DOI: 10.24412/2070-1381-2021-89-184-196

Киберпреступность в России: новый вызов для общества и государства

Швыряев Павел Сергеевич
Аспирант, факультет государственного управления, МГУ имени М.В. Ломоносова, Москва, РФ.
E-mail: ShvyryaevPS@spa.msu.ru
SPIN-код РИНЦ: 6531-8970

Аннотация
Статья посвящена рассмотрению киберпреступности как новой угрозы современного мира. Цель анализа заключается в изучении актуального состояния киберпреступной деятельности, стремительный рост которой отмечается в Российской Федерации, и ее динамики за последние несколько лет. На основании ежемесячной статистики о состоянии преступности, публикуемой Министерством внутренних дел РФ, построены и проанализированы временные ряды по количеству официально зарегистрированных в 2017–2020 гг. преступлениях с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (киберпреступления). Показано, что киберпреступная деятельность активно развивалась в России в течение последних нескольких лет, а во время «коронакризиса» приняла черты социальной проблемы государственного масштаба. Сформулированы также ключевые факторы, которые в значительной степени способствовали возникновению негативной ситуации: низкий уровень цифровой грамотности населения на фоне процесса цифровизации, ускорившегося и углубившегося во время пандемии COVID-19; недостаточно эффективное противодействие киберпреступной деятельности (низкий уровень компетенций со стороны правоохранительных органов, несовершенство антифрод-инфраструктуры — комплекса технологий и программного обеспечения, разработанного для противодействия киберпреступной деятельности). В результате — невысокий процент раскрываемости киберпреступлений, плохой уровень подготовки к работе на опережение и оперативное пресечение преступной активности. Киберпреступность становится одной из наиболее серьезных проблем современного российского общества, наносящей огромный урон российской экономике и благосостоянию граждан. Проблема киберпреступности — сложная социальная проблема, которая требует комплексного решения с активным участием различных заинтересованных сторон: государственных органов, коммерческих и некоммерческих организаций, научного сообщества, международных партнеров. Феномен киберпреступности требует дальнейшего научного изучения для формулирования и реализации эффективных решений по противодействию в Российской Федерации.

Ключевые слова
Цифровизация, киберпреступность, социальная инженерия, кибербезопасность, цифровая грамотность, правоохранительные органы.

Cybercrime in Russia as a New Challenge for Society and State

Pavel S. Shvyriaev
Postgraduate student, School of Public Administration, Lomonosov Moscow State University, Moscow, Russian Federation.
E-mail: ShvyryaevPS@spa.msu.ru

Abstract
The article is devoted to cybercrime as a new threat of modern world. The aim is to analyze the current state and dynamics of cybercriminal activity over the past few years, the rapid growth of which has been noted in the Russian Federation. The data of the Ministry of Internal Affairs of the Russian Federation on the number of cybercrimes in 2017–2020 were used for analysis. Based on the data, time series were built and analyzed for the number of officially registered cybercrimes. It is shown that cybercriminal activity has been actively developing in Russia over the past few years, and during the coronavirus crisis it took on the features of a social problem of a national scale. Key factors have been formulated, which largely contributed to the formation of a negative situation: the low level of population digital literacy despite the digitalization process; inefficiency in countering cybercriminal activity (low level of competence of law enforcement agencies, imperfect antifraud infrastructure). As a result, there is a low percentage of cybercrime detection in the Russian Federation, a poor level of preparation to work proactively and promptly suppress criminal activity. Cybercrime is becoming one of the most serious problems of modern Russian society, causing enormous damage to the Russian economy and the well-being of citizens. The problem of cybercrime is a complex social problem that requires a comprehensive solution with the active participation of various stakeholders: government agencies, commercial and non-profit organizations, the scientific community, and international partners. The phenomenon of cybercrime requires further scientific study in order to formulate and implement effective solutions to counter in the Russian Federation.

Keywords
Digitalization, cybercrime, social engineering, cybersecurity, digital literacy, law enforcement agency.

Введение

Цифровизация — один из основополагающих процессов современности. ЮНКТАД (Конференция ООН по торговле и развитию, орган Генеральной Ассамблеи ООН) в своем отчете, посвященном кризису COVID-19, отмечает следующие тренды цифровизации: удаленная работа и онлайн-конференции, использование соцсетей для общения и получения информации, рост электронной коммерции, защита персональных данных[1].

Пандемия COVID-19 существенным образом повлияла на поведение и привычки людей, на то, как люди используют технологии [Monteith et al. 2021, 1]. Прямо сейчас мы можем наблюдать оформление глобального цифрового мира, в который инвестируется все больше ресурсов в виде инфраструктуры, денег, технологий, идей и человеческого времени и который обособляется от мира физического и обретает свою субъектность. В выборе между физическим и цифровым миром современный человек все чаще отдает предпочтение последнему: сегодня совсем не удивительно, что люди общаются виртуально [Fors 2013, 46], оплачивают покупки безналично, работают удаленно или проводят досуг онлайн[2].

Цифровые технологии, снимая физические ограничения реального мира, открыли широкие возможности для новых форматов обучения [Kameneva 2020, 18], обмена информацией, работы, общения, взаимодействия и творчества для миллиардов людей. Вместе с тем по мере становления нового цифрового мира одной из главных его характеристик становятся хрупкость и неустойчивость. Сюда можно отнести как глобальные сбои, которые затрагивают миллиарды людей по всей планете[3], так и феномен киберпреступности.

Борьба с киберпреступностью является одной из наиболее актуальных проблем в мире [Протасевич, Зверянская 2011, 29]. Киберпреступность стала глобальной, международной и серьезной проблемой [Stanciu, Tinca 2017, 628]. Это негативная черта, но вместе с тем неотъемлемая часть процесса цифровизации, которая затрагивает все большее количество людей и наносит громадный урон мировой и государственной экономике. Только за 2020 г. россияне перевели мошенникам около 150 млрд рублей[4]. По заявлениям зампреда Сбербанка Станислава Кузнецова, ущерб российской экономике от киберпреступлений может достичь 6 трлн рублей к началу 2022 г.[5], это около 5,6% от ВВП страны за 2020 г.[6]. Прогнозы экспертов по мировой экономике также неутешительны: согласно отчету Cybersecurity Ventures, в ближайшие несколько лет глобальный урон от киберпреступности будет расти на 15% ежегодно и составит 10,5 триллионов долларов США к 2025 г.[7]. Эксперты компании подчеркивают, что киберпреступность — один из главных вызовов, с которым человечество столкнется в ближайшие пару десятилетий[8]. Проблема уязвимости цифровых систем перед киберпреступностью становится

[1] The COVID-19 Crisis: Accentuating the Need to Bridge Digital Divides // UNCTAD [Электронный ресурс]. URL: https://unctad.org/system/files/official-document/dtlinf2020d1_en.pdf (дата обращения: 01.09.2021).
[2] Доля безналичных платежей в России достигла 70% // Ведомости [Электронный ресурс]. URL: https://www.vedomosti.ru/finance/news/2021/02/12/857761-dolya-beznalichnih-platezhei-v-rossii-dostigla-70 (дата обращения: 01.09.2021); Ozimek A. Economist Report: Future Workforce [Электронный ресурс]. URL: https://www.upwork.com/press/releases/economist-report-future-workforce (дата обращения: 01.09.2021); Global Online Content Consumption Doubled in 2020 // Forbes [Электронный ресурс]. URL: https://www.forbes.com/sites/johnkoetsier/2020/09/26/global-online-content-consumption-doubled-in-2020/?sh=596af3e92fde (дата обращения: 01.09.2021).
[3] Марк Цукерберг извинился за глобальный сбой в работе сервисов Facebook // BBC [Электронный ресурс]. URL: https://www.bbc.com/russian/news-58796393 (дата обращения: 10.10. 2021).
[4] Не пойман — не разговор // Коммерсантъ [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4627498 (дата обращения: 01.09.2021).
[5] Потери экономики РФ от кибератак оценили в 6 трлн руб. // Вести.ру [Электронный ресурс]. URL: https://www.vesti.ru/finance/article/2585133 (дата обращения: 01.09.2021).
[6] Росстат представляет первую оценку ВВП за 2020 г. // Федеральная служба государственной статистики [Электронный ресурс]. URL: https://rosstat.gov.ru/folder/313/document/113015 (дата обращения: 01.09.2021).
[7] Cybercrime To Cost The World $10.5 Trillion Annually By 2025 [Электронный ресурс]. URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (дата обращения: 01.09.2021).
[8] Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021 [Электронный ресурс]. URL: https://cybersecurityventures.com/annual-cybercrime-report-2020/ (дата обращения: 01.09.2021).

настолько серьезной, что даже ведущие мировые компании в области кибербезопасности подвергаются успешным атакам со стороны злоумышленников[9]. Неудивительно, что в этой связи эксперты считают рост киберпреступности одной из наиболее опасных угроз информационной безопасности[10].

Проблема киберпреступности приковывает внимание и российских властей. На важность вопросов кибербезопасности в современном мире обращало внимание и высшее политическое руководство страны: президент Владимир Путин[11], премьер-министр Михаил Мишустин, председатели Совета Федерации Валентина Матвиенко и Государственной Думы Вячеслав Володин[12]. Проблема киберпреступности требует серьезных и незамедлительных мер, прежде всего со стороны государственных органов.

В ответ на рост количества преступлений в России за последние годы были созданы специальные подразделения по борьбе с кибермошенничеством[13], запущены специальные разделы по информированию населения[14]; в некоторых регионах функционируют автоматизированные системы для выявления преступлений в киберпространстве[15], проводятся тематические рабочие заседания на уровне парламента страны[16], принимаются новые законы[17]; кроме того, устанавливается сотрудничество с международными партнерами[18], а также вносится в ООН совместный с США проект конвенции против киберпреступности[19]. Несмотря на предпринимаемые действия со стороны государственных органов России, сложившаяся ситуация с уровнем киберпреступности в стране остается тревожной: российские правоохранительные органы отмечают взрывной рост (на 74%) количества зарегистрированных киберпреступлений в 2020 г. по сравнению с предыдущим годом[20], при этом процент раскрываемости остается

[9] When a top cybersecurity firm gets hacked, what is the takeaway for the average netizen? // USA Today [Электронный ресурс]. URL: https://www.usatoday.com/story/tech/2020/12/12/hacked-top-cybersecurity-firm-fireeye-says-nation-state-culprit/6511242002/ (дата обращения: 01.09.2021).
[10] Киберпреступность — самая опасная угроза информационной безопасности // РИА Новости [Электронный ресурс]. URL: https://ria.ru/20130422/933965574.html (дата обращения: 01.09.2021).
[11] Путин назвал кибербезопасность одной из важнейших тем современности // ТАСС [Электронный ресурс]. URL: https://tass.ru/politika/11637535 (дата обращения: 01.09.2021); Это просто подонки: Путин рассказал, как бороться с телефонными мошенниками // Вести.ру [Электронный ресурс]. URL: https://www.vesti.ru/article/2582333 (дата обращения: 01.09.2021).
[12] Мишустин рассказал о росте активности киберпреступности в России // Известия [Электронный ресурс]. URL: https://iz.ru/1032919/2020-07-08/mishustin-rasskazal-o-roste-aktivnosti-kiberprestupnosti-v-rossii (дата обращения: 01.09.2021); СФ призывает к международному сотрудничеству в борьбе с киберпреступностью // ТАСС [Электронный ресурс]. URL: https://tass.ru/politika/4371805 (дата обращения: 01.09.2021); Володин предложил ужесточить наказание за телефонное мошенничество // Российская газета [Электронный ресурс]. URL: https://rg.ru/2021/07/23/volodin-predlozhil-uzhestochit-nakazanie-za-telefonnoe-moshennichestvo.html (дата обращения: 01.09.2021); Володин предложил ужесточить наказание за телефонное мошенничество // Российская газета [Электронный ресурс]. URL: https://rg.ru/2021/07/23/volodin-predlozhil-uzhestochit-nakazanie-za-telefonnoe-moshennichestvo.html (дата обращения: 01.09.2021).
[13] В СК создали подразделение для борьбы с киберпреступлениями // Известия [Электронный ресурс]. URL: https://iz.ru/956157/2019-12-19/v-sk-sozdali-podrazdelenie-dlia-borby-s-kiberprestupleniiami (дата обращения: 01.09.2021).
[14] На Госуслугах запущен раздел «Жизненные ситуации: финансовое мошенничество» // Сайт Министерства финансов РФ [Электронный ресурс]. URL: https://minfin.gov.ru/ru/press-center/?id_4=37587-na_gosuslugakh_zapushchen_razdel_zhiznennye_situatsii_finansovoe_moshennichestvo (дата обращения: 01.09.2018).
[15] Генпрокуратура подготовила меры по борьбе с киберпреступностью в России // ТАСС [Электронный ресурс]. URL: https://tass.ru/obschestvo/9032391 (дата обращения: 01.09.2021).
[16] Депутаты обсудили вопросы противостояния киберпреступности // Сайт Государственный Думы РФ [Электронный ресурс]. URL: http://duma.gov.ru/news/51067/ (дата обращения: 01.09.2021).
[17] Путин подписал закон о блокировке мошеннических сайтов // Сайт Парламентской Газеты [Электронный ресурс]. URL: https://www.pnp.ru/politics/putin-podpisal-zakon-o-blokirovke-moshennicheskikh-saytov.html (дата обращения: 01.09.2021).
[18] Бортников сообщил о договоренности ФСБ с США по выявлению киберпреступников // Ведомости [Электронный ресурс]. URL: https://www.vedomosti.ru/politics/news/2021/06/23/875223-bortnikov-soobschil-o-dogovorennosti-fsb-s-ssha-po-viyavleniyu-kiberprestupnikov (дата обращения: 01.09.2021).
[19] Россия внесла в ООН проект конвенции против киберпреступности // ТАСС [Электронный ресурс]. URL: https://tass.ru/politika/11997481 (дата обращения: 01.09.2021).
[20] В России зафиксирован угрожающий рост киберпреступлений // Сайт Российской Газеты [Электронный ресурс]. URL: https://rg.ru/2021/04/23/v-rossii-zafiksirovan-ugrozhaiushchij-rost-kiberprestuplenij.html (дата обращения: 01.09.2021).

невысоким[21]. Российская газета, официальный печатный орган Правительства РФ, назвала эту ситуацию «угрожающей»[22], а в генпрокуратуре заявили об угрозе нацбезопасности со стороны киберпреступности[23].

Проблема киберпреступности в России остается острой, несмотря на деятельность властей и ведущих компаний[24] в сфере борьбы с незаконной деятельностью. Киберпреступность — масштабный и сложный феномен, противодействие которому требует тесной кооперации различных заинтересованных сторон: международных партнеров, государственных и правоохранительных органов, коммерческих и некоммерческих организаций, научно-исследовательского сообщества. Для реализации грамотной и эффективной политики противодействия киберпреступности важно провести глубокий анализ текущего состояния и тенденций развития феномена киберпреступности в России.

Цель данной статьи — проанализировать актуальное состояние киберпреступности в России и динамику за последние несколько лет. Для достижения заявленной цели необходимо решить следующие задачи:

— проанализировать динамику развития киберпреступности в Российской Федерации в 2017–2020 гг., используя статистику Министерства внутренних дел о количестве зарегистрированных преступлений в стране;

— проанализировать новостные источники, комментарии и отчеты экспертов по проблеме киберпреступности в России и мире;

— сформулировать и обосновать ключевые факторы, которые послужили причиной ухудшения ситуации с киберпреступностью в России за последние несколько лет.

Методология исследования

Источником данных для анализа в рамках статьи является статистика Министерства внутренних дел РФ, опубликованная на официальном сайте в разделе отчетов о состоянии преступности в стране[25]. В данном разделе начиная с января 2003 г. на ежемесячной основе публикуется отчет-характеристика о состоянии преступности в РФ за прошедший месяц. Отчет содержит резюме об общем состоянии преступности в стране, в нем отмечаются наиболее значимые изменения и тенденции. Помимо краткой характеристики, дается подробный отчет, который содержит следующую информацию: статистику в разбивке по типам преступлений, сведения о потерпевших, характеристику нарушителей порядка, сведения о раскрытых преступления прошлых лет, состояние и динамику преступности в регионах.

Для анализа в рамках данной статьи используется статистика по преступлениям, совершенным с использованием информационно-коммуникационных технологий или в сфере компьютерной информации. Интересно отметить, что если в самых ранних опубликованных отчетах о преступлениях в сфере компьютерной информации давалась только общая статистика

[21] В Генпрокуратуре заявили, что киберпреступность стала представлять угрозу нацбезопасности // ТАСС [Электронный ресурс]. URL: https://tass.ru/obschestvo/11451173 (дата обращения: 01.09.2021).
[22] В России зафиксирован угрожающий рост киберпреступлений // Сайт Российской Газеты [Электронный ресурс]. URL: https://rg.ru/2021/04/23/v-rossii-zafiksirovan-ugrozhaiushchij-rost-kiberprestuplenij.html (дата обращения: 01.09.2021).
[23] В Генпрокуратуре заявили, что киберпреступность стала представлять угрозу нацбезопасности // ТАСС [Электронный ресурс]. URL: https://tass.ru/obschestvo/11451173 (дата обращения: 01.09.2021).
[24] «Мы научились защищать наших клиентов». Зампред правления Сбербанка — о кибермошенничестве и киберграмотности // Lenta.ru [Электронный ресурс]. URL: https://lenta.ru/articles/2021/09/07/kuznetsov/ (дата обращения: 11.10.2021); Искусственный интеллект отследит поведение клиента банка // Ведомости [Электронный ресурс]. URL: https://www.vedomosti.ru/finance/articles/2021/09/21/887658-iskusstvennii-intellekt (дата обращения: 11.10.2021).
[25] Состояние преступности // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports (дата обращения: 01.09.2021).

о количестве совершенных преступлений, то в последних актуальных отчетах состояние киберпреступности анализируется подробно: дается детализированная статистика в разбивке по типам совершенных преступлений, раскрываемости, приводится статистика по регионам. Сейчас в самых последних отчетах за 2021 г. раздел с характеристикой киберпреступлений занимает наибольшее количество страниц относительно аналитики по другим типам нарушений и составляет в среднем 8–9% от общего объема отчета. На основании отмеченных тенденций в составлении отчетности можно сделать вывод о том, что статистика по киберпреступности становится важным объектом анализа для составителей отчетов в МВД РФ, подчеркивается ее значимость для читателей и СМИ.

Киберпреступления: тенденции развития

Чтобы проиллюстрировать общие тенденции развития киберпреступности в России, построим график, показывающий количество официально зарегистрированных преступлений в 2017–2020 гг. (Рисунок 1).

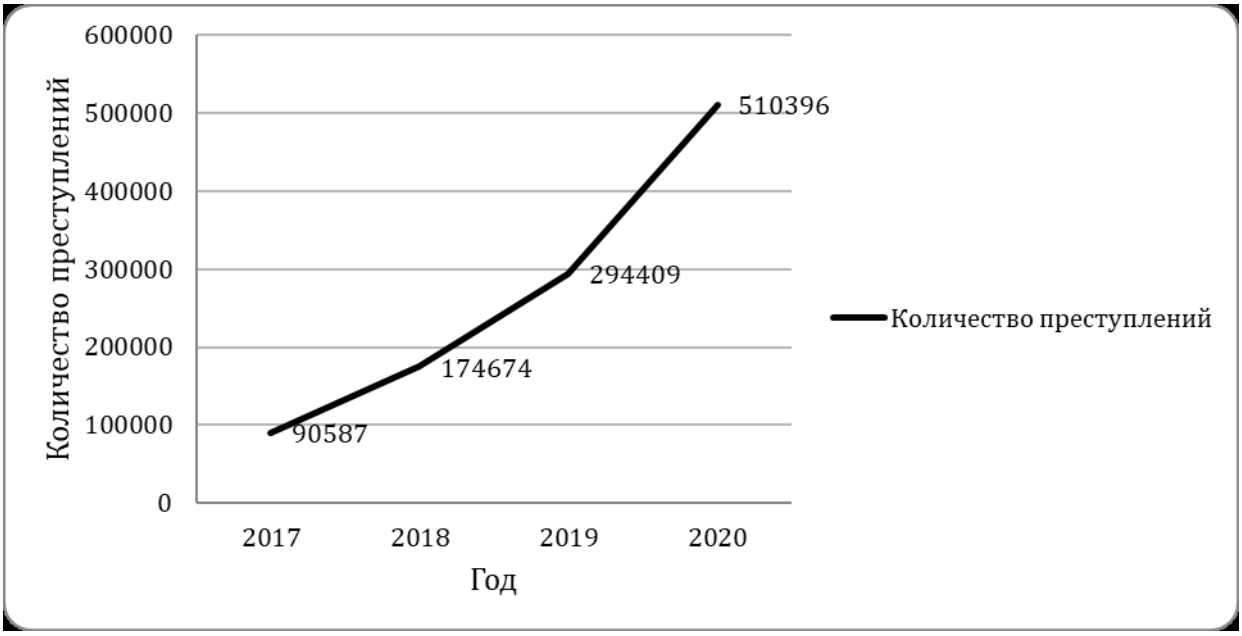

Рисунок 1. Количество официально зарегистрированных преступлений в 2017–2020 гг., совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[26]

Представленные данные свидетельствуют о стабильно высоком росте количества регистрируемых киберпреступлений в последние годы в России. По всей видимости, в 2021 г. повышательный тренд сохранится: в период с января по август текущего года зарегистрировано 358,8 тысяч преступлений, что на 12,7% больше, чем за аналогичный период прошлого года[27].

[26] Составлено автором на основании: Состояние преступности в Российской Федерации за январь–декабрь 2017 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/12167987/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2018 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/16053092/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2019 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/19412450/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2020 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 01.09.2021).

[27] Краткая характеристика состояния преступности в Российской Федерации за январь–август 2021 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/26023627/ (дата обращения: 12.10.2021).

Сложившаяся ситуация серьезна, находит отклик среди общественности. В СМИ проблему кибермошенничества сравнивали с пандемией, отмечали волны кибератак, а россиян называли «легкой добычей»[28].

Рост интереса к проблеме кибермошенничества можно отметить и среди рядовых граждан страны. Рассмотрим динамику запросов по словосочетанию «Телефонные мошенники» в России в сервисе Google Trends.

Рисунок 2. Динамика популярности поискового запроса «Телефонные мошенники» в поисковой системе Google на территории РФ в 2016–2021 гг.[29]

Можно отметить заметный рост количества поисковых запросов в 2020 и 2021 гг., на которые пришелся всплеск активности телефонных мошенников. Исследование Tinkoff Data[30] показало, что звонки от спамеров получают 98% россиян, а от мошенников — 90%. Постоянные звонки с неизвестных номеров, большая часть из которых от спамеров и мошенников[31], — новая реальность, в которой вынуждены жить граждане России. В ответ на возникшую проблему, вызывающую раздражение у подавляющего большинства получателей звонков[32], граждане активнее начали интересоваться инструментами защиты. И это показывают данные аналитического сервиса Google Trends (Рисунок 3).

[28] Киберпреступность переросла в пандемию // Ведомости [Электронный ресурс]. URL: https://www.vedomosti.ru/forum/technologii_novoj_realnosti/columns/2020/12/02/849244-kiberprestupnost (дата обращения: 01.09.2021); Эксперты предупредили о волне повторных атак на жертв кибермошенников // РБК [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/09/04/2020/5e8e292f9a79474e49fe1732 (дата обращения: 01.09.2021); Ну и гаджеты: россияне стали самой легкой добычей для кибермошенников // Известия [Электронный ресурс]. URL: https://iz.ru/897320/anna-kaledina/nu-i-gadzhety-rossiiane-stali-samoi-legkoi-dobychei-dlia-kibermoshennikov (дата обращения: 01.09.2021).
[29] Составлено автором с использованием аналитического сервиса Google Trends.
[30] Исследование Tinkoff Data: более 90% россиян сталкиваются со звонками спамеров и мошенников // Сайт компании «Тинькофф Банк» [Электронный ресурс]. URL: https://www.tinkoff.ru/about/news/17052021-tinkoff-data-study-more-than-90-percent-russians-video-calls-spammers-scammers/ (дата обращения: 01.09.2021).
[31] Там же.
[32] Там же.

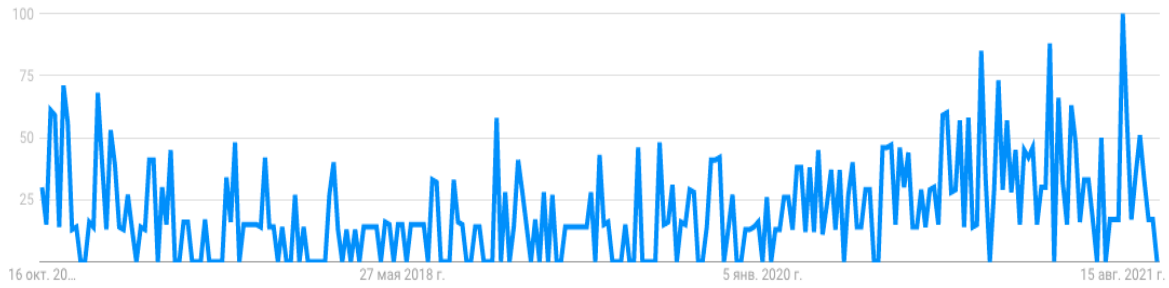

Рисунок 3. Динамика популярности запроса «Антиспам» в поисковой системе Google на территории РФ в 2016–2021 гг.[33]

Рост популярности запроса пришелся на начало 2020 г. и усилился в 2021 г., совпадая с волной мошеннических звонков в России: люди, столкнувшись с проблемой, пытаются решить ее самостоятельно, в том числе с помощью специальных антиспам-сервисов.

Помимо общего количества киберпреступлений, особого внимания заслуживает доля киберпреступлений среди всех зарегистрированных преступлений в России (Рисунок 4).

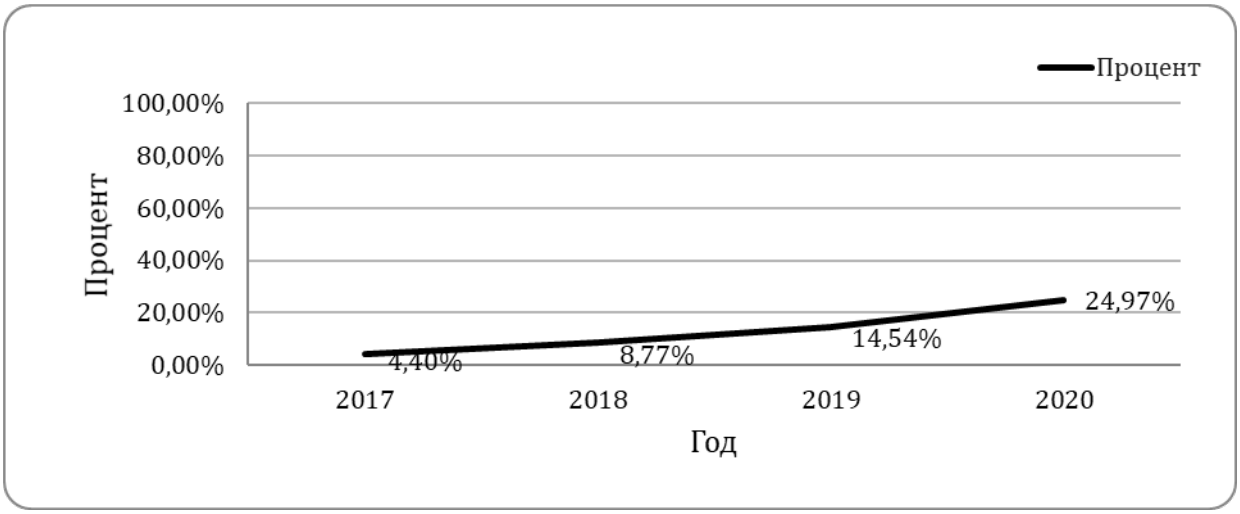

Рисунок 4. Доля (в процентах) киберпреступлений по годам среди всех зарегистрированных преступлений в 2017–2020 гг.[34]

За четыре года произошел более чем пятикратный рост: в 2020 г. почти каждое четвертое преступление совершалось с использованием информационно-телекоммуникационных технологий. В 2021 г. стремительный рост доли преступлений продолжился и по состоянию на август 2021 г. составляет 26,5%[35]. Таким образом, на текущий момент киберпреступление является одной из самых быстро растущих категорий преступлений в России. В наиболее

[33] Составлено автором с использованием аналитического сервиса Google Trends.
[34] Составлено автором на основании: Состояние преступности в Российской Федерации за январь–декабрь 2017 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/12167987/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2018 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/16053092/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2019 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/19412450/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2020 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 01.09.2021).
[35] Краткая характеристика состояния преступности в Российской Федерации за январь-август 2021 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/26023627/ (дата обращения: 01.09.2021).

экономически развитых субъектах в январе–августе 2021 г. показатель приблизился к 40%[36]: в Москве — 39,7%, в Санкт-Петербурге — 38,9%. По всей видимости, сложившийся устойчивый тренд на увеличение доли киберпреступлений по всей стране в ближайшее время сохранится, а крупнейшие города России показывают «опережающее развитие» в данном процессе.

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

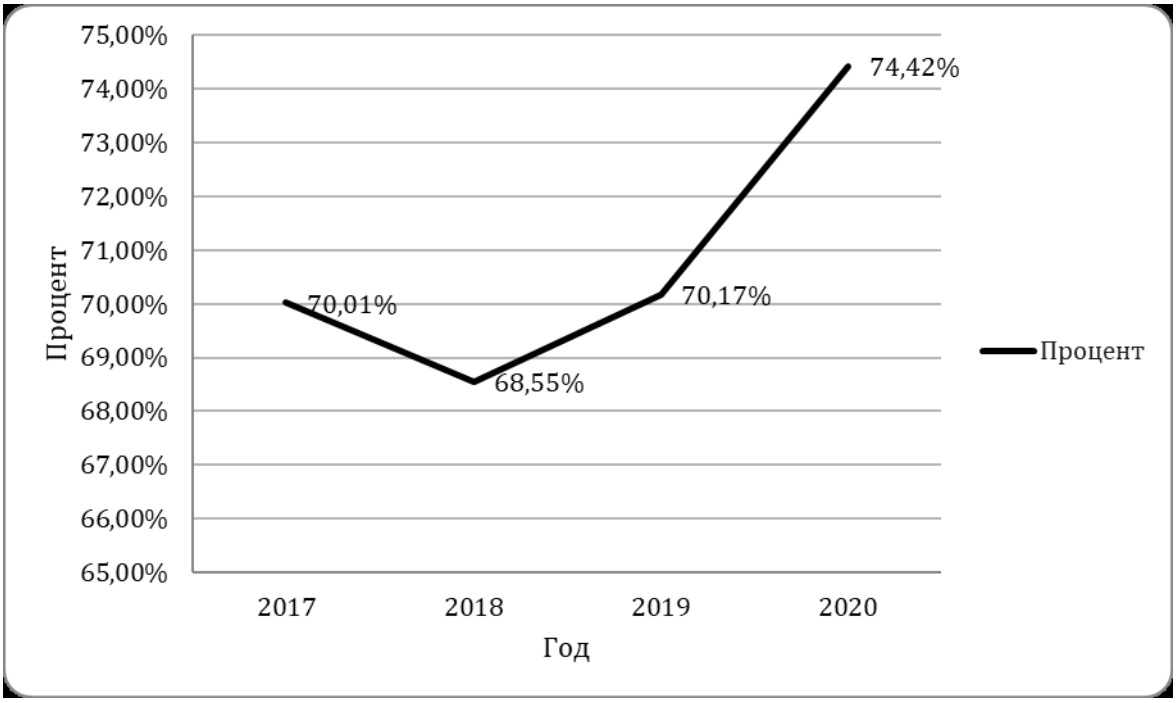

Рисунок 5. Доля нераскрытых киберпреступлений относительно всех зарегистрированных преступлений в 2017–2020 гг.[37]

Доля нераскрытых киберпреступлений не только остается на стабильно высоком уровне — в районе 70%, но и показывает небольшой рост в последние три года, несмотря на активную деятельность российских государственных органов и организаций, особенно банковского сектора.

Причины роста числа киберпреступлений

Прямо сейчас мы наблюдаем мощную волну цифровизации преступной деятельности, активное использование технологий при совершении противоправных действий. Но какие причины привели к столь резкому росту активности киберпреступников в последние годы? Перечислим ключевые факторы, которые, по нашему мнению, способствовали возникновению негативной ситуации с состоянием киберпреступности в стране.

Во-первых, дисбаланс между темпами цифровизации в России и ростом уровня цифровых компетенций граждан страны. Масштабы цифровизации в России велики: например, на 2020 г. пришелся рекорд по количеству выданных банковских карт[38], активное использование

[36] Там же.
[37] Составлено автором на основании: Состояние преступности в Российской Федерации за январь–декабрь 2017 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/12167987/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2018 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/16053092/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2019 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/19412450/ (дата обращения: 01.09.2021); Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2020 г. // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 01.09.2021).
[38] Банки в год пандемии увеличили выдачи карт до рекорда за семь лет // РБК [Электронный ресурс]. URL: https://www.rbc.ru/finances/06/03/2021/60422c739a79471a763211a7 (дата обращения: 01.09.2021).

безналичных способов оплаты[39], рост аудитории соцсетей[40] и их активности[41]. Наряду с этим сохраняется низкий уровень компетенций россиян в сфере цифровых технологий: согласно исследованию НАФИ, с 2019 г. остается неизменным количество россиян с продвинутым уровнем цифровых компетенций — 27%[42]. Авторы подчеркивают, что многие граждане до сих пор обладают недостаточными знаниями и навыками в сфере информационных технологий, необходимыми для безопасного использования цифровых продуктов. Стоит оговориться, что высокий уровень цифровых компетенций не гарантирует полную защиту от киберпреступников, особенно использующих методы социальной инженерии, однако снижает вероятность стать жертвой мошенников. На текущий момент сложилась ситуация, когда многие граждане вынужденно или добровольно пользуются цифровыми продуктами, не имея для этого достаточного уровня знаний и навыков. Такие обстоятельства — благодатная почва для роста кибермошенничества. Например, по состоянию на 2021 г. более 70% пенсионеров в России получают выплаты на банковские карты[43]. Пожилые люди — один из наиболее уязвимых слоев населения, что подтверждается исследованиями: например, пожилой возраст положительно связан с общим уровнем доверия, в том числе и к незнакомцам [Li, Fung 2013, 352]. Данной особенностью пожилых людей нередко пользуются мошенники, эксплуатируя доверие людей преклонного возраста и совершая в отношении них финансовые преступления [DeLiema 2018, 706]. В течение пандемии пенсионерам и семьям с детьми периодически производились единовременные массовые выплаты от государства, что также привлекало внимание мошенников[44].

Часто и сами граждане создают благоприятные условия для совершения в отношении них киберпреступлений, разглашая личную информацию в соцсетях, которой эффективно пользуются преступники[45], которые совершают действия по распространению вирусов, финансовому мошенничеству, краже аккаунтов [Yulianto et al. 2016, 207]. Особенно часто стали применяться методы социальной инженерии, которые показывают высочайший уровень эффективности, принуждая человека совершать порой абсолютно абсурдные вещи, например выбрасывать собственные сбережения в окно[46]. Неудивительно, что преступления с использованием методов социальной инженерии рассматриваются как серьезная угроза безопасности не только отдельно взятого человека, но и информационных сетей различных организаций [Conteh, Nabie 2016, 8]. Факты свидетельствуют о том, что в обозримом будущем именно такого рода преступления будут наиболее распространенными среди всех видов киберпреступлений [Breda et al. 2017].

Во-вторых, недостаточный уровень эффективности в противодействия киберпреступной деятельности: низкий уровень компетенций со стороны правоохранительных органов, несовершенство антифрод-инфраструктуры. Проблема подчеркивается в том числе и высшим

[39] Доля безналичных платежей в России достигла 70% // Ведомости [Электронный ресурс]. URL: https://www.vedomosti.ru/finance/news/2021/02/12/857761-dolya-beznalichnih-platezhei-v-rossii-dostigla-70 (дата обращения: 01.09.2021).
[40] Instagram обошел «ВКонтакте» по числу активных авторов в России // РБК [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/30/11/2020/5fc4aa2c9a7947f4bfbce6db (дата обращения: 01.09.2021).
[41] «Вконтакте» отметил рост активности пользователей // РИА Новости [Электронный ресурс]. URL: https://ria.ru/20211005/vkontakte-1753089397.html (дата обращения: 17.10.2021).
[42] Вынужденная цифровизация: исследование цифровой грамотности россиян в 2021 г. // НАФИ [Электронный ресурс]. URL: https://nafi.ru/analytics/vynuzhdennaya-tsifrovizatsiya-issledovanie-tsifrovoy-gramotnosti-rossiyan-v-2021-godu/ (дата обращения: 01.09.2021).
[43] Голикова: 30,7 млн пенсионеров получат на карту 10 тысяч рублей 2 сентября // Российская газета [Электронный ресурс]. URL: https://rg.ru/2021/08/30/golikova-307-mln-pensionerov-poluchat-na-kartu-10-tysiach-rublej-2-sentiabria.html (дата обращения: 01.09.2021).
[44] Компенсация (не) полагается: «Лаборатория Касперского» обнаружила в Google Play новые фейковые приложения с социальными выплатами // АО «Лаборатория Касперского» [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2021_kompensaciya-ne-polagaetsya-laboratoriya-kasperskogo-obnaruzhila-v-google-play-novye-fejkovye-prilozheniya-s-socialnymi-vyplatami (дата обращения: 01.09.2021).
[45] ЦБ: россияне слишком доверяют социальным сетям, и этим пользуются мошенники // ТАСС [Электронный ресурс]. URL: https://tass.ru/interviews/6577000 (дата обращения: 01.09.2021).
[46] Мошенники стали просить россиян выбрасывать деньги в окно // Lenta.ru [Электронный ресурс]. URL: https://lenta.ru/news/2021/06/18/guliki/ (дата обращения: 01.09.2021).

руководством правоохранительных органов. Так, начальник Главного управления международно-правового сотрудничества Генпрокуратуры РФ Петр Городов сообщил[47], что правоохранительные органы отстают от киберпреступников в техническом обеспечении и инструментах связи. Генпрокурор РФ Игорь Краснов на фоне растущего числа киберпреступлений заявил о том, что правоохранительные органы практически не могут противостоять киберпреступности[48]. Следствием недостаточного уровня компетенций правоохранительных органов становится низкий процент раскрываемости киберпреступлений, который продолжает снижаться в последние несколько лет. Стоит подчеркнуть, что проблема быстрого роста количества преступлений существовала и до пандемии, и не заметить ее было невозможно. На основании представленных в статье данных можно отметить, что ежегодно практически удваивалось количество совершаемых киберпреступлений в России в 2018 и 2019 гг., а их доля среди всех преступлений с 2017 по 2019 гг. увеличилась в 3,3 раза. Тем не менее активных действий со стороны властей в допандемийный период не предпринималось: например, еще в 2015 г. была направлена инициатива о создании подразделения МВД по борьбе с преступлениями в соцсетях[49], в 2019 г. Владимир Путин усомнился в необходимости создания киберполиции[50]. В 2021 г. президент уже констатировал проблему с раскрываемостью киберпреступлений в стране[51].

Помимо низкой раскрываемости, существуют проблемы со скоростью реагирования на активность кибермошенников. Так, на Прямой линии с Владимиром Путиным в 2021 г. президент отметил, что сейчас на блокировку мошеннических фишинговых сайтов уходит до трех дней, хотя ранее уходили недели или даже месяцы[52]. Одна из особенностей фишинга — это его хорошая масштабируемость[53], и деятельность мошеннического сайта даже в течение нескольких минут может нанести значительный урон. Защита граждан от фишинговых сайтов — важный аспект информационной безопасности [Alsharnouby et al. 2015, 69], и стоит констатировать, что на текущий момент скорость реакции российских правоохранительных органов на такого рода преступную активность все еще недостаточно оперативная, несмотря на положительную динамику.

Таким образом, несколько лет назад был незамечен или проигнорирован тренд на зарождение новой масштабной социальной проблемы в России — киберпреступности. Было упущено время на работу с населением, подготовку инфраструктуры, соответствующих подразделений, налаживание международного сотрудничества и выстраивание законодательной базы. Сейчас можно наблюдать поспешные действия в попытке исправить ситуацию, которая становится все более критической: создание в МВД РФ и Следственном комитете подразделений по борьбе с киберпреступностью, работа по информированию граждан о новых видах мошеннических схем, запуск специальной платформы для борьбы с мошенничеством, международное сотрудничество на высочайшем уровне, технологии по определению телефонных мошенников со стороны банковского сектора.

[47] ГП: правоохранительные органы отстают в технических возможностях от киберпреступников // ТАСС [Электронный ресурс]. URL: https://tass.ru/politika/8915711 (дата обращения: 01.09.2021).
[48] Генпрокурор РФ заявил о бессилии правоохранительных органов перед киберпреступниками // Интерфакс [Электронный ресурс]. URL: https://www.interfax.ru/russia/699548 (дата обращения: 01.09.2021)
[49] МВД просят заняться фейковыми аккаунтами и «троллями» в соцсетях // Известия [Электронный ресурс]. URL: https://iz.ru/news/585245 (дата обращения: 01.09.2021).
[50] Путин усомнился в необходимости киберполиции // Коммерсантъ [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4082595 (дата обращения: 01.09.2021).
[51] Путин словами «мы не успеваем» объяснил рост числа преступлений в ИТ // РБК [Электронный ресурс]. URL: https://www.rbc.ru/politics/03/03/2021/603f6ae59a7947b29b0e9b18 (дата обращения: 01.09.2021).
[52] Путин назвал подонками обманывающих пенсионеров телефонных мошенников // Известия [Электронный ресурс]. URL: https://iz.ru/1186294/2021-06-30/putin-nazval-podonkami-obmanyvaiushchikh-pensionerov-telefonnykh-moshennikov (дата обращения: 01.09.2021).
[53] Lastdrager E. From Fishing to Phishing: Ph.D. Thesis. Enschede, 2018. P. 5. DOI: 10.3990/1.9789036544795.

Тем не менее сторона противодействия преступной деятельности в данном противостоянии занимает на текущий момент отстающую позицию: количество киберпреступлений продолжает расти, что и показали результаты исследования в рамках данной статьи.

Заключение

Результаты представленного анализа официальной статистики показали, что в России в последние годы наблюдается взрывной рост киберпреступлений, особенно усилившийся в период пандемии COVID-19. Стоит констатировать, что предпосылки зарождения и развития киберпреступности формировались в России в течение последних нескольких лет. Во-первых, это цифровизация различных сторон жизнедеятельности россиян: например, высокий интерес к банковским картам и счетам, безналичным способам оплаты, онлайн-досуг и активное использование соцсетей. Во-вторых, сохраняющийся низкий уровень цифровых компетенций граждан страны. В-третьих, низкая квалификация правоохранительных органов, несовершенство антифрод-инфраструктуры, неспособность оперативно пресекать киберпреступную деятельность и эффективно расследовать инциденты в цифровой среде. В данный момент большинство мер со стороны государства не предупреждающие, а контрмеры в ответ на уже совершенные преступления [Дерюгин 2019, 48]. За несколько лет в России сформировалась ситуация, когда большое количество новых неопытных пользователей вступили в незнакомую для себя цифровую среду, не осознавая всех рисков и опасностей своих действий. Ситуация усугубилась недостаточным уровнем подготовленности правоохранительных органов и антифрод-инфраструктуры, что в результате привело к неконтролируемому росту киберпреступности в стране, низкому проценту раскрываемости, малоэффективному противодействию преступной деятельности и невысокой скорости реагирования на кибермошенничество.

Пандемия COVID-19 и вынужденная форсированная цифровизация в России в связи с самоизоляцией послужили лишь катализаторами тех проблем, которые формировались на протяжении нескольких лет до начала «коронакризиса». Сегодня, когда о проблеме кибермошенничества говорят уже повсюду, важно сначала замедлить, а впоследствии остановить высокие на текущий момент темпы прироста новых случаев киберпреступлений. По нашему мнению, для решения этой комплексной, сложной и многогранной проблемы требуется масштабная и долгосрочная кооперативная работа государственных и правоохранительных органов, коммерческих и некоммерческих организаций, научного сообщества, активное взаимодействие с международными партнерами. Для эффективного противодействия виртуальным преступникам необходима многоуровневая институциональная система кибербезопасности, которая защищала бы и простых граждан, и государственные институты [Карпова 2014, 48]. Сейчас становится очевидным, что киберпреступность — это не просто социальная проблема, а вызов всему российскому обществу, который требует незамедлительного и жесткого ответа.

Список литературы:

Дерюгин Р.А. Киберпреступность в России: современное состояние и Актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 2. С. 46–49.

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

Протасевич А.А., Зверянская Л.П. Борьба с киберпреступностью как актуальная задача современной науки // Всероссийский криминологический журнал. 2011. № 3. С. 28–33.

Alsharnouby M., Alaca F., Chiasson S. Why Phishing Still Works: User Strategies for Combating Phishing Attacks // International Journal of Human-Computer Studies. 2015. Vol. 82. P. 69–82. DOI: https://doi.org/10.1016/j.ijhcs.2015.05.005.

Breda F., Barbosa H., Morais T. Social Engineering and Cyber Security // Education and Development Conference. Valencia, Spain. 6–8 March. 2017. P. 4204–4211. DOI: 10.21125/inted.2017.1008.

Conteh N.Y., Royer M.D. The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor // International Journal of Computer (IJC). 2016. Vol. 20. № 1. P. 1–12.

DeLiema M. Elder Fraud and Financial Exploitation: Application of Routine Activity Theory // Gerontologist. 2018. Vol. 58. Is. 4. P. 706–718. DOI: 10.1093/geront/gnw258.

Fors A. The Ontology of the Subject in Digitalization // Handbook of Research on Technoself: Identity in a Technological Society / ed. by R. Luppicini. Hershey, PA: IGI Global, 2013. P. 45–63. DOI: https://doi.org/10.4018/978-1-4666-2211-1.ch003.

Kameneva T. Didactics of Digital Century: Issues and Trends of E-Learning Development. Фізико-математична освіта: науковий журнал. 2020. № 4 (26). С. 13–20. DOI: https://doi.org/10.31110/2413-1571-2020-026-4-002.

Li T., Fung H. Age Differences in Trust: An Investigation Across 38 Countries // Journals of Gerontology Series B: Psychological Sciences and Social Sciences. 2013. Vol. 68. Is. 3. P. 347–355. DOI: https://doi.org/10.1093/geronb/gbs072.

Monteith S., Bauer M., Alda M., Geddes J., Whybrow P., Glenn T. Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry // Current Psychiatry Reports. 2021. Vol. 23. Is. 4. DOI: 10.1007/s11920-021-01228-w.

Stanciu V., Tinca A. Exploring Cybercrime — Realities and Challenges // Journal of Accounting and Management Information Systems. 2017. Vol. 16. Is. 4. P. 610–632. DOI: 10.24818/jamis.2017.04009.

Yulianto B., Purnomo F., Madyatmadja E., Meyliana M., Prabowo H. Potential Threats of Information Disclosure in Social Media: A Systematic Literature Review // ComTech Computer Mathematics and Engineering Applications. 2016. Vol. 7. Is. 3. P. 201–211. DOI: https://doi.org/10.21512/comtech.v7i3.2499.

References:

Alsharnouby M., Alaca F., Chiasson S. (2015) Why Phishing Still Works: User Strategies for Combating Phishing Attacks. *International Journal of Human-Computer Studies*. Vol. 82. P. 69–82. DOI: https://doi.org/10.1016/j.ijhcs.2015.05.005.

Breda F., Barbosa H., Morais T. (2017) Social Engineering and Cyber Security. *Education and Development Conference.* Valencia, Spain. 6–8 March. P. 4204–4211. DOI: 10.21125/inted.2017.1008.

Conteh N.Y., Royer M.D. (2016) The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor. *International Journal of Computer (IJC).* Vol. 20. No. 1. P. 1–12.

DeLiema M. (2018) Elder Fraud and Financial Exploitation: Application of Routine Activity Theory. *Gerontologist*. Vol. 58. Is. 4. P. 706–718. DOI: 10.1093/geront/gnw258.

Deryugin R.A. (2019) Cybercrime in Russia: Modern Condition and Actual Problems. *Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii*. No. 2. P. 46–49.

Fors A. (2013) The Ontology of the Subject in Digitalization. In: Luppicini R. (ed.) *Handbook of Research on Technoself: Identity in a Technological Society.* Hershey, PA: IGI Global. P. 45–63. DOI: https://doi.org/10.4018/978-1-4666-2211-1.ch003.

Kameneva T. (2020) Didactics of Digital Century: Issues and Trends of E-Learning Development. *Fiziko-matematichna osvita: naukoviy zhurnal.* No. 4 (26). P. 13–20. DOI: https://doi.org/10.31110/2413-1571-2020-026-4-002.

Karpova D.N. (2014) Cybercrime: A Global Challenge and Its Solution. *Vlast'.* No. 8. P. 46–50.

Li T., Fung H. (2013) Age Differences in Trust: An Investigation Across 38 Countries. *Journals of Gerontology Series B: Psychological Sciences and Social Sciences* Vol. 68. Is. 3. P. 347–355. DOI: https://doi.org/10.1093/geronb/gbs072.

Monteith S., Bauer M., Alda M., Geddes J., Whybrow P., Glenn T. (2021) Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports.* Vol. 23. Is. 4. DOI: 10.1007/s11920-021-01228-w.

Protasyevich A.A., Zveryanskaya L.P. (2011) Fighting Cybercrimes as an Urgent Task for Contemporary Research. *Vserossiyskiy kriminologicheskiy zhurnal.* No. 3. P. 28–33.

Stanciu V., Tinca A. (2017) Exploring Cybercrime — Realities and Challenges. *Journal of Accounting and Management Information Systems.* Vol. 16. Is. 4. P. 610–632. DOI: 10.24818/jamis.2017.04009.

Yulianto B., Purnomo F., Madyatmadja E., Meyliana M., Prabowo H. (2016) Potential Threats of Information Disclosure in Social Media: A Systematic Literature Review. *ComTech Computer Mathematics and Engineering Applications.* Vol. 7. Is. 3. P. 201–211. DOI: https://doi.org/10.21512/comtech.v7i3.2499.

Дата поступления/Received: 01.09.2021