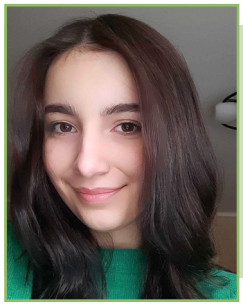
ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 343:316(045)

Анализ динамики экономических преступлений с использованием ИКТ в России



Анастасия Дмитриевна Сверчкова, *студентка факультета экономики, Финансовый университет, Липецкий филиал, Липецк, Россия*
Anastasia D. Sverchkova, *student, Faculty of Economics, Financial University (Lipetsk branch), Lipetsk, Russia*
anastayshe@gmail.com

Алина Дмитриевна Гуляева, *студентка факультета экономики, Финансовый университет, Липецкий филиал, Липецк, Россия*
Alina D. Gulyaeva, *student, Faculty of Economics, Financial University (Lipetsk branch), Lipetsk, Russia*
alina240802@mail.ru

АННОТАЦИЯ

В данной статье раскрывается одно из негативных последствий внедрения цифровизации в повседневную жизнь, а именно возникновение преступлений в IT-сфере. В статье рассматривается проблема наиболее распространенных экономических преступлений с использованием информационных технологий за период с 2019 по 2022 г., структурный анализ их видов, а также методы борьбы с ними. Цель исследования: раскрыть причины появления киберпреступности, наиболее частые схемы мошенничества и предложить меры по совершенствованию борьбы с киберпреступностью. Данная тема не так давно заинтересовала исследователей, но при этом от нее во многом зависит будущее развитие экономики страны, так как жертвами становятся как юридические, так и физические лица, при этом неся огромные финансовые потери.

Ключевые слова: *киберпреступность; мошенничество; экономические преступления; структурный анализ; модель Хольта-Винтерса*

Для цитирования: **Сверчкова А.Д., Гуляева А.Д. Анализ динамики экономических преступлений с использованием ИКТ в России.** ***Научные записки молодых исследователей.*** **2023;11(1):45–55.**

Научный руководитель: ***Уродовских В.Н.,*** *кандидат технических наук, доцент, доцент кафедры учета и информационные технологии в бизнесе, Финансовый университет, Липецкий филиал, Липецк, Россия / Scientific supervisor:* ***Urodovskikh V.N.,*** *Cand. Sci. (Tech.), Associate Professor, Department of Accounting and Information Technologies in Business, Financial University, Lipetsk branch, Lipetsk, Russia.*

ORIGINAL PAPER

Analysis of the Dynamics of Economic Crimes in ICT-Sphere in Russia

ABSTRACT

The research reveals one of the negative consequences of introducing digitalization into everyday life, namely the occurrence of crimes in the IT-sphere. The article deals with the problem of the most common economic crimes using information technology for the period from 2019 to 2022, a structural analysis of their types, as well as methods to combat them. The purpose of the study is to reveal the causes of the cybercrime emergence, the most frequent fraud schemes, and to propose measures to improve the fight against cybercrime. This topic has recently interested researchers, but at the same time, the future development of the country's economy largely depends on it, since both legal entities and individuals become victims, while incurring huge financial losses.

Keywords: *cybercrime; fraud; economic crimes; structural analysis; Holt-Winters model*

For citation: **Sverchkova A. D., Gulyaeva A. D. Analysis of the dynamics of economic crimes in ICT-Sphere in Russia. *Nauchnye zapiski molodykh issledovatelei = Scientific notes of young researchers*. 2023;11(1):45–55.**

Введение

Внедрение цифровизации в экономическую жизнь страны стало одним из поворотных моментов ее развития. Цифровые технологии оказали влияние на многие бизнес-процессы в различных сферах экономики, и особенно в банковском секторе. Существенные изменения произошли после появления пандемии коронавируса, когда возникла острая потребность в дистанционном банковском обслуживании. При этом полностью изменился функционал банка как инструмента. Если раньше он был только посредником в проведении трансакций, то в настоящее время банки продвигают свои финансовые услуги в информационном пространстве, что влечет за собой ряд угроз для пользователей.

Более того, такие преступления сопровождаются материальными убытками. В III квартале 2022 г. были зафиксированы убытки в размере 4 млрд руб. от мошеннических действий. Рост уровня преступности в IT-сфере приводит к тому, что снижается уровень доверия общества к информационным технологиям и их желание развиваться, так как будет создаваться ощущение их ненадежности.

Материалы и методы

Теоретико-методологическую основу исследования составляют статистические сборники Министерства внутренних дел РФ о состояние преступности в России и Центрального банка РФ, материалы исследований IT-компаний, материалы СМИ (РБК, РИА Новости и др.), труды исследователей-экономистов, а также Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

Результаты исследования

Результатами исследования будет являться структурно-динамический анализ экономических преступлений за период 2019–2022 гг. и их краткосрочный прогноз на 2023 г. при помощи адаптивной мультипликативной модели Хольта-Винтерса. А также необходимо будет определить ключевые причины роста киберпреступности, раскрыть основные схемы мошенничества и предложить меры по снижению уровня преступности.

Банки предлагают клиентам сервисы бесконтактной оплаты, систему быстрых платежей (СБП), единую биометрическую систему (ЕБС). Также предоставляют возможность подать заявку на выпуск или перевыпуск дебетовой карты или на выдачу кредита с помощью IT-технологий в режиме онлайн. Система интернет-банкинга позволяет совершать действия, не выходя из дома. На *рис. 1* показано соотношение тех, кто использует

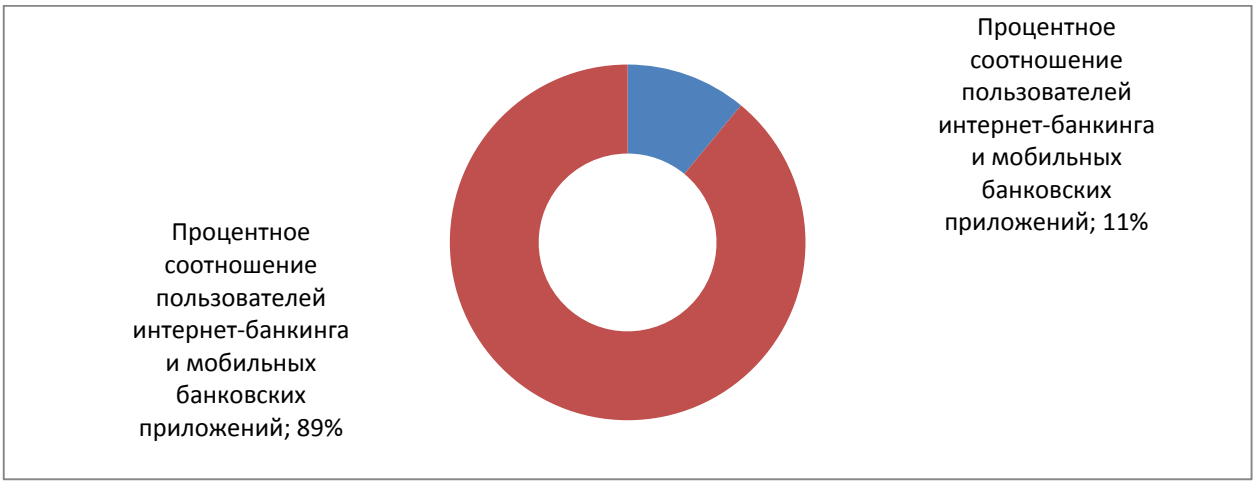


Рис. 1. **Структура пользователей интернет-банкинга и мобильных банковских приложений**

Источник: e-Finance User Index.

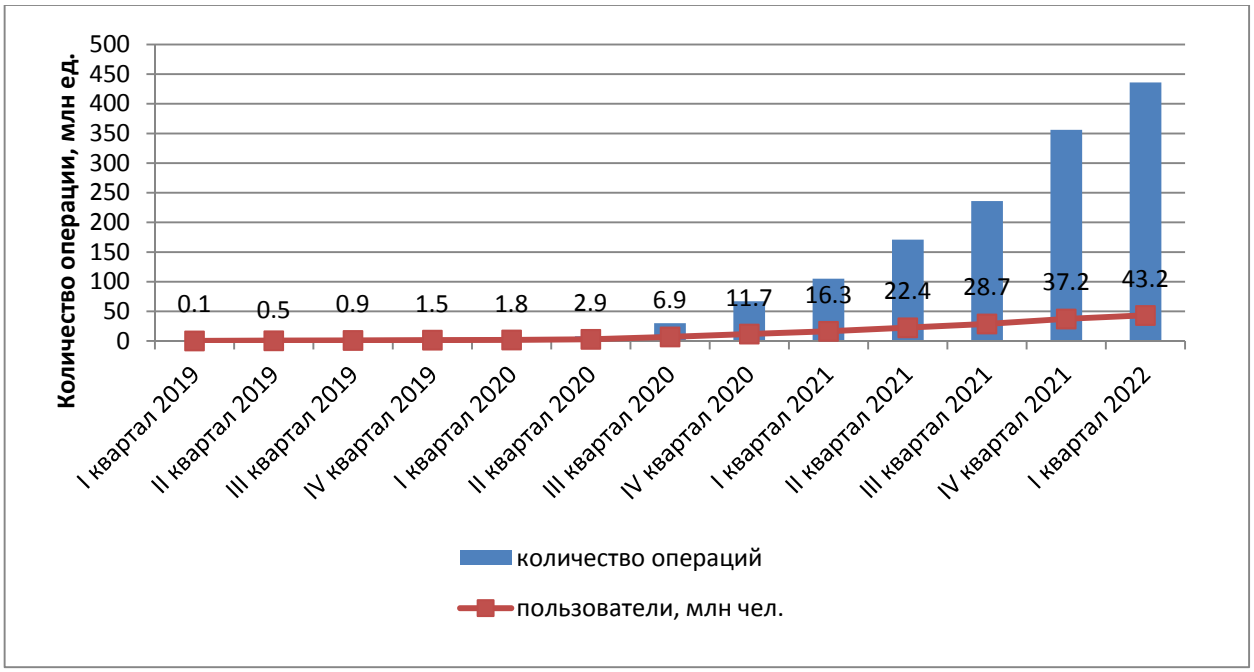


Рис. 2. **Количество операций и пользователей системой СБП за период 2019–2022 г., в млн ед.**

Источник: составлено авторами по данным Банка России.

интернет-банкинг (89%), и тех, то не использует мобильный банк (11%)[1].

Благодаря значительному количеству пользователей интернет-банкинга и мобильных банковских приложений наблюдается рост пользователей системой быстрых платежей (поквартальные данные за период 2019–2022 гг.), количество операций и пользователей (*рис. 2*)[2].

Как можно заметить на *рис. 2*, за три года количество пользователей выросло со 100 тыс. чел. до 43,2 млн чел., а количество операций возросло на 435,9 млн ед.

С переходом банков в формат интернет-банкинга появилась угроза информационной безопасности по отношению не только к персональным данным клиентов, но и к информации служебного пользования. В связи с этим встает остро вопрос сохранности баз данных. Чтобы разобраться в этой проблеме, необходимо узнать, что представляет собой цифровая преступность в банковской сфере.

[1] e-Finance User Index. URL: http://www.spbit.su/news/n191264 (дата обращения: 04.12.2022).

[2] СБП: основные показатели. Банк России. URL: https://cbr.ru/analytics/nps/sbp/1_2022/ (дата обращения: 04.12.2022).

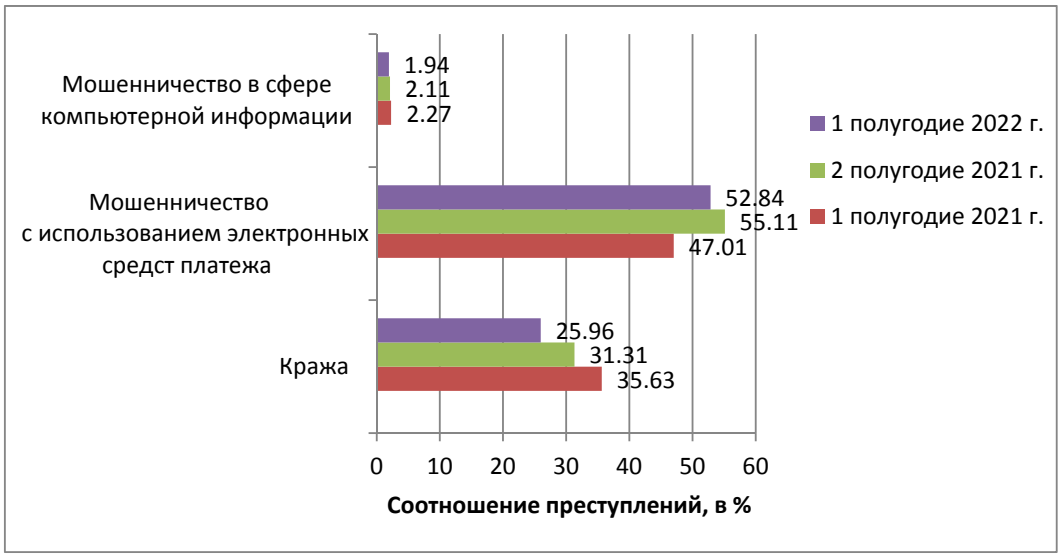


Рис. 3. **Структура преступлений экономической направленности МВД за период 1 полугодие 2021 г. по 2 полугодие 2022 г.**

Источник: составлено авторами по данным МВД.

В цифровой криминологии дается свое определение цифровой преступности. Она рассматривается как «социальное противоправное явление, включающее в себя совокупность преступлений, совершаемых в сфере цифровых технологий или с их использованием, в том числе включая незаконное завладение и предложение или распространение информации в информационно-телекоммуникационных сетях и в виртуальной среде, дополняющей реальность»[3].

Несмотря на то что понятие «киберпреступность» не новое и зародилось в 1960-е гг. вместе с появлением ЭВМ, а уже через двадцать лет начали набирать обороты хакерские группировки за рубежом, которые занимались кражей паролей и номеров кредитных карт, со временем объект преступления не изменился, усовершенствовались только его методы.

Чаще всего среди экономических преступлений с использованием информационно-коммуникационных технологий, согласно статистике МВД, встречается мошенничество с использованием электронных средств платежа, кража, мошенничество в сфере компьютерной информации (*рис. 3*).

Согласно данным с официального сайта МВД в 1 полугодии 2022 г. отмечен прирост краж на 10% по сравнению с 1 полугодием предыдущего года. Стоит отметить, что при этом снижается доля мошенничества с использованием электронных средств платежа (на 5,83%), однако среди всех видов преступлений мошенничество с использованием электронных средств платежа за последние два года составляет существенную часть среди остальных преступлений. Это в очередной раз подчеркивает необходимость в обеспечении информационной безопасности общества от цифровых преступлений.

Для того чтобы понять причину роста такого рода преступлений, необходимо изучить методы, применяемые преступником, а также факторы, которые влияют на рост преступности.

Исследуя совокупность причин цифровой преступности, необходимо обратить внимание на социально-правовой характер вопроса. В настоящее время цифровые технологии только находятся в стадии становления. Однако с их развитием происходит смена одних профессий на другие, из-за чего кадры, которые не смогли приспособиться, остаются без работы. Высокий уровень безработицы всегда отрицательно влияет на криминологическую ситуацию в стране и в мире в целом. По данным Генеральной прокуратуры РФ в 2020 г., доля безработных среди преступников составляла примерно 60%[4].

[3] Ящук Я.Г., Пинкевич Т.В., Смольянинов Е.С. Цифровая криминология. Учебное пособие. М.: Академия управления МВД России; 2021. URL: https://docviewer.yandex.ru/view/956189157/?page=21 (дата обращения: 04.12.2022).

[4] Новости Генеральной прокуратуры Российской Федерации. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news/archive?item=8282060 (дата обращения: 04.12.2022).

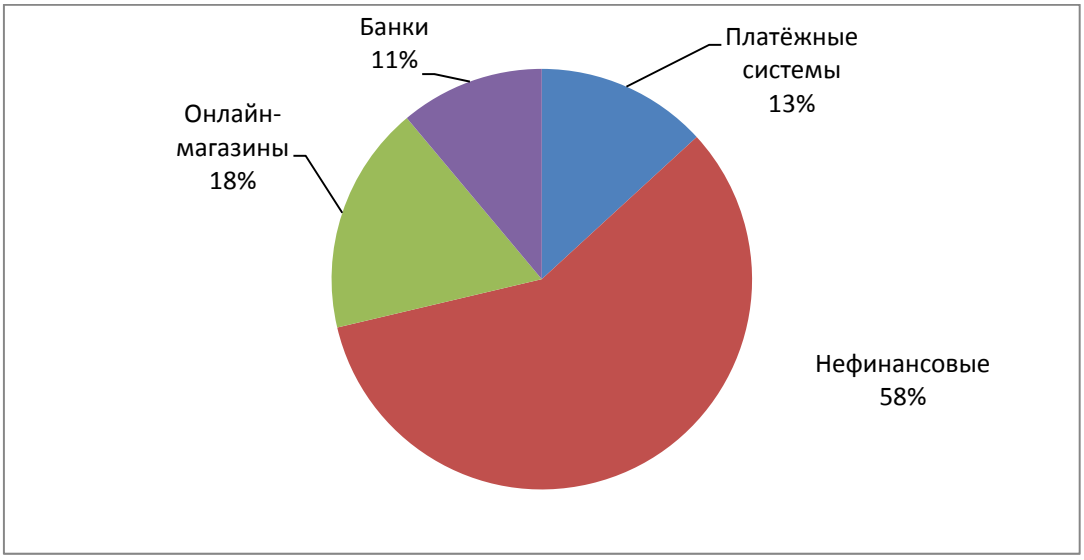


Рис. 4. **Структура случаев финансового фишинга по типам за 2021 г.**

Источник: отчет о финансовых киберугрозах от лаборатории Касперского.

Снижение уровня жизни значительной части людей также негативно сказывается на преступности. С начала пандемии более 50% россиян сообщили о значительных падениях в доходах.

Следует также обратить внимание на такую причину возникновения киберпреступности, как цифровое неравенство, т.е. отсутствие доступа к телекоммуникациям и интернету у определенных социальных групп. Причинами возникновения цифрового барьера в Российской практике являются географическая удаленность, трудности в освоении некоторых регионов и сложные климатические условия. Все эти причины увеличивают издержки на проведения связи и, как следствие, увеличивается стоимость информационно-коммуникационных услуг. Из-за неравномерного получения информации возникает разрыв между знаниями, который, во-первых, влечет за собой низкий уровень знаний в своей профессиональной деятельности по сравнению с другими специалистами, что в скором времени приведет к безработице, во-вторых, это может привести к отсутствию базовых цифровых навыков и знаний.

Проблеме киберграмотности уже сейчас уделяется особое внимание со стороны государства. По данным исследования Минцифры, «средний индекс киберграмотности населения России составляет 48,2 пункта из 100 возможных. Также 41% россиян оценил свой уровень киберграмотности на 1–3 баллов». При этом стоить отметить, что высокий уровень цифровых компетенций не гарантирует полную защиту от киберпреступников, однако снижает вероятность стать жертвой мошенников [1].

Существует основные 3 вида преступлений в IT-сфере: фишинг, хакинг и кардинг.

Минцифры провело исследование уровня киберграмотности россиян, в котором выяснило, что чуть меньше половины россиян не смогли определить ни одну из существующих киберугроз и только 14% знают о существовании такого вида киберпреступности, как фишинг[5].

Т. В. Пинкевич дает определение фишинг-атакам как «вид интернет-мошенничества, построенный на принципах социальной инженерии (хищение с использованием электронных средств доступа персональных данных, номеров кредитных карт, паролей и персональных данных с целью дальнейшего их использования для хищения денежных средств, которые в дальнейшем невозможно оспорить)»[6]. Структура случаев финансового фишинга представлена на *рис. 4*[7].

[5] Интернет-ресурс: Минцифры провело исследование киберграмотности россиян. URL: https://www.cnews.ru/news/line/2022–11–22_mintsifry_provelo_issledovanie (дата обращения: 04.12.2022).

[6] Ящук Я.Г., Пинкевич Т.В., Смольянинов Е.С. Учебное пособие. Цифровая криминология. М.: Академия управления МВД России; 2021. URL: https://docviewer.yandex.ru/view/956189157/?page=21 (дата обращения: 04.12.2022).

[7] Финансовые киберугрозы в 2021 году. URL: https://securelist.ru/financial-cyberthreats-in-2021/104553/ (дата обращения: 04.12.2022).

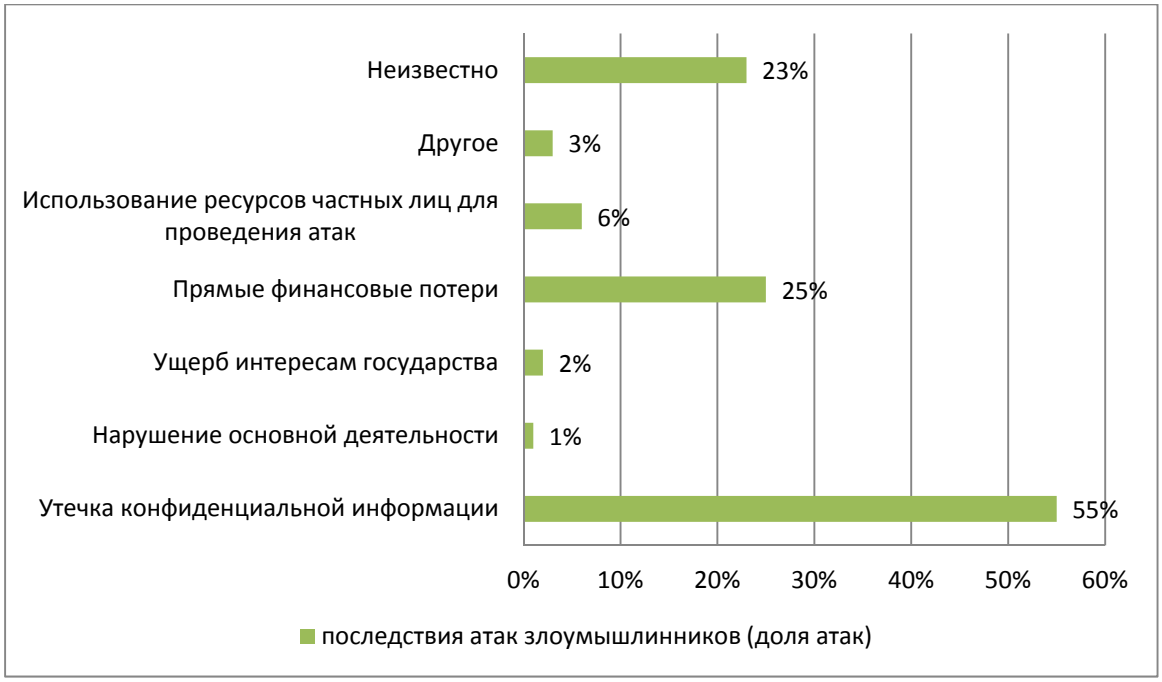


Рис. 5. **Последствия атак злоумышленников (доля атак) за I квартал 2022 г.**

Источник: исследование Positive technologies.

Нефинансовые фишинг атаки занимают лидирующую позицию среди других атак и составляют 58%. Наиболее распространенной схемой является отправка поддельного уведомления от разных маркетплейсов, банков или электронных платежных систем с просьбой перейти по ссылки для ознакомления с новой продукцией, получения скидки или обновления профиля. Жертва переходит на точную копию сайта и вводит свои персональные данные. Структура последствий атак злоумышленников представлена на *рис. 5*[8].

Атаки киберпреступников в первую очередь были направлены на получение конфиденциальной информации (55%). В I квартале 2022 г. количество атак увеличилось на 14,8% по сравнению с IV кварталом 2021 г. Злоумышленники в первую очередь, согласно *рис. 5*, были заинтересованы на кражу учетных данных (46%), второе место занимает кража данных платежных карт (21%).

На *рис. 6* продемонстрирована структура украденных данных (в атаках на частных лиц) за I квартал 2022 г.[9]

Из статистических данных следует, что чаще всего объектом кражи являются учетные данные (46%) и данные платежных карт (21%).

Согласно цифровой криминологии 21% успешных кибератак начинается с перехода по фишинговым ссылкам, 11% преступлений начинаются с запуска вредоносных приложений, в остальных 70% кибератак в основе лежит социальная инженерия[10].

Для того чтобы «заставить» человека воспользоваться фишинговым сайтом, мошенники используют метод социальной инженерии. Данный метод предполагает психологическое воздействие на человека для дальнейшего получения персональных данных. Злоумышленник может использовать различные рычаги давления: начиная от страха за благополучие близкого человека и заканчивая возможностью «выигрыша» крупной суммы.

В цифровой криминологии хакингом является изменение строения программного обеспечения для создания вредоносного продукта[11]. К хакингу также относятся DDoS-атаки — воздействие на нормальное функционирование сайта, прино-

[8] Актуальные киберугрозы: I квартал 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 04.12.2022).

[9] Актуальные киберугрозы: I квартал 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 04.12.2022).

[10] Чеклист для борьбы с фишингом: URL: http://habr.com/ru/company/cisco/blog/465085/ (дата обращения: 26.11.2022).

[11] Ящук Я.Г., Пинкевич Т.В., Смольянинов Е.С. Цифровая криминология. Учебное пособие. М.: Академия управления МВД России; 2021. URL: https://docviewer.yandex.ru/view/956189157/?page=21 (дата обращения: 04.12.2022).

Рис. 6. **Структура украденных данных (в атаках на частных лиц) за I квартал 2022 г.**

Источник: исследование Positive technologies.

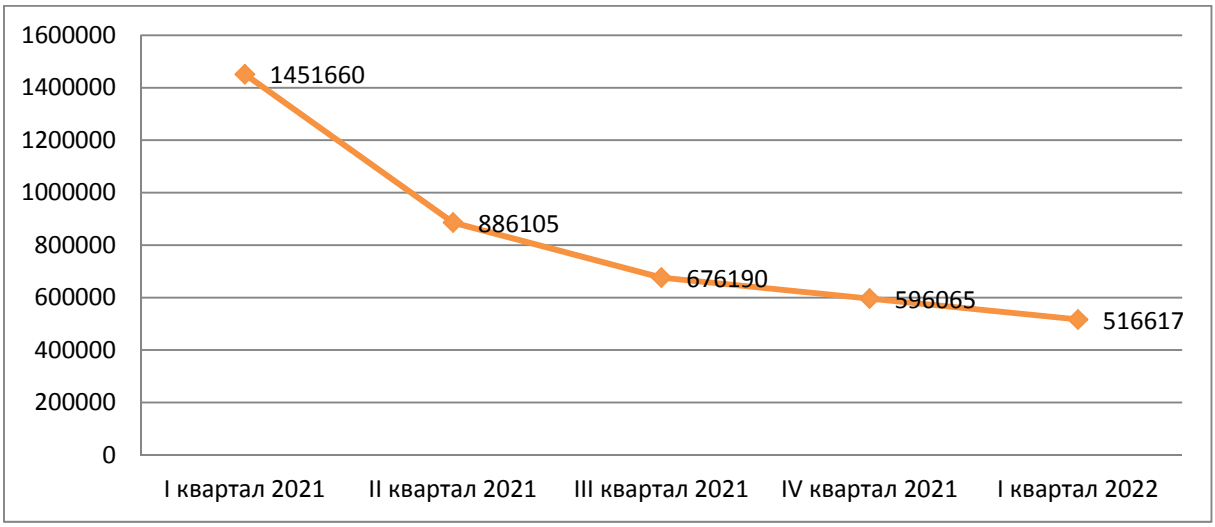


Рис. 7. **Количество обнаруженных вредоносных установочных пакетов ПО, I квартал 2021 — I квартал 2022 г.**

Источник: Лаборатория Касперского, 2021–2022 гг.

сящего доход, как правило, осуществляются по заказу недобросовестного конкурента [2]. На *рис. 7* представлено количество обнаруженных вредоносных установочных пакетов ПО за период 2021–2022 гг.[12]

«Лаборатория Касперского» выяснила, что количество вредоносных программ за период с I квартала 2021 по I квартал 2022 г. сократилось на 79 448 пакетов, или на 35,59%. На *рис. 8* показана структура вредоносного ПО за I квартал 2022 г.[13]

Согласно сайту «Positive technologies» лидирующие позиции занимают «Банковский троян» (35%) и «Шпионское ПО» (38%). Распространяются эти вредоносные программы чаще всего через электронную почту (20%), мессенджеры и SMS-сообщения (17%), сайты (34%), поддельные обновления (3%), официальные магазины

[12] Количество обнаруженных вредоносных установочных пакетов ПО. URL: https://securelist.ru/it-threat-evolution-in-q2–2022-non-mobile-statistics/105744/ (дата обращения: 04.12.2022).

[13] Актуальные киберугрозы: I квартал 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 04.12.2022).

Рис. 8. **Структура вредоносного ПО (доля с использованием ВПО) за I квартал 2022 г.**

Источник: Positive technologies, I квартал 2022 г.

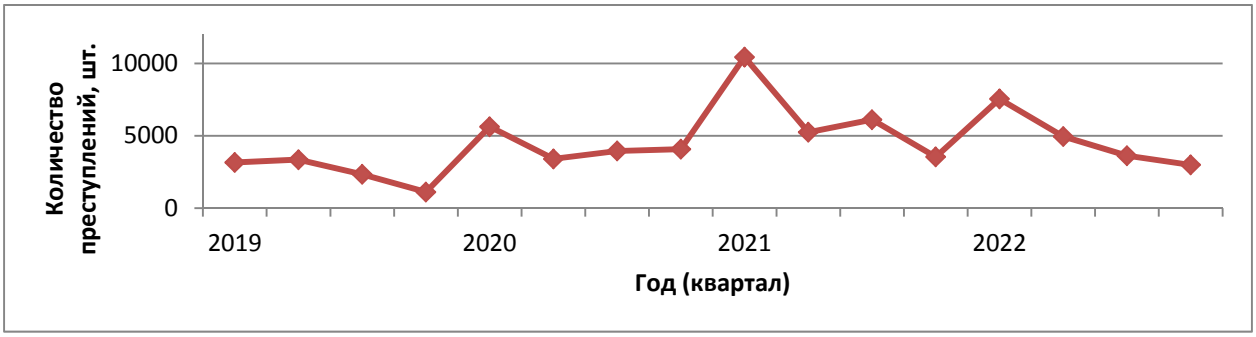


Рис. 9. **Количество совершенных преступлений с использованием ИКТ за период I квартала 2019 по IV квартал 2022 г.**

Источник: составлено авторами по данным МВД России.

приложений (12%), социальные сети (8%) и другое (6%).

Еще одной разновидностью киберпреступлений является кардинг. Его классифицируют как особо опасное мошенничество, которое базируется на принципе кражи баз данных о кредитных картах с целью дальнейшего «отмывания» денежных средств и приобретения незаконным путем товара без согласия владельца карты.

Для предотвращения такого рода преступлений используются методы криминологического прогнозирования, которые направлены на выявление тенденций и закономерностей развития преступности. Для осуществления криминологического прогноза учитываются такие факторы, как показатели социально-экономического развития региона или страны, экспертная оценка состояния киберпреступности за предыдущие и текущий периоды, анализ причин роста цифровой преступности прошлых периодов. На *рис. 9* представлена динамика совершенных преступлением ИКТ в период с 2019 по 2022 г. и линейный тренд.

Визуальный анализ динамики преступлений с использованием IT-технологий за период I квартал 2019 по IV квартал 2022 г. *на рис. 9* показал, что преступления имеют сезонный характер. Можно предположить, что фактор сезонности связан с повышением покупательской активности в период праздников. Линейный тренд киберпреступлений все равно остается восходящим за период 2019–2022 гг. Линейный характер тренда и наличие сезонности позволяют для построения прогноза на 2023 г. и последующие годы использовать адаптивную мультипликативную модель Хольта-Винтерса. Были также рассмотрены другие модели прогнозирования, но характер колебаний был близок к сезонным, поэтому была выбрана модель Хольта-Винтерса.

Таблица

Количество совершенных экономических преступлений с использованием информационно-коммуникационных технологий в период с 2019 по 2022 г.

Показатель	Временной период, год, квартал															
	2019				2020				2021				2022			
Квартал	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
Y факт	3155	3350	2337	1114	5627	3401	3950	4074	10439	5246	6113	3542	7545	4953	3625	2989

Источник: составлено авторами по данным МВД России.

Для проведения анализа использовались поквартальные данные МВД РФ о количестве совершенных экономических преступлений с использованием информационно-коммуникационных технологий в периоде с 2019 по 2022 г. (см. *таблицу*).

Далее были рассчитаны показатели по формулам, приведенным ниже.

$$Y_{p(t+k)} = [a_t + k^*b_t]^*F_{(t+k-L)},$$

где k — период упреждения внутри временного ряда; $Y_{p(t)}$ — расчетное значение экономического показателя для t-го периода; b_t, a_t, F_t — коэффициенты модели, они адаптируются, уточняются по мере перехода от членов ряда с номером $t - 1$ и t; $F_{(t+k-L)}$ — значение коэффициента сезонности того периода, для которого рассчитывается экономический показатель; L — период сезонности (для квартального $L = 4$).

Адаптация к новому значению параметра времени t коэффициентов модели производится с помощью формул:

$$b_t = \alpha_3^*[a_{(t)} - a_{(t-1)}] + (1 - \alpha_3)^*b_{(t-1)},$$
$$a_t = \alpha_1^*Y(t)/F_{(t-L)} + (1 - \alpha_1)^*[a_{(t-1)} + b_{(t-1)}],$$
$$F_t = \alpha_2^*Y(t)/a_{(t)} + (1 - \alpha_2)^*F_{(t-L)}.$$

Параметры сглаживания a_1, a_2, a_3 подбираются путем перебора из условий; в расчетах приняты равными: $\alpha_1 = 0{,}4893$; $\alpha_2 = 0$; $\alpha_3 = 0{,}9077$. Точность модели составляет 17%. Подбор параметров модели оптимизировался с помощью инструмента «Поиск решения» и повысил точность модели.

На базе этих показателей рассчитывается $Y_p(t)$ и сопоставляется с фактическими значениями (*рис. 10*).

Как видно из *рис. 10*, в I квартале 2021 г. произошло резкое увеличение количества преступлений. Как отмечает Банк России, в I квартале 2021 г. было украдено на 57% больше, чем в том же периоде предыдущего года. Во-первых, это связано с тем, что в этот период активно осуществлялся переход клиентов на дистанционное обслуживание клиентов финансового рынка, во-вторых, из-за новогодних праздников жертвы декабрьских преступлений смогли обратиться в правоохранительные органы только в январе. Данный скачок можно охарактеризовать как сезонный пик активности из-за праздников, когда жертва менее защищена. В 2022 г. в I квартале наблюдается резкий скачок преступлений по сравнению с предыдущим годом, а затем видно значительное сокращение по каждому последующему кварталу. Такое изменение связано с ведением во II квартале 2022 г. новых программ борьбы с преступностью в IT-сфере. Основываясь на краткосрочном прогнозе, можно предположить, что в 2023 г. количество преступлений в I квартале увеличится до 5247, а затем будет постепенно снижаться до 2501. Прогнозная модель Хольта-Винтерса повторяет динамику предыдущего года, т.е. заметно снижение уровня преступности.

Существует комплекс мер по предотвращению экономических преступлений, связанных с IT-сферой. Условно их можно поделить на 3 группы: правовые, организационно-технические и криминалистические.

К первой группе относятся меры по предупреждению мошеннических операций на уровне законодательства, устанавливаются тем самым различные нормы наказания за противоправные действия.

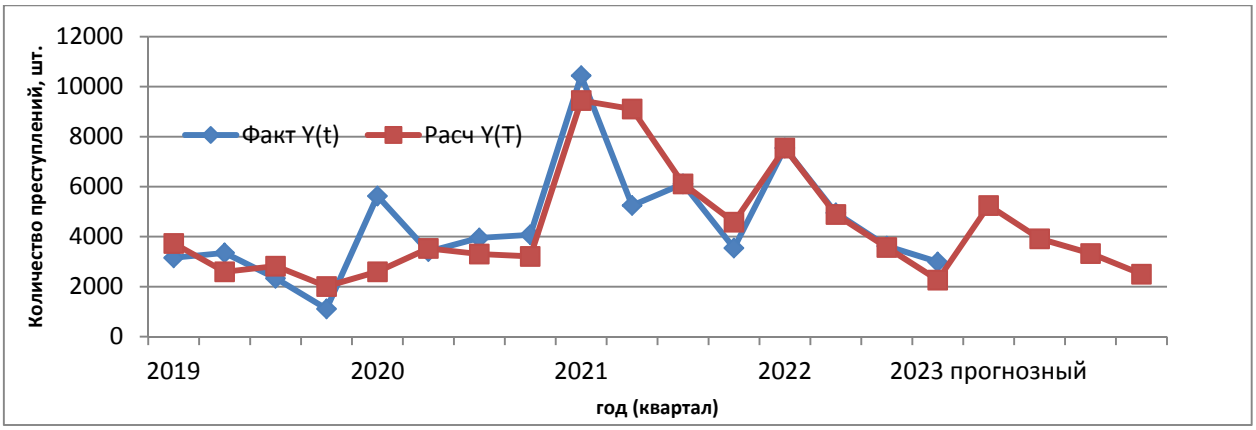


Рис. 10. **Динамика фактического количества экономический преступлений и результата прогноза по модели Хольта-Уинтерса**

Источник: составлено авторами по данным МВР России.

Организационно-технические меры защиты включают в себя совокупность мероприятий, такие как подбор и инструктаж персонала, назначение ответственного лица по обеспечению безопасности, организация программно-технического обеспечения и т.п. Такая мера предотвращения киберпреступности больше подходит для юридических лиц.

В Российской Федерации активно создаются и реализуются нормативно-правовые меры борьбы с киберпреступностью. Центральный банк РФ разработал особую систему ФинЦЕНТР, согласно которой происходит обработка инцидентов, связанных с мошенническими действиями в области кредитно-финансовой сферы. ФинЦЕНТР объединяет практически всех участников денежно-кредитных отношений, которые имеют непосредственное отношение к информационной безопасности: участников финансового рынка, органы внутренних дел, разработчиков антивирусных программ и провайдеров связи.

Ответом государства на увеличивающиеся количество киберпреступлений также стал Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и изменения в структуре МВД России. С конца сентября 2022 г. появилось новое структурное подразделение, вошедшее в систему центрального аппарата Министерства Внутренних дел России. Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий осуществляет функции по предотвращению и профилактики правонарушений в сфере IT-технологий, мониторинг данных с целью выявления запрещенных законом материалов, а также сотрудничество с другими подразделениями, государственными органами, финансово-кредитными учреждениями.

Несмотря на меры, которые принимает государство по борьбе с киберпреступлениями, эксперты из компании Swordfish Security прогнозируют рост кибератак на 50%, увеличение фишинговых атак на 15%, а число успешных атак может увеличиться на 30–40%. Эксперты связывают это с тем, что из-за ухода с российского рынка многих иностранных ПО перестали выпускаться обновления программ, что и сделало их уязвимыми для кибератак. Еще одной причиной является нехватка сотрудников в области информационной безопасности, по данным МВД их дефицит составляет порядка 170 тыс. специалистов. Также система подготовки юридических и технических кадров не вполне соответствует существующим угрозам [3].

Выводы

Таким образом, по результатам проводимого анализа можно сказать, что необходимо обращать внимание на предыдущий опыт эффективной борьбы с преступлениями в IT-сфере. Для сдерживания роста киберпреступности государство уже разработало и выводит на рынок российское ПО, однако процесс интеграции очень длителен и сложен, так как обучение сотрудников и обычных пользователей требует времени и дополнительных затрат. На наш взгляд, государству и компаниям следует обратить внимание на обучение

граждан и сотрудников киберграмотности. Это как минимум позволит снизить число успешных фишинговых кибератак. Также необходимо дальнейшее совершенствование законодательной базы, так как в Уголовном кодексе не отражены основные способы и средства совершения киберпреступлений. В данный момент большинство мер со стороны государства не предупреждающие, а контрмеры в ответ на уже совершенные преступления [4]. Наиболее отстающей сферой в области правового регулирования уголовных преступлений является электронный оборот денежных средств [5]. Для того чтобы улучшить профессиональную подготовку кадров для государственных органов в области информационной безопасности, необходимо в первую очередь наладить взаимодействие вузов с организациями, занимающимися созданием продуктов для цифровой безопасности, например «Лаборатория Касперского», «Цитадель», «Softline» и другие.

Список источников

1. Швыряев П. С. Киберпреступность в России: новый вызов для общества и государства. 2021. URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-novyy-vyzov-dlya-obschestva-i-gosudarstva
2. Сафронкина О.В. Киберпреступность как форма экономической преступности: Международной научно-практической конференции. Криминалистика в условиях развития информационного общества. 59-е ежегодные криминалистические чтения. М.; 2018:263.
3. Гончар В.В. Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемым с использованием информационных технологий: сборник статей Международной научно-практической конференции. Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения). М.; 2018:75.
4. Дерюгин Р.А. Киберпреступность в России: современное состояние и Актуальные проблемы. *Вестник Уральского юридического института МВД России.* 2019;(2):46–49.
5. Куява Т.Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия. *Молодой ученый.* 2016;29(133):255–257. URL: https://moluch.ru/archive/133/37306/.

References

1. Shvyryaev P. S. Cybercrime in Russia: a new challenge for society and the state. 2021. URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-novyy-vyzov-dlya-obschestva-i-gosudarstva. (In Russ.).
2. Safronkina O.V. Cybercrime as a form of economic crime: International Scientific and Practical Conference. Criminalistics in the context of the development of the information society. 59th Annual Forensic Readings. Moscow; 2018:263. (In Russ.).
3. Gonchar V.V. Some issues of improving the training of personnel specializing in the investigation of crimes committed using information technology: A collection of articles of the International Scientific and Practical Conference. Forensic science in the context of the development of the information society (59th Annual Forensic Readings). Moscow; 2018:75. (In Russ.).
4. Deryugin R.A. Cybercrime in Russia: Current state and current problems. *Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii = Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia.* 2019;(2):46–49. (In Russ.).
5. Kuyava T. Yu. Cybercrime: Problems of criminal law assessment and organization of counteraction. *Molodoj uchenyj = Young scientist.* 2016;29(133):255–257. URL: https://moluch.ru/archive/133/37306/. (In Russ.).