Елена Владимировна Андрианова

кандидат социологических наук, доцент, заведующий кафедрой общей и экономической социологии Тюменского государственного университета, г. Тюмень, e.v.andrianova@utmn.ru

Камиль Ильгизович Шакиров

студент направления «Социология» Тюменского государственного университета, г. Тюмень, k1m6@yandex.ru

СОЦИАЛЬНЫЙ ПОРТРЕТ ЖЕРТВ КИБЕРМОШЕННИЧЕСТВА

Аннотация. Многие страны в последние годы сталкиваются с проблемой роста экономических хищений с помощью информационно-коммуникационных технологий. Кибермошенничество представляется как многогранное явление, которое из года в год эволюционирует и виктимизирует все новые социально-демографические группы населения. В работе представлен социальный портрет жертв кибермошенников по результатам исследования их демографических и социально-экономических характеристик. Основой для анализа являются данные официальной статистики, открытые данные Министерства внутренних дел за период 2020–2022 г. в Российской Федерации.

Ключевые слова: кибермошенничество, виктимизация, социальный портрет, жертва.

Elena Vladimirovna Andrianova

Candidate of Sociological Sciences, Associate Professor, Head of the Department of General and Economic Sociology of Tyumen State University, Tyumen, e.v.andrianova@utmn.ru

Kamil Ilgizovich Shakirov

Student of the Sociology department of Tyumen State University, Tyumen, k1m6@yandex.ru

SOCIAL PORTRAIT OF VICTIMS OF CYBERBULLYING

Abstract. In recent years, many countries have been facing the problem of increasing economic theft with the help of information and communication technologies. Cyberbullying is presented as a multifaceted phenomenon that evolves from year to year and victimizes all new socio-demographic groups of the population. The paper presents a social portrait of victims of cybercriminals based on the results of a study of their demographic and socio-economic characteristics. The basis for the analysis is the data of official statistics, open data of the Ministry of Internal Affairs for the period 2020-2022 in the Russian Federation.

Keywords: cyberbullying, victimization, social portrait, victim.

Киберпреступление — это преступная деятельность, совершающаяся при помощи информационных технологий (устройства или сети) [1, с. 78]. Такое деяние может иметь экономический характер, это уже будет называться кибермошенничеством. Последнее имеет цель — причинить ущерб материального (кража денег) или иного характера (кража данных, но без извлечения прямой прибыли). Деяния регулируются Уголовным Кодексом РФ (ст. 157, 159, 272, 273, 274) [2].

Кибермошенничество как преступное деяние имеет несколько стратегий воздействия на жертву:

1. Вишинг (англ. voice + phishing) — вид телефонного мошенничества, когда злоумышленники путем «социальной инженерии» пытаются выведать у жертвы конфиденциальную информацию.

2. Фишинг (англ. phishing) — вид интернет-мошенничества, когда злоумышленники при помощи ссылок (обычно по электронной почте) вынуждают жертву передать им конфиденциальные данные [3, с. 113-114].

Информационные технологии для общества — это безусловное благо, позволившее снизить издержки, связанные с длиной трансакций. Но, с другой стороны, возникли новые издержки, которые вызваны использованием этих технологий [4, с.133]. И как часто бывает, «слабым местом» сетевой части являются не информационные технологии, а сам человек. Современное общество научилось распознавать кибермошенников и им противостоять, но технологии обмана не стоят на месте, что позволяет «информационным злоумышленникам» виктимизировать новые слои населения.

Кибермошенничество в России имеет глубокие корни. Первое киберпреступление на территории СССР произошло в Вильнюсе в 1979 г. Оно было связано с недостатком программного обеспечения ЭВМ «Онега», что позволило сотруднику почты совершать хищения денежных средств, направляемых пенсионерам (пенсии, пособия, льготы). Но для нашего понимания, как развивалось массовое кибермошенничество, стоит рассмотреть его историю, начиная с 1990-х, когда информационные технологии начали повсеместно проникать на российский рынок.

Первый этап связан с развитием в 1990-х гг. телефонных сетей, а также их распространением по всей России. Прочного законодательства, регулирующие киберпространство, еще не было. Кибермошенники во всю использовали «социальную инженерию» для вымогания конфиденциальных данных. Интернет был еще в самом зачаточном состоянии и не имел большего распространения. Чаще всего жертвами кибермошенничеств были люди старшего возраста.

Второй этап связан с развитием и распространением в 2000-х широкополосного интернета и социальных сетей. С того времени телефонное и интернет-мошенничество были разграничены. Кибермошенники начали использовать автоматизированные системы сбора данных в купе с «социальной инженерией». С того времени было зафиксировано, что социальный портрет жертвы кибермошенничества стал «молодеть» [5, с. 139].

На современном этапе развития кибермошенничества стала намного больше применяться «социальная инженерия», а не взлом технических средств [6, с.120]. Такой тренд обусловлен эффективным мониторингом фишинговых сайтов со стороны правоохранительных органов и Минцифры. Но, в любой системе «слабое место» — это человек.

По данным МВД РФ за 2022 г. количество зарегистрированных преступлений, связанных с кибермошенничеством выросло на 215% по сравнению с 2019 годом. Тут сыграла особую роль пандемия, вызванная COVID-19, которая в свою очередь ускорила цифровизацию экономики (см. рис. 1).

По данным ЦБ РФ за 2022 г. кибермошенники нанесли ущерб российской экономике на 14.1 млрд рублей, что составляет рост на 69% по сравнению с 2020 г. (см. рис. 2). Однако тут стоит отметить, что данные ЦБ связаны с «операциями, которые даны без согласия клиента», что не учитывает общий ущерб от кибермошенничества (например, с применением «социальной инженерии»). Однако, по данным RTM Group общий ущерб от кибермошенничества может достигать 165 млрд рублей. Такая цифра свидетельствует об очень опасном явлении, которое может воздействовать на экономику в макроэкономических масштабах.

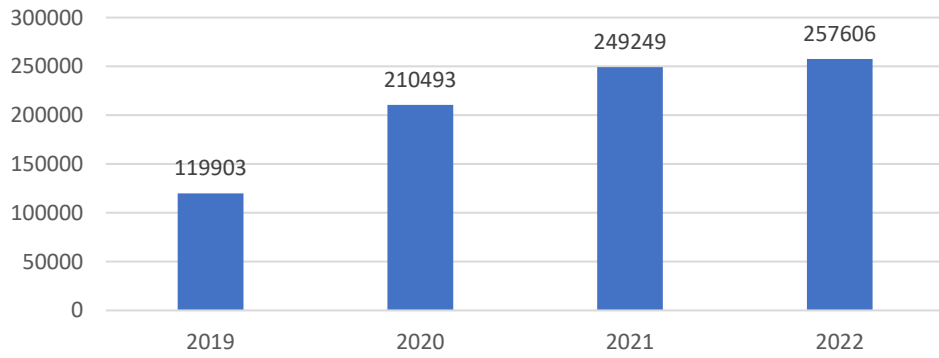

Рис. 1. Количество преступлений, совершенных по статьям 159 УК РФ в сфере информационно-телекоммуникационных технологий

Источник [7-9].

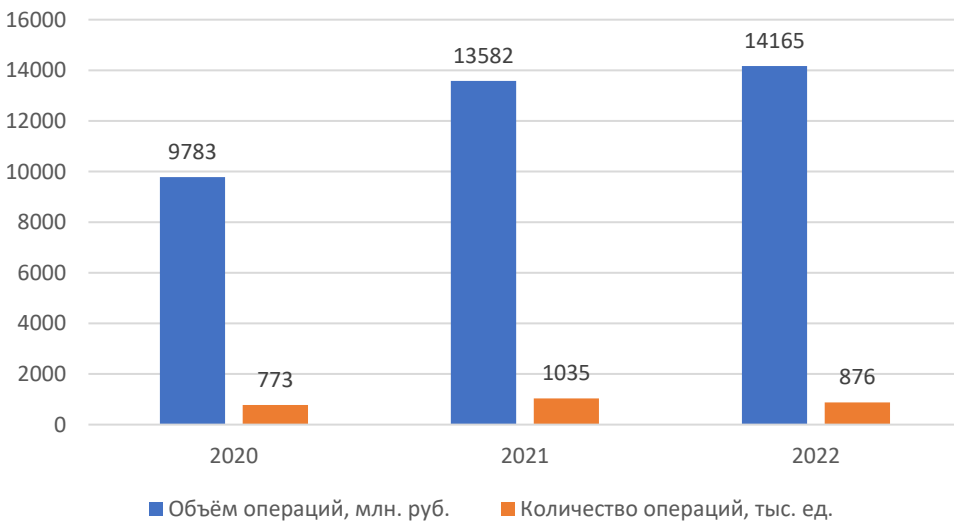

Рис. 2. Общий объем и количество операций без согласия клиентов

Источник: [10, 11].

В свою очередь аналитики ЦБ РФ утверждают, что количество кибермошенничеств неуклонно падает, но с другой стороны, растет их «средний чек». Это говорит о том, что действия кибермошенников стали целевыми и эффективными, что нам дает право использовать предполагаемый социальный портрет жертвы.

Мы будем опираться на данные банковских структур (ЦБ и банки) и виктимиологической статистики МВД [12, с. 19-22], так как они в большей степени располагают информацией об их заемщиках и подозрительных транзакциях. Наша цель — это выявить общие закономерности и спрогнозировать, как будет меняться данный социальный портрет (табл. 1).

Таблица 1

Социальный портрет жертвы кибермошенничества в Российской Федерации

Социально дем. характеристики	*Банки и МВД РФ*				
	ЦБ РФ	*ВТБ*	*ОТП Банк*	*КБ ФинТех*	*МВД РФ*
Возраст (лет)	25–44	35–49	18–33	28–37	30–49
Семейное положение	–	–	Холост/не замужем	Холост/не замужем	–
Проживание (город/село) /место жительства	Город	–	–	Город	Город
Уровень достатка/источник дохода	Средний	–	–	–	Без постоянного источника доходов

Источник: составлено авторами на основе данных [12-16].

Для более глубокого анализа стоит разобрать каждый пункт по отдельности, чтобы показать наглядность данного социального портрета.

1. В научных работах часто указывают в социальном портрете половую принадлежность респондента. Однако, в этом случае, количество мужчин и женщин будет в равных количествах и будет повторять структуру половозрастной пирамиды в РФ.

2. Возраст жертв кибермошенничества по данным банков и МВД имеет очень широкий разброс. Однако, мы видим, что чаще всего жертвами становится наиболее экономически активные граждане, что расходится с зарубежными данными по кибермошенничеству в США, где люди старше 50 лет чаще всего попадают на кибермошенников [17].

3. Семейное положение играет роль «сдерживающего механизма». Как гипотеза, люди в браке чаще друг с другом советуются, чтобы обезопасить свои средства от мошенников.

4. Город как сильный экономический агент, замыкающий на себе платежеспособный спрос и множество услуг, наиболее подвержен влиянию кибермошенников.

5. Однако, тут стоит обратить внимание на то, что по статистике МВД РФ наиболее подверженные (по доходу) виктимизации — это люди без постоянного источника дохода. Как гипотеза, такие люди наиболее склонны к «легким деньгам», поэтому попадаются чаще на мошенников, нежели другие слои населения. Также мы можем предположить, что прекарные занятые чаще всего попадаются на кибермошенничества по сравнению с имеющими постоянную работу.

Данный обзор социальных портретов дает нам понять, какие слои населения наиболее подвержены виктимизации, но для более полного анализа нужны дальнейшие исследования социального портрета жертвы с более глубоким применением вторичных данных банков и правоохранительных органов РФ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика / С.И. Буз // Юристъ-Правоведъ. — 2019. — № 4(91). — С. 78-82.
2. Что такое кибермошенничество и какая наступает за него уголовная ответственность // Московская межрегиональная транспортная прокуратура: сайт. — URL: https://epp.genproc.gov.ru/web/mmtp/activity/legal-education/explain?item=69345532 (дата обращения 17.04.2023).
3. Маилян А. В. Актуальные вопросы расследования и раскрытия кибермошенничества «Фишинг» // Философия права. — 2022. — № 2. — С. 112-115.
4. Красовская Н. Р., Гуляев А. А. К вопросу о кибермошенничестве / Н. Р. Красовская, А. А. Гуляев // Вестник Удмуртского университета. Социология. Политология. Международные отношения. — 2022. — № 1. — С. 133-138.
5. Старостенко О. А. Закономерности становления и развития кибермошенничества в России и за рубежом/ О. А. Старостенко // Вестник Уральского юридического института МВД России. — 2021. — № 1. — С. 138-143.
6. Асанова И.П. Актуальные вопросы борьбы с масштабами роста кибермошенничества / И.П. Асанова // Вестник Российского университета кооперации. — 2021. — № 4 (46). — С. 120-123.
7. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2020 г. // МВД РФ: сайт. — URL: https://мвд.рф/reports/item/22678184 (дата обращения 17.04.2023).
8. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2021 г. // МВД РФ: сайт. — URL: https://мвд.рф/reports/item/28021552 (дата обращения 17.04.2023).
9. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2022 г. // МВД РФ: сайт. — URL: https://мвд.рф/reports/item/35396677 (дата обращения 17.04.2023).
10. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2021 год // Аналитический обзор ЦБ РФ: сайт. — URL: https://cbr.ru/analytics/ib/operations_survey/2021/ (дата обращения 17.04.2023).
11. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2022 год // Аналитический обзор ЦБ РФ: сайт. — URL: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения 17.04.2023).
12. Кабанов П.А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021–2022 гг. / П.А. Кабанов // Виктимология. — 2023. — № 1. С. 17-28.
13. В России описали портрет типичной жертвы телефонных мошенников // Информационный портал Лента. ру: сайт. — URL: https://lenta.ru/news/2020/12/06/victim/ (дата обращения 17.04.2023).
14. ВТБ описал типичную жертву финансовых мошенников // РБК: сайт. — URL: https://www.rbc.ru/society/23/06/2021/60d1cd2c9a7947cd10c61ba3?utm_source=yxnews&utm_medium=desktop (дата обращения 17.04.2023).
15. Кабанов П.А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021–2022 гг. / П.А. Кабанов // Виктимология. –2023. — № 1. С. 17-28.
16. ОТП Банк составил социальный портрет жертвы телефонных мошенников // ОТП Банк: сайт. — URL: https://www.otpbank.ru/about/press-centr/news/0115384/ (дата обращения 17.04.2023).
17. Internet Crime Report 2021 // Federal Bureau of Investigation: [website]. — URL: https://www.ic3.gov/media/PDF/AnnualReport/2021_IC3Report.pdf (дата обращения 17.04.2023).