УДК 343.97 DOI 10.51980/2686-939X_2023_2_51

СОСТОЯНИЕ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИИ И РЕСПУБЛИКЕ ТАТАРСТАН (НА ПРИМЕРЕ КРАЖ И МОШЕННИЧЕСТВ)

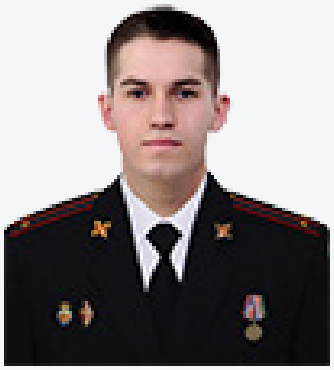
THE STATE OF CRIME IN THE SPHERE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES IN RUSSIA AND THE REPUBLIC OF TATARSTAN (BY THE EXAMPLE OF THEFT AND FRAUD)

Рамис Ренатович Газимов,
заместитель начальника Управления уголовного розыска МВД по Республике Татарстан — начальник отдела

rgazimov6@mvd.ru

Динар Минзеферович Фарахиев,
оперуполномоченный Управления экономической безопасности и противодействия коррупции МВД по Республике Татарстан

dfarakhiev@mvd.ru



Ключевые слова:
преступность, кражи (ст. 159 УК РФ), мошенничество (ст. 159 УК РФ), информационно-телекоммуникационные технологии, статистические данные, Россия, Республика Татарстан, минимизация.

В статье авторами анализируются статистические данные о кражах и мошеннических действиях на территории России и Республики Татарстан, совершаемые (совершенные) с использованием информационно-телекоммуникационных технологий (ИТТ). Авторы делают вывод о большом влиянии на увеличение количества преступлений, совершенных с использованием ИТТ, пандемии коронавируса COVID-19, в результате которой

сформировались дополнительные условия для еще большего усиления криминальной активности мошенников на территории России. В заключение предлагается ряд мер, направленных на минимизацию преступлений, предусмотренных статьями 158 и 159 УК РФ, совершенных с использованием ИТТ.

Keywords:
crime, theft (Article 159 of the Criminal Code of the Russian Federation), fraud (Article 159 of the Criminal Code of the Russian Federation), information and telecommunication technologies, statistical data, Russia, Republic of Tatarstan, minimization.

In the article, the authors analyze statistical data on thefts and fraudulent activities in Russia and the Republic of Tatarstan, committing (committed) using information and telecommunication technologies information and telecommunication technologies (ITT). The authors conclude that the COVID-19 coronavirus pandemic has a great influence on the increase in the number of crimes committed using ITT, as a result of which additional conditions have been formed for an even greater increase in the criminal activity of fraudsters in Russia. In conclusion, a number of measures are proposed aimed at minimizing the crimes provided for by Articles 158 and 159 of the Criminal Code of the Russian Federation, committed with the use of information and telecommunication technologies.

Повсеместное внедрение информационно-телекоммуникационных технологий (далее – ИТТ) значительно облегчает жизнь современного человека, оказывает существенное влияние на модернизацию правоотношений, в которых он участвует. Однако, как показывает опыт, научно-технический прогресс в этой области используется не только в благих целях. Широкое распространение его достижений предоставило дополнительные возможности как законопослушным гражданам, так и злоумышленникам. Это обстоятельство не могло не отразиться на характеристиках современной преступности, о чем наглядно свидетельствуют результаты криминологического анализа ее количественных и качественных показателей. Первоочередное значение приобретает задача поиска эффективных способов борьбы с преступностью данного вида, что невозможно без полного представления о ее свойствах [3, с. 60].

В настоящее время развитие общественных отношений в России сопровождается увеличением угроз в информационной сфере в зависимости от разнообразных форм социально опасных проявлений. Наиболее опасным источником угроз социально-экономической безопасности нашего государства

выступает преступность в информационном пространстве, так как развитие сферы ИТТ приводит к зарождению и неуклонному росту количества преступлений, в том числе краж и мошенничеств, совершаемых с использованием ИТТ. Также увеличивается размер причиняемого материального ущерба от данных преступлений [2, с. 46]. Причиненный ущерб за 2022 г. в Республике Татарстан от исследуемых преступлений составил 2 млрд 895 млн рублей.

Наибольшее распространение использование ИТТ в процессе совершения преступлений, в том числе краж и мошенничеств, получило в 2019 г. Так, в 2019 г. на территории России были зарегистрированы 294,4 тыс. преступлений, совершенных с использованием ИТТ, или на 68,5% больше, чем за 2018 г. В общем числе зарегистрированных преступлений их удельный вес увеличился с 8,8% в 2018 г. до 14,5%[1].

Почти половина таких преступлений (48,5%) относятся к категориям тяжких и особо тяжких: 142,7 тыс. (+149,0%); половина (53,3%) совершаются с использованием сети Интернет: 157,0 тыс. (+45,4%), более трети (39,5%) – средств мобильной связи: 116,2 тыс. (+89,5%). Четыре таких преступления (80,0%) из пяти совершаются путем кражи или мошенничества: 235,5 тыс. (+83,2%) .

Год за годом преступления, совершенные посредством ИТТ, увеличиваются. В 2020 г. каждое четвертое (25,0%) зарегистрированное преступление совершалось с использованием ИТТ (всего 510,4 тыс., +73,4%). По сравнению с 2019 г. в 2020 г. число тяжких и особо тяжких деяний увеличилось на 3,9%. В 2021 г. были зарегистрированы 517,7 тыс. преступлений, совершенных с использованием ИТТ (+1,4%). Больше половины таких преступлений (55,7%) относились к категориям тяжких и особо тяжких (288,3 тыс., +7,7%) .

В 2022 г. были зарегистрированы 522,1 тыс. преступлений, совершенных с использованием ИТТ или в сфере компьютерной информации, что на 0,8% больше, чем в 2021 г. В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,8% в 2021 г. до 26,5% .

Больше половины таких преступлений (52,1%) относились к категориям тяжких и особо тяжких (272,2 тыс., -5,6%), почти три четверти (73,0%) были совершены с использованием сети Интернет (381,1 тыс., +8,4%), более трети (40,8%) – средств мобильной связи (213,0 тыс., -2,1%). Почти три четверти таких преступлений (71,1%) были совершены путем кражи или мошенничества: 371,2 тыс. (-8,6%) .

В 2022 г. мошенники для совершения преступлений с использованием ИТТ использовали:

1) расчетные (пластиковые) карты – в 127 149 случаях;

1 Здесь и далее статистические сведения приводятся по: Состояние преступность на территории Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 16.02.2023).

2) компьютерную технику – в 29 140 случаях;
3) фиктивные электронные платежи – в 1 325 случаях;
4) сеть Интернет – в 381 112 случаях, в том числе для совершения:
5) краж ст. 158 УК РФ – 113 565;
6) мошенничеств ст. 159, 159.3, 159.6 УК РФ – 257 606 .

Анализ статистических данных показывает, что в настоящее время использование ИТТ становится пре-обладающим способом совершения мошенничества и краж. При этом следует отметить, что впервые за последние годы удалось добиться снижения совершаемых «дистанционных» хищений в Республике Татарстан, число которых в 2022 г. составило 13 452 (АППГ – 14 201, снижение на 863 преступления или 6,1%). На кражи с банковских счетов и мошенничества в сфере ИТТ приходится четверть от всех зарегистрированных преступлений (52 189) в Республике Татарстан.

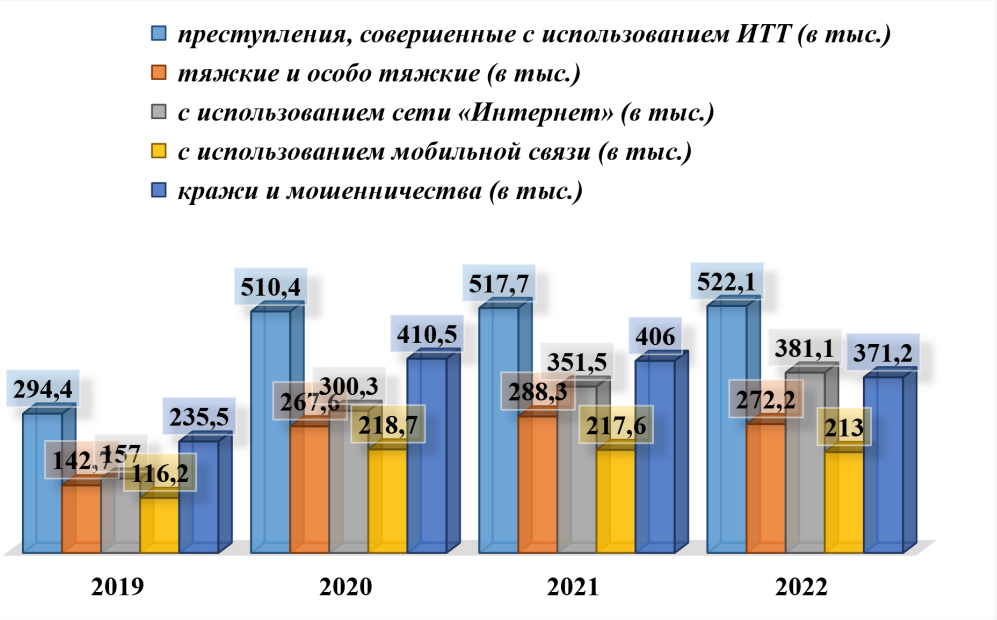


Диаграмма. Статистические данные о состоянии преступности на территории Российской Федерации за 2019-2022 гг.

Таблица 1

Количество зарегистрированных преступлений, расследуемых уголовных дел и лиц, привлеченных к ответственности за совершение краж и мошенничеств с использованием ИТТ, в 2022 году в Приволжском федеральном округе

		Республика Татарстан	Республика Башкортостан	Нижний Новгород	Оренбург	Пермь	Самара
Преступлений в сфере ИТТ	Расслед.	4779	3296	3472	1811	3340	3779
	Лица	2923	2578	2008	1312	1938	1548
	Зарег.	17993	13462	11050	6052	10786	11468
Ст. 159 УК РФ	Расслед.	1611	376	563	425	531	344
	Лица	617	196	148	181	153	141
	Зарег.	9445	5562	5113	2574	4026	4399
П. «г» ч. 3 ст. 158 УК РФ	Расслед.	1206	1381	800	680	925	745
	Лица	1176	1321	751	578	907	662
	Зарег.	3893	3857	1879	1535	2237	2265
Общее количество	Расслед.	2817	1757	1363	1105	1456	1089
	Лица	1793	1517	899	759	1060	803
	Зарег.	13338	9419	6992	4109	6263	6664

Вместе с тем показатели зарегистрированных преступлений, предусмотренных ст. 158 и 159 УК РФ, совершенных с использованием ИТТ, в Татарстане остаются достаточно высокими:

1) первое место по количеству зарегистрированных краж и мошенничеств (13 338) в Приволжском федеральном округе (таблица 1);

2) четвертое место в России (таблица 2).

Таблица 2

Количество зарегистрированных преступлений, расследуемых уголовных дел и лиц, привлеченных к ответственности за совершение краж и мошенничеств с использованием ИТТ, в 2022 году в России

		Республика Татарстан	Москва	Московская область	СПб и Ленобласть	Краснодар	Республика Башкортостан	Свердловская область	Челябинск
Преступлений в сфере ИТТ	**Зарег.**	17993	50503	15061	28298	22603	13462	11794	17281
	Расслед.	4779	12461	4419	6373	5407	3296	4057	6954
	Лица	2923	6708	3618	3423	4030	2578	3459	3807
Ст. 159 УК РФ	**Зарег.**	9445	31261	8738	16062	13595	5562	4743	6741
	Расслед.	1611	6611	729	752	1570	376	376	1177
	Лица	617	1537	397	373	548	196	214	398
П. «г» ч. 3 ст. 158 УК РФ	**Зарег.**	3893	11390	2912	5706	3448	3857	2137	3133
	Расслед.	1206	2164	1772	1858	1331	1381	1337	1150
	Лица	1176	2063	1684	1653	1225	1321	1198	1044
Общее количество	**Зарег.**	13338	42651	11650	21768	17043	9419	6880	9874
	Расслед.	2817	8775	2501	2610	2901	1757	1713	2327
	Лица	1793	3600	2081	2026	1773	1517	1412	1442

Наиболее распространенными способами хищения денежных средств у граждан нашей страны в сфере ИТТ на протяжении многих лет остаются мошенничества и кражи, что детерминировано признаком «дистанционных преступных действий». Дистанционный характер преступлений, связанных с кражами и мошенничествами, совершенных с использованием ИТТ, позволяет злоумышленникам скрываться от следствия, дознания и суда, поскольку их местоположение в большинстве случаев анонимно в связи с использованием ими программного обеспечения, позволяющего скрывать (шифровать) IP-, ID-адреса.

Одним из важных факторов, способствующих совершению мошенничеств и преступлений других видов с использованием ИТТ, является недостаточный уровень навыков граждан в использовании информационных технологий в сочетании с низким уровнем правовой и финансовой грамотности. Специалисты отмечают, что, несмотря на увеличение за последние четыре года числа пользователей информационного пространства, уверенных в защищенности своих персональных данных, около двух третей (62%) россиян чувствуют себя неуверенно, используя гаджеты и цифровые технологии, боятся стать жертвой кибермошенников, а наиболее уязвимыми чувствуют себя люди старше 45 лет[2].

На основании вышеизложенного предлагаем рассмотреть социальный портрет жертвы от преступлений, предусмотренных ст. 158 и 159 УК РФ, совершенных с использованием ИТТ, по данным Информационного центра МВД по Республике Татарстан (таблицы 3, 4):

Таблица 3

Пол и возрастной критерий потерпевших от преступлений, предусмотренных ст. 158 и 159 УК РФ, совершенных с использованием ИТТ, в Республике Татарстан в 2021-2022 гг.

	Пол		**Возрастной критерий (в %)**				
	Мужской	Женский	До 18 лет	18-29	30-49	50-59	Старше 60 лет
2021	43	57	1	25	46	13	15
2022	43	57	1	25	45	13	16
+/-	0	0	0	0	0	0	0

Мы видим, что пол и возрастной критерий лиц, ставших жертвами преступлений, предусмотренных ст. 158 и 159

2 Жертвы киберохотников: россияне старше 45 лет меньше других защищены от цифровых мошенников. URL: https:// nafi.ru/analytics/ (дата обращения: 15.02.2023).

Таблица 4

Род занятий потерпевших от преступлений, предусмотренных ст. 158 и 159 УК РФ, совершенных с использованием ИТТ, в Республике Татарстан в 2021-2022 гг.

	Род занятий (в %)							
	Студент	Без ист-ка дохода	Пенсионер	ИП	Рабочий	Инвалиды	Декрет. отпуск	Гос. служба
2021	3	18	15	2	56	2	2	2
2022	3	18	17	2	55	1	2	2
+/-	*0*	*0*	*+2*	*0*	*-1*	*-1*	*0*	*0*

УК РФ, совершенных с использованием ИТТ, остаются стабильными на протяжении двух последних лет. По роду занятий число пенсионеров, потерпевших от краж и мошеннических действий, совершенных с использованием ИТТ, в 2022 г. увеличилось на 2%; уменьшилось число рабочих и инвалидов, в отношении которых были совершены исследуемые виды преступлений в 2022 г.

Проанализированная практика избрания наказаний в Республике Татарстан в отношении лиц, совершивших «дистанционные» мошенничества (ч.ч. 2, 3, 4 ст.159 УК РФ) и краж (п. «г» ч.3 ст.158 УК РФ), свидетельствует о том, что процент обвинительных приговоров с назначением преступникам реального лишения свободы вырос – из 1116 лиц, осужденных в 2022 г., 326 приговорены к лишению свободы, или 29,2% (2021 г. – из 959 лиц 216 – с лишением свободы, или 22,5%).

В 2022 г. к лишению свободы были приговорены 326 преступников, которые получили следующие сроки:

– до одного года – 61 лицо,

– более 1 года – 181 лицо,

– более 3 лет – 67 лиц,

– более 5 лет – 16 лиц,

– более 10 лет – 1 лицо (таблица 5).

Таблица 5

Статистика осужденных лиц, совершивших преступления, предусмотренные ст. 158 и 159 УК РФ с использованием ИТТ в Республике Татарстан в 2021-2022 гг.

	Ч. 2 ст. 159 УК РФ		Ч.ч. 3 и 4 ст. 159 УК РФ		П. «г» ч. 3 ст. 158 УК РФ		Итого	
	2021	2022	2021	2022	2021	2022	2021	2022
Осуждено лиц всего:	86	130	49	76	824	960	959	1116
из них лишение свободы	27	58	18	30	171	238	216	326
условный срок	42	52	26	37	566	558	334	647
обязательные работы	4	9	-	-	1	2	5	11
исправительные работы	8	4	-	-	1	4	9	8
ограничение свободы	1	2	-	1	1	-	2	3
штраф	4	5	5	8	84	158	93	171

Нередко совершению телефонного и интернет-мошенничества способствует сознательное пренебрежение гражданами доступными способами защиты своих средств. По данным российских банков, клиенты пока не спешат воспользоваться новой возможностью защиты от злоумышленников, которая заключается в запрете совершения определенных операций по своим счетам или установлении на них лимитов[3]. Между тем почти две трети опрошенных экспертов положительно оценивают введение такой меры, полагая, что это будет способ-

3 Шерункова О. Граждане не хотят себя ограничивать. URL: https://www.kommersant.ru/doc/5606464 (дата обращения: 22.02.2023).

ствовать более эффективному предупреждению краж и мошенничеств, совершаемых с использованием ИТТ, и снижению их уровня.

Особое значение в связи с этим приобретают меры виктимологической профилактики. Так, Банк России публикует информацию о современных мошеннических схемах и действиях, которые могут помочь гражданам распознать мошенников и защитить свои денежные средства. В настоящее время активно используются такие схемы, как «обмен кешбэка на рубли», «компенсация похищенных денег», «проверка данных счета на предмет утечки», «сообщения о дефиците наличных рублей и валюты», «перевод денег на специальный счет Центрального банка», «оформление «встречного» кредита». Основываясь на результатах обобщения типичных схем хищения денежных средств, Банк России предлагает рекомендации, соблюдение которых помогает избежать противоправных посягательств: никому не сообщать свои паспортные данные и финансовые сведения, не публиковать такую информацию в социальных сетях, на форумах и на сайтах в Интернете, не хранить данные карты и PIN-код на компьютере или в смартфоне, не отвечать на звонки с неизвестного номера от якобы сотрудника банка, правоохранительных органов или государственной организации с сомнительным предложением, не реагировать на звонки с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный счет», или с предложением оформить кредит, не совершать покупки на непроверенных сайтах, не вводить личные и финансовые данные на сомнительных сайтах и не переходить по ссылкам из подозрительных писем, в которых предлагают, например, пройти опрос, получить какую-либо выплату[4].

Одним из наиболее негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Одновременно усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса [5, с. 321].

Анализ статистических данных позволяет сделать вывод, что на протяжении двух лет совершенствуются методика раскрытия и расследования преступлений, совершаемых с использованием ИТТ, и меры предупредительной направленности. Ежегодно растет количество предварительно расследованных преступлений, предусмотренных ст. 158 и 159 УК РФ, совершенных с использованием ИТТ, а также преступлений, уголовные дела о которых направлены в суд, но массив деяний, уголовные дела о которых приостановлены по п. 1-3 ч. 1 ст. 208 УПК РФ, по-прежнему превышает эти показатели более чем в три раза.

4 Противодействие мошенническим практикам. URL: https://cbr.ru/information_security/pmp/ (дата обращения: 15.02.2023).

Проведенный анализ показывает, что преступность в сфере ИТТ имеет разнообразные проявления, а перечень способствующих ей факторов широк и неоднороден. Наиболее перспективными направлениями повышения эффективности противодействия преступности данного вида следует считать правовое просвещение населения, повышение уровня финансовой и компьютерной грамотности граждан, виктимологическую профилактику, о которой ранее уже говорилось, более активное информирование граждан о способах совершения мошеннических действий, а также совершенствование и более активное применение технических средств обеспечения безопасности информации. Имеется необходимость принять дополнительные меры, направленные на совершенствование кадрового обеспечения деятельности правоохранительных органов в сфере выявления, пресечения и расследования преступлений, совершаемых в информационном пространстве, в том числе повышение квалификации сотрудников правоохранительных органов, их профессиональную переподготовку, а также на совершенствование технического оснащения правоохранительных органов[5].

В условиях агрессивных действий криминального мира лишь общественное мнение может положительно повлиять на процесс создания условий и возможностей для правоохранительных органов в части оперативного использования современных криминалистических методов, инструментов и рекомендаций при выявлении и расследовании преступлений, связанных с дистанционным хищением денежных средств, и иных видов киберпреступности [1, с. 32].

Чтобы обезопасить собственные финансовые активы, необходимо соблюдать ряд основных правил:

– следует использовать отдельную дебетовую карту для совершения покупок; пополнять ее разово – только одним платежом; не регистрировать ее в системе мобильных платежей с функцией Near Field Communication, к примеру, МИР Pay, Tinkoff Pay, SberPay и т.д.;

– не следует привязывать электронную почту к банковским картам;

– желательно не оплачивать покупки через сеть Интернет с привязкой банковских реквизитов;

– не переходить по ссылкам интернет-ресурсов, которые были получены от неизвестных пользователей информационного пространства;

– стараться избегать использования VPN-программ в целях сохранения конфиденциальности персональных данных [подр.: 4, с. 239].

5 Отчет о результатах рассмотрения уголовных дел о преступлениях коррупционной направленности по вступившим в законную силу приговорам и другим судебным постановлениям (форма 10.4.1 Судебного департамента при Верховном Суде Российской Федерации) : приказ Судебного департамента при Верховном Суде РФ от 11.04.2017 N 65 // СПС «КонсультантПлюс» (дата обращения: 22.02.2023).

Библиографический список

1. Минзянова, Д.Ф. Организация деятельности оперативных подразделений полиции по раскрытию дистанционного хищения денежных средств в процессе цифровизации / Д.Ф. Минзянова, Д.М. Фарахиев // Современная наука. – 2022. – N 3. – С. 30-33.

2. Нуянзин, С.В. Преступность в сфере информационно-телекоммуникационных технологий: современное состояние и некоторые меры по противодействию ей / С.В. Нуянзин, А.О. Виноградов, С.В. Тришкин // Научный портал МВД России. – 2020. – N 4(52). – С. 45-54.

3. Павловская, Н.В. Преступность в сфере информационно-телекоммуникационных технологий и результаты борьбы с ней / Н.В. Павловская, Д.А. Соколов, А.А. Литвинов // Вестник Университета прокуратуры Российской Федерации. – 2022. – N 6(92). – С. 60-71.

4. Фарахиев, Д.М. Трансформация способов и схем совершения мошеннических действий в процессе цифровизации / Д.М. Фарахиев, С.А. Чередниченко // Научный дайджест Восточно-Сибирского института МВД России. – 2022. – N 4(18). – С. 232-241.

5. Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения) : сборник материалов I Всероссийского науч.-практической конференции (Москва, 27 янв. 2021 г.) / под общ. ред. О.С. Капинус ; [науч. ред. В.В. Меркурьев, П.В. Агапов ; сост. М.В. Ульянов, Н.В. Сальников] ; Университет прокуратуры России. – М., 2021. – 460 с.