв отношений с «недружественными» странами?	
4	Заключительный блок	1	Если Вы хотели бы что–то добавить по проблеме киберпреступности и стратегиям борьбы с ней, это можно сделать в рамках данного блока.	