Развитие территорий. 2022. № 4. С. 42—48.
Territory Development. 2022;(4):42—48.

Информационные системы и процессы

Научная статья
УДК: 311:343.9
DOI: 10.32324/2412-8945-2022-4-42-48

СТАТИСТИЧЕСКИЙ АНАЛИЗ ТЕНДЕНЦИЙ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ В УСЛОВИЯХ СОВРЕМЕННОЙ ЭКОНОМИКИ

Мария Николаевна Белоусова[1]✉, Виталий Андреевич Белоусов[2], Ольга Михайловна Данилина[3]
[1, 2, 3] Государственный университет управления, Москва, Российская Федерация
Автор, ответственный за переписку: Мария Николаевна Белоусова, mn_belousova@guu.ru

Аннотация. Статья посвящена исследованию проблем распространения проявлений киберпреступности, которые приобрели большую популярность в последнее время. Проведен анализ сведений о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий в России в 2019—2022 гг. Рассмотрено развитие актуальных информационных угроз по кварталам за 2019—2022 гг.: мобильных угроз, новых модификаций шифровальщиков, мобильных банковских троянцев, мобильных троянцев-вымогателей. Проведен статистический анализ тенденций развития киберпреступности, построены оптимистический и пессимистический прогнозы информационных угроз.

Ключевые слова: киберпреступность, статистический анализ, прогноз, кибератаки, информационные угрозы
Для цитирования: Белоусова М. Н., Белоусов В. А., Данилина О. М. Статистический анализ тенденций развития киберпреступности в условиях современной экономики // Развитие территорий. 2022. № 4. С. 42—48. DOI: 10.32324/2412-8945-2022-4-42-48.

Information systems and processes

Original article

STATISTICAL ANALYSIS OF TRENDS IN CYBERCRIME IN TODAY'S ECONOMY

Mariya N. Belousova[1]✉, Vitaliy A. Belousov[2], Olga M. Danilina[3]
[1, 2, 3] State University of Management, Moscow, Russian Federation
Corresponding author: Mariya N. Belousova, mn_belousova@guu.ru

Abstract. The The article is devoted to the study of the problems of the spread of cybercrime, which has recently become very popular. We analyze information about crimes committed with the use of information and telecommunication technologies in Russia in 2019-2022. We consider the development of actual information threats by quarters for 2019-2022: mobile threats, new modifications of encryptors, mobile banking Trojans, mobile Trojan-extortionists. Statistical analysis of cybercrime development trends and optimistic and pessimistic forecasts of information threats were made.

Keywords: cybercrime, statistical analysis, forecast, cyber attacks, information threats
For citation: Belousova M.N., Belousov V.A., Danilina O.M. Statistical analysis of trends in cybercrime in today's economy. *Territory Development*. 2022;(4):42—48. (In Russ.). DOI: 10.32324/2412-8945-2022-4-42-48.

Введение

Сегодня информация является главным аспектом любой деятельности. Использование современных компьютеров для передачи информации предоставило обществу много возможностей: быструю передачу адресату, легкость обработки, простоту манипуляций и доступ к ней. Новейшие технологии способствуют замене человеческой деятельности машинами, что приводит к зависимости общества от компьютеров. С развитием информационных технологий все предприятия, учреждения, организации начали использовать компьютеры и другие новейшие гаджеты, а указанный процесс получил название «автоматизация».

Благодаря всеобщему распространению указанного процесса компьютерная сеть образовала отдельный мир — киберпространство. Поскольку такое пространство имеет особый характер, компьютерные технологии облегчили совершение преступлений традиционного характера, к которым можно отнести шпионаж, мошенничество, кражу, личное оскорбление (клевету), распространение порнографии. Также компьютерные технологии способствовали возникновению новых видов уголовных преступлений: хищение компьютерной информации, DoS-атаки, распространение вредоносных программ (вирусов), фишинг, кибертерроризм (компьютерный экстремизм), удаление программ или данных, рассылка писем (спам), создание ложных интернет-аукционов и т. п.

В настоящее время киберпреступность стала серьезной межгосударственной и транснациональной проблемой.

Вопросам кибербезопасности нашей страны уделяли внимание многочисленные ученые. Так,

Д. А. Тершуков обосновал необходимость информационной безопасности как составной части национальной безопасности страны [1]. Кроме того, проблемы информационной безопасности исследовались в научных трудах А. В. Шободоевой [2], Е. А. Муньковой [2].

Отдельные аспекты развития и становления информационных отношений, вопросы осуществления противодействия киберпреступности рассматривались ведущими отечественными учеными Т. А. Гончаровой [3], Л. В. Набоковым [3], Н. А. Казаковой [4], А. А. Петюковой [4], Б. А. Тарчоковым [5]. Однако указанные исследования в основном сосредоточены на теоретических аспектах киберпреступности. Впрочем беспокойство, связанное с масштабами и влиянием пандемии COVID-19, заставляет предприятия анализировать текущую ситуацию и разрабатывать меры, которые следует принять для защиты информации.

Целью исследования является анализ тенденций развития киберпреступности, построение оптимистичного и пессимистичного прогнозов. Использованы методы математической статистики; метод скользящей средней для прогнозирования; методы общей теории статистики, а именно относительных, абсолютных и средних величин, методы синтеза и анализа. Для наглядного отображения статистических данных применялись графический и табличный методы визуализации данных.

Проведем анализ сведений о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в России [6].

Анализируя данные за период с октября 2019 по май 2022 г., следует отметить рост числа следующих преступлений: совершенных с использованием или применением расчетных (пластиковых) карт (на 79 %), программных средств (на 21 %), фиктивных электронных платежей (на 12 %), сети Интернет (на 34 %), средств мобильной связи (на 29 %), мошенничество в сфере информации (на 41 %), изготовление порнографических материалов (на 28 %), публичные призывы к осуществлению экстремистской деятельности (на 33 %), неправомерный доступ к компьютерной информации (на 18 %).

Следует выделить и отрицательный прирост по отдельным статьям: преступления, совершенные с использованием или применением компьютерной техники (на 15 %), незаконные организация и проведение азартных игр (на 83 %), публичные призывы к осуществлению террористической деятельности (на 15 %), создание, использование и распространение вредоносных компьютерных программ (на 41 %).

При этом следует отметить, что количество преступлений по статьям фиктивных электронных платежей, мошенничества в сфере компьютерной информации, публичные призывы к осуществлению террористической и экстремистской деятельности, создание, использование и распространение вредоносных компьютерных программ являются незначительными и в целом не влияют на общую картину компьютерной преступности в России.

По нашему мнению, в период с февраля 2020 по декабрь 2021 г. мировая пандемия COVID-19 послужила обострению проблем, связанных с кибербезопасностью, так как кризисные ситуации традиционно вызывают активизацию различных хакерских группировок. Основные факторы, которые потенциально способствуют повышению деструктивной (противозаконной) киберативности:

1) практика введения режима карантина ведет к стимулированию работодателей изменять характер производственных отношений с работниками на условиях удаленной работы. В большинстве случаев такие взаимодействия происходят с помощью сети Интернет. Следовательно, количество потенциально уязвимых соединений, которые могут привести к компрометации информации о самой организации или о ее работниках, увеличивается;

2) ограничения на передвижение, максимальное ограничение наличных расчетов, а также увеличение времени, которое граждане проводят дома, приводит не только к росту времени пользования сетью Интернет в целом, но и к интенсификации электронных платежей, что также стимулирует мошенническую деятельность;

3) кризисы и паника всегда использовались хакерами в их деятельности. В такие периоды традиционно возрастает количество фишинговых атак — увеличение фальшивых писем (с malware-вложениями) и фальшивых сайтов (для сбора персональной и банковской информации граждан).

Хакеры умело маскируют свои атаки под информирование граждан о развитии пандемии. Чаще всего, чтобы ввести в заблуждение, они используют в своих фишинг-рассылках актуальные слова: «дезинфицирующие средства», «лекарства», «вакцины», «тесты», «медицинские маски», «перчатки» и т. п. Также распространенными стали ссылки на сайтах «отслеживание COVID-19», которые на самом деле являются ссылками на фишинговые сайты, которые похищают логины и пароли пользователей глобальной сети Интернет. Увеличилось и количество мошеннических (фишинговых) сайтов, которые «работают» под видом платежных онлайн-сервисов, а на самом деле — похищают средства или карточные реквизиты.

На основе данных компании «Positive technology» [7] за декабрь 2018 — май 2022 г. были построены оптимистичный и пессимистичный прогнозы количества кибератак на сентябрь и ноябрь 2022 г. (рис. 1).

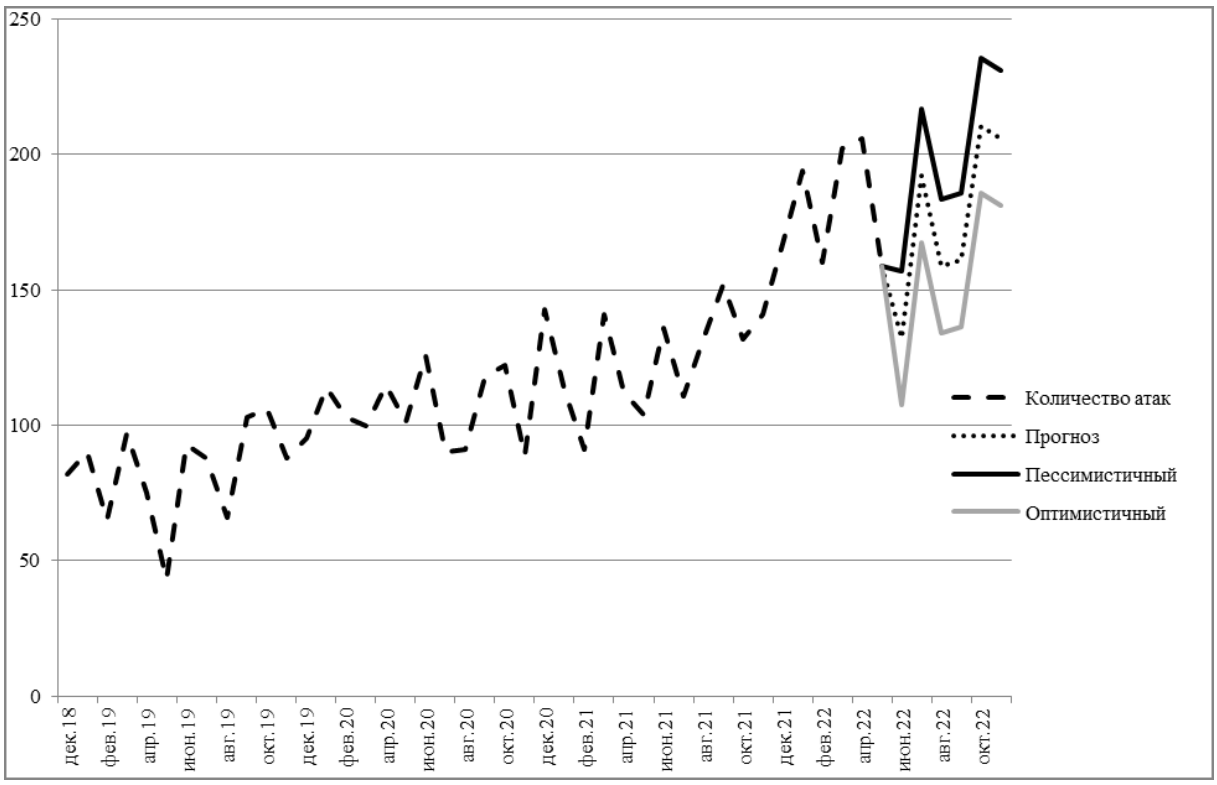

Рис. 1. Количество кибератак за 2018—2022 гг. по месяцам
Number of cyberattacks for 2018-2022 by month

На основе данных лаборатории Касперского [8 ; 9] был проведен анализ развития информационных угроз по всему миру по кварталам, за период III квартал 2019 — II квартал 2022 г.

Так, за исследуемый период сократилось количество мобильных угроз на 22 %, новых модификаций шифровальщиков — на 68 %, возросло на 97 % количество мобильных банковских троянцев, уменьшилось на 96 % количество мобильных троянцев-вымогателей (таблица).

Развитие информационных угроз по всему миру по кварталам, за период III квартал 2019 — II квартал 2022 г., количество пакетов
The development of information threats around the world by quarter, for the period III quarter 2019 — II quarter 2022, number of packages

Квартал	Мобильные угрозы	Новые модификации шифровальщиков	Мобильные банковские троянцы	Мобильные троянцы-вымогатели
Q3 2019	1 598 196	13 693	19 748	108 073
Q4 2019	1 479 967	18 305	13 606	17 355
Q1 2020	1 322 578	5 236	18 912	8 787
Q2 2020	1 744 244	7 620	61 045	14 119
Q3 2020	1 305 015	5 195	55 101	13 075
Q4 2020	1 001 019	8 632	18 501	24 020
Q1 2021	905 174	5 222	29 841	27 928
Q2 2021	753 550	16 017	13 899	23 294
Q3 2021	870 617	13 138	13 129	13 179
Q4 2021	980 993	17 686	15 410	5 406
Q1 2022	1 152 662	5 225	42 115	4 339
Q2 2022	1 245 894	4 406	38 951	3 805
Темп роста Q2 2022 к Q3 2019, %	78	32	197	4

На основе квартальных данных лаборатории Касперского нами были построены оптимистичный и пессимистичный прогнозы следующих угроз: мобильных угроз (рис. 2), мобильных банковских троянцев (рис. 3).

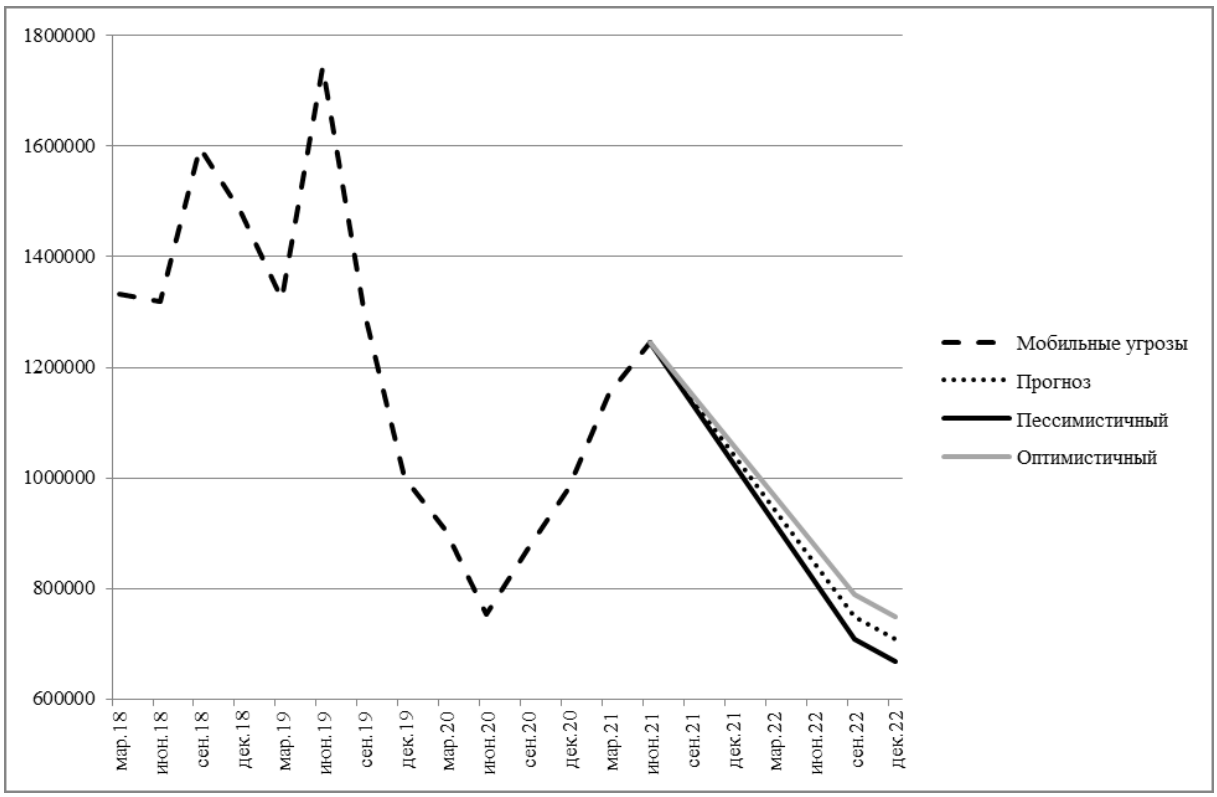

Рис. 2. Количество обнаруженных вредоносных установочных пакетов по кварталам, Q3 2019—2022
Number of detected malicious installation packages by quarter, Q3 2019—2022

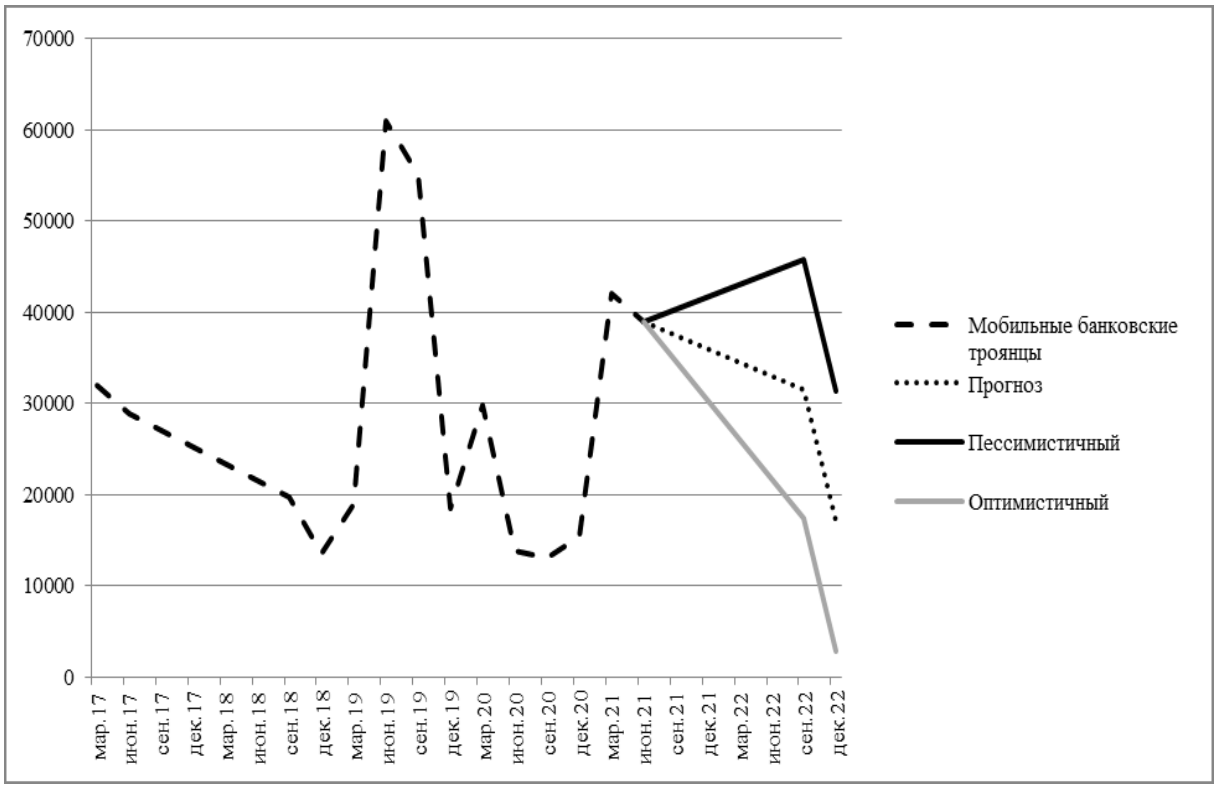

Рис. 3. Количество установочных пакетов мобильных банковских троянцев по кварталам, Q3 2019—2022
Number of mobile banking Trojan installer packages by quarter, Q3 2019—2022

В отчете за 2022 г. компании Kaspersky Security Network, занимающейся кибербезопасностью, говорится, что во время пандемии увеличилось количество сетевых атак, связанных с играми. Так, в марте — апреле 2022 г. количество заблокированных попыток перенаправить пользователей лаборатории Касперского на фишинговые страницы для одной из самых популярных игровых платформ увеличилось на 40 % по сравнению с февралем 2022 г. По данным Kaspersky

Security Network, значительно увеличилось количество ежедневных попыток перенаправить пользователей на вредоносные сайты, использующие игровую тему (в апреле на 54 % больше по сравнению с январем). «Многие из этих атак, связанных с видеоиграми, не особенно изощренны; в их успехе есть большая пользовательская составляющая. Последние несколько месяцев показали, что пользователи очень подвержены фишинговым атакам или переходу по вредоносным ссылкам, когда дело доходит до игр — независимо от того, ищут ли они пиратские версии или хотят получить чит, который поможет им выиграть», — говорится в заявлении эксперта по безопасности в лаборатории Касперского Марии Наместниковой. Чаще всего преступники использовали Minecraft. Его имя использовалось более чем в 130 000 веб-атаках. Другими наиболее популярными играми, используемыми в атаках, были Counter Strike: Global Offensive и The Witcher 3.

Было замечено, что пользователей часто соблазняли такими обещаниями, как бесплатные версии популярных игр, обновления и расширения или читы. Однако, если пользователи переходят по этим ссылкам, могут быть загружены самые разные вредоносные программы — от вредоносных программ для кражи паролей до программ-вымогателей и майнеров, программного обеспечения, которое тайно добывает криптовалюту с компьютера жертвы. «Теперь, когда многие игроки начали использовать те же машины, которые они используют для входа в корпоративные сети для игр, их осторожность должна быть удвоена: рискованные действия делают уязвимыми не только личные данные или деньги, но и корпоративные ресурсы. Работая из дома, по возможности, старайтесь не использовать свой персональный компьютер для доступа к корпоративной сети, — сказал Юрий Наместников, эксперт по безопасности лаборатории Касперского. — Этой весной миллионы людей во всем мире вынуждены были оставаться внутри, поскольку многие страны ввели в действие те или иные меры изоляции или ограничения передвижения». Поскольку дома все больше людей и у них больше свободного времени, многие обратились к доступным онлайн-развлечениям, включая видеоигры. Начиная с марта общее количество пользователей Steam (самая популярная игровая онлайн-платформа, сообщество и магазин) значительно выросло, и к 30 марта платформа достигла рекордного уровня как для активных, так и для одновременных пользователей, играющих в игры. Согласно данным «антифишинговой системы» Касперского, по сравнению с февралем, количество заблокированных перенаправлений на фишинговые страницы, содержащие слово «Steam», в апреле увеличилось на 40 %.

В целом анализ количества веб-атак, использующих игровую тематику, в период с января по май 2022 г. дает следующую картину (рис. 4).

При этом на протяжении трех месяцев — с февраля по апрель 2022 г. — наблюдается рост количества атак семейства Bruteforce (рис. 5).

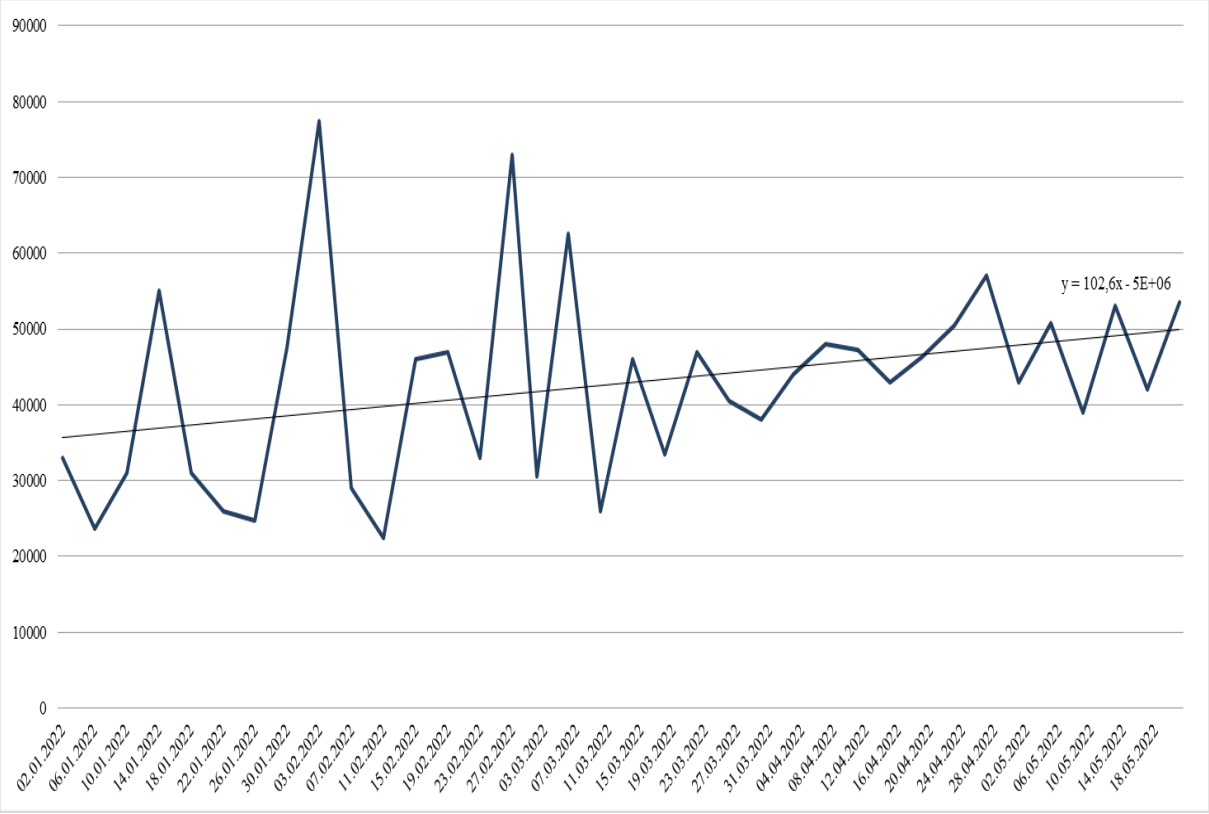

Рис. 4. Количество веб-атак по всему миру, использующих игровую тематику, в период с января по май 2022 г.
Number of web attacks globally that use game-themed attacks between January and May 2022

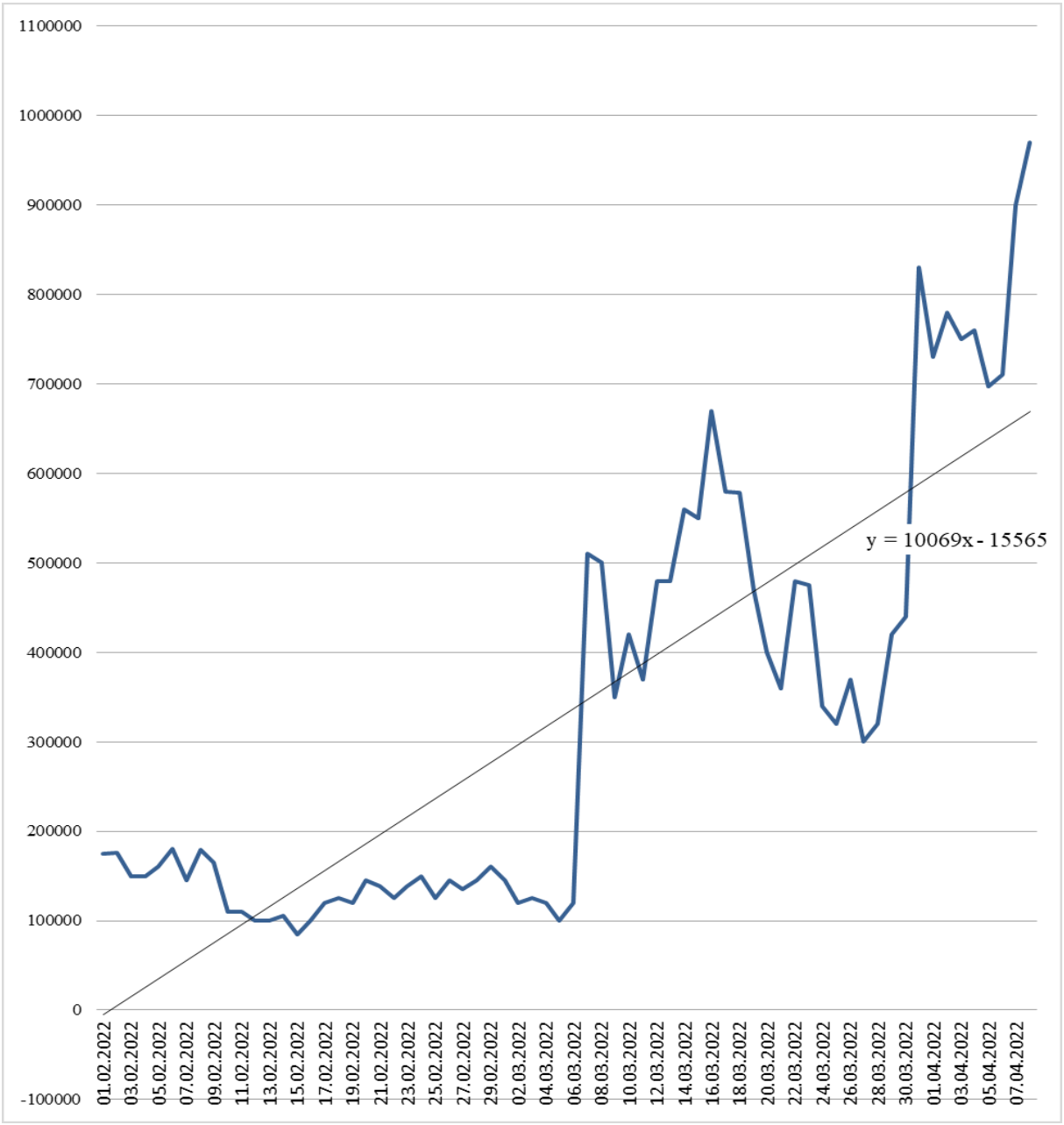

Рис. 5. Количество атак семейства Bruteforce.Generic.RDP, февраль — апрель 2022 г.
Number of Bruteforce.Generic.RDP family attacks, February — April 2022

Проблема киберпреступности на современном этапе исторического развития приобретает глобальный масштаб и представляет угрозу информационному обществу. Статистические данные по числу выявленных киберпреступлений за последние годы указывают на их рост и изменение качественных признаков.

Учитывая вышесказанное, можно сделать вывод о том, что киберпреступность стала проблемой именно в XXI в. в связи с оживленной модернизацией технологий и общества, и с каждым годом количество киберпреступлений, которые поглощают все больше средств, растет. Конечно, принимаются меры по противодействию такому виду преступности, но их недостаточно, поэтому необходимо разрабатывать новые методы борьбы, которые дадут гораздо больше положительных результатов, а также помогут улучшить или разработать системы защиты, дающих возможность избежать или минимизировать такие виды преступлений.

Список источников

1. *Тершуков Д. А.* Анализ современных угроз информационной безопасности // NBI-technologies. 2018. № 3. URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-informatsionnoy-bezopasnosti (дата обращения: 14.05.2022).

2. *Шободоева А. В., Мунькова Е. А.* Угрозы информационной безопасности Российской Федерации // Проблемы обеспечения национальной безопасности в контексте изменения геополитической ситуации. Иркутск, 2017. С. 244—254.

3. *Гончарова Т. А., Набоков Л. В.* Киберпреступность в России: проблемные аспекты и предупреждение преступности // Инновационная экономика и право. 2022. № 1. С. 118—124.

4. *Казакова Н. А., Петюкова А. А.* Анализ развития рынка кибербезопасности в России и за рубежом // Маркетинг в России и за рубежом. 2021. № 1. С. 57—64.

5. *Тарчоков Б. А.* Тенденции развития киберпреступности в глобальном информационном пространстве // Проблемы экономики и юридической практики. 2021. Т. 17, № 1. С. 198—201.

6. *Краткая* характеристика состояния преступности в Российской Федерации за январь-апрель 2022 года. URL: https://мвд.рф/reports/item/30105559 (дата обращения: 14.05.2022).

7. *Данные* экспертизы компании Positive technology. URL: https://ar2021.ptsecurity.com/download/full-reports/ar_ru annual-report_pages_pt_2021.pdf (дата обращения: 14.05.2022).

8. *Данные* Kaspersky Security Network. URL: https://securelist.ru/it-threat-evolution-in-q1-2022-mobile-statistics/105235/ (дата обращения: 14.05.2022).

9. *Развитие* информационных угроз во втором квартале 2020 года. URL: https://securelist.ru/it-threat-evolution-q2-2020/97887/ (дата обращения: 14.05.2022).

References

1. Tershukov D.A. Analiz sovremennykh ugroz informatsionnoi bezopasnosti [Analysis of modern threats to information security], *NBI-technologies*, 2018, no. 3. Available at: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-informatsionnoy-bezopasnosti (accessed: 14.05.2022).

2. Shobodoeva A.V., Mun'kova E.A. Ugrozy informatsionnoi bezopasnosti Rossiiskoi Federatsii [Threats to information security of the Russian Federation], *Problemy obespecheniya natsional'noi bezopasnosti v kontekste izmeneniya geopoliticheskoi situatsii [Problems of National Security in the context of the changing geopolitical situation]*. Irkutsk, 2017, pp. 244—254.

3. Goncharova T.A., Nabokov L.V. Kiberprestupnost' v Rossii: problemnye aspekty i preduprezhdenie prestupnosti [Cybercrime in Russia: problematic aspects and crime prevention], *Innovatsionnaya ekonomika i pravo [Innovative economics and law]*, 2022, no. 1, pp. 118—124.

4. Kazakova N.A., Petyukova A.A. Analiz razvitiya rynka kiberbezopasnosti v Rossii i za rubezhom [Analysis of cybersecurity market development in Russia and abroad], *Marketing v Rossii i za rubezhom* [*Marketing in Russia and abroad*], 2021, no.1, pp. 57—64.

5. Tarchokov B.A. Tendentsii razvitiya kiberprestupnosti v global'nom informatsionnom prostranstve [Trends in cybercrime in the global information space], *Problemy ekonomiki i yuridicheskoi praktiki* [*Problems of economics and legal practice*], 2021, vol. 17, no. 1, pp. 198—201.

6. Kratkaya kharakteristika sostoyaniya prestupnosti v Rossiiskoi Federatsii za yanvar'-aprel' 2022 goda [Summary of the state of crime in the Russian Federation in January-April 2022]. Available at: https://mvd.rf/reports/item/30105559 (accessed: 14.05.2022).

7. *Dannye* ekspertizy kompanii Positive technology [Positive technology. Positive technology expertise data]. Available at: https://ar2021.ptsecurity.com/download/full-reports/ar_ru_annual-report_pages_pt_2021.pdf (accessed: 14.05.2022).

8. *Dannye* Kaspersky Security Network [Kaspersky Security Network data]. Available at: https://securelist.ru/it-threat-evolution-in-q1-2022-mobile-statistics/105235/ (accessed: 14.05.2022).

9. *Razvitie* informatsionnykh ugroz vo vtorom kvartale 2020 goda [Development of information threats in the second quarter of 2020]. Available at: https://securelist.ru/it-threat-evolution-q2-2020/97887/ (accessed: 14.05.2022).

Информация об авторах

Белоусова Мария Николаевна — кандидат экономических наук, доцент кафедры информационных систем, Государственный университет управления, Москва, Российская Федерация. E-mail: mn_belousova@guu.ru

Белоусов Виталий Андреевич — старший преподаватель кафедры информационных систем, Государственный университет управления, Москва, Российская Федерация. E-mail: va_belousov@guu.ru

Данилина Ольга Михайловна — кандидат экономических наук, доцент, доцент кафедры информационных систем, Государственный университет управления, Москва, Российская Федерация. E-mail: danilina_om@guu.ru

Information about the authors

Mariya N. Belousova — Candidate of Economic Sciences, Associate Professor of the Department of Information Systems, State University of Management, Moscow, Russian Federation. E-mail: mn_belousova@guu.ru

Vitaliy A. Belousov — Senior Lecturer, Department of Information Systems, State University of Management, Moscow, Russian Federation. E-mail: va_belousov@guu.ru

Olga M. Danilina — Candidate of Economic Sciences, Associate Professor, Associate Professor of Information Systems Department, State University of Management, Moscow, Russian Federation. E-mail: danilina_om@guu.ru

Статья поступила в редакцию 25.07.2022; одобрена после рецензирования 25.09.2022; принята к публикации 15.10.2022.

The article was submitted 25.07.2022; approved after reviewing 25.09.2022; accepted for publication 15.10.2022.