УДК 343.3/.7, 343.9

К ВОПРОСУ О ВЛИЯНИИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ: ПРЕВЕНЦИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Проурзина Ольга Юрьевна – преподаватель-методист информационного центра ФГКОУ ВО Санкт-Петербургский университет МВД России, эл. почта: oprourzina@mail.ru.

198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1, тел. +7-921-655-14-24

«Человек должен быть готов к переменам и адаптации в новых условиях. Побеждает всегда тот, кто не остается равнодушным, кто борется.»

В.И. Терентьева

THE IMPACT OF AUTOMATED INFORMATION SYSTEMS: CRIME PREVENTION, PERFORMED USING SOCIAL ENGINEERING

Prourzina Olga Yurievna – teacher-methodologist of the information center of Saint Petersburg University of the Ministry of Internal Affairs of Russia, e-mail: oprourzina@mail.ru.

198206, Saint Petersburg, Pilutov str, 1, mobile phone: +7-921-655-14-24

Аннотация: в настоящей статье проведен обзор детерминант виктимности граждан, ставших жертвами преступлений, совершенных с применением информационно-коммуникационных технологий и социальной инженерии. Рассмотрены способы противодействия правонарушениям, предложена разработка системы социальной превенции в качестве обеспечения национальной безопасности государства и защиты благополучия населения.

Ключевые слова: безопасность, преступность, социальная инженерия, доверие, уязвимость, цифровизация населения.

Abstract: this paper provides a review of the determinants of victimization of citizens who have become victims of crimes committed using information and communication technologies and social engineering. Ways to combat crime are considered, and the development of a system of social prevention is proposed to ensure the national security of the state and protect the well-being of the population.
Key words: security, crime, social engineering, trust, vulnerability, digitalization of the population.

Введение. Наше общество шагнуло в эру цифровых технологий. Общество Информации применяет средства цифровизации во всех сферах деятельности. Информационно-коммуникационные устройства стали повседневными спутниками в профессиональной деятельности и личной жизни человека.

В современном мире мы наблюдаем, как новые технологии стали частью личной среды, достраивают когнитивную и социальную системы. Зачастую именно законопослушные граждане становятся жертвами мошеннических схем, организованных преступными группами. Мошенники на доверии применяют типовые сценарии для совершения преступлений в отношении граждан, чьи персональные данные стали им известны. Применяя методы запугивания и убеждения преступники, действующие в рамках сообщества, вынуждают жертву действовать по заранее заготовленному сценарию. Используя исключительно вербальное побуждение, злоумышленники получают необходимую для дистанционного хищения информацию, убеждают граждан самостоятельно перевести денежные средства на неизвестные счета. Действия преступников организованы исключительно в дистанционном формате с использованием информационных систем различного назначения, начиная от ведения переговоров посредством сотовой связи и заканчивая виртуальным сопровождением жертв правонарушений по маршруту следования в финансово-кредитные организации. Целью преступников является получение кодов для доступа к счетам гражданина в финансовых организациях для управлениями

ими. Манипуляции над человеком в процессе телефонного разговора, внушение страха за свои сбережения, навязывание своего мнения и вынуждение действовать по указанию неизвестных – сегодня мы называем это методами социальной инженерии. На самом деле это ни что иное, как мошенничество на доверии, однако современность диктует свои условия и научно-технический прогресс не только помогает развиваться обществу и улучшать все сферы деятельности человечества, но и динамично вооружает преступность.

Целью настоящего исследования является формулирование предложений для разработки системы социальной превенции цифровых преступлений, основанной на условиях возникновения виктимности населения в схемах мошенничества, совершенного с применением методов социальной инженерии.

Задачи, которые необходимо решить для достижения поставленной цели, определим как способы противодействия социальной инженерии преступников.

Обзор проблемы. Согласно данным отчетов, ежегодно публикуемым на официальном сайте Центрального Банка России объем денежных потерь российских граждан от телефонного мошенничества в 2022 году составил 14,2 миллиарда рублей. При этом максимальная, единовременно похищенная сумма достигла 500 миллионов рублей. Под влиянием телефонных преступников в 2022 году российские граждане пытались оформить кредиты на 200 миллиардов рублей, а 83% граждан России хотя б раз сталкивались с попытками кибермошенничества.

Таблица 1

Общий объем и количество операций, совершенных без согласия клиентов

Год	Общий объем операций без согласия клиента, млрд. руб.	Количество операций, тыс. ед.	Объем операций, млрд. руб.	
			Физ. лица	Юр. лица
2021	13, 582	1 035,01	12, 131	1, 451
2022	14, 165	876,59	13, 357	0, 807
2023	15, 791	1 165,99	15, 258	0,533

Заместитель председателя Правления ПАО «Сбербанк России» Станислав Кузнецов сообщил, что Сбербанк зафиксировал рост числа попыток телефонного мошенничества в отношении россиян. В 2023 году число попыток телефонного мошенничества в отношении россиян достигло 8,6 миллионов в сутки против 5 миллионов в 2022 году. По его словам, основная угроза - это телефонное мошенничество, доля которого в общем объеме кибермошенничества составляет 90%. Рекордный рост попыток кибермошенничества в отношении россиян в 2022 году число достигло 5 млн в сутки, а сегодня это уже 8,6 миллионов в сутки. По его словам, самой популярной схемой мошенничества по-прежнему остается схема с переводом или взносом на «безопасный счет». По оценкам Сбербанка, на нее приходится свыше 77% попыток мошенничества. С. Кузнецов пояснил, что распространенными уловками в рамках этой схемы являются звонок от имени службы безопасности о смене финансового номера, оформление кредита на клиента и попытка снять деньги у него.

В настоящее время в нашей стране отсутствует методика расследования так называемых цифровых преступлений. Согласимся с Лозовицкой Г.П., д.ю.н., профессором кафедры государственно-правовых и уголовно-правовых дисциплин Российского экономического университета им. Г.В. Плеханова, которая утверждает, что « определения высокотехнологичной и цифровой преступности, равно как и преступности технотронной должны быть закреплены в нормативных правовых актах Российской Федерации и за их совершение должна быть предусмотрена уголовная ответственность, равнозначная ответственности за тяжкие и особо тяжкие преступления.»

Социальная инженерия как маркер технологического развития общества в настоящее время приобрела негативные коннотации. Для противодействия преступности, применяющей новейшие технологии в умелом сочетании с известными ранее способами совершения преступлений необходим ряд мер, для предупреждения данного вида преступлений. Мы считаем, что сегодня требуется

разработка мер государственного и ведомственного регулирования для применения системы социальной превенции цифровых преступлений.

Как справедливо заметил Себякин А.Г. «тенденции роста преступлений, совершённых с использованием компьютерных и информационно-телекоммуникационных средств, обуславливают необходимость разработки адекватных мер по внедрению в практику научно обоснованных технико-криминалистических средств, приёмов и методов, направленных на раскрытие и расследование преступлений». Однако для недопущения совершения данных преступлений или снижения их количества необходимо разработать систему превенции.

Приказом МВД России от 29.12.2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации» была создана так называемая «киберполиция». Задачи, возложенные на это подразделение, будут лишь увеличиваться, а расследуемые преступления усложняться, на наш взгляд. Сегодня назрела необходимость в помощи правоохранительным органам для борьбы с киберпреступностью.

Тщательное изучение влияние современных достижений науки и техники позволит использовать их во благо человечества, а нежелательные проявления исключить или минимизировать.

Практически ежедневно в средствах массовой информации появляются сведения о новой жертве телефонного мошенничества. И это уже становится обыденностью. Поражают размеры денежных средств, которыми удалось завладеть правонарушителям и по-детски наивная доверчивость жертвы, вне зависимости от пола, возраста, рода деятельности, образования, уровнем владения информационными технологиями и видом доступных информационно-коммуникационных устройств. Каждый случай данного вида преступления по-своему уникален, ведь всех жертв нельзя объединить по нескольким признакам, их объединяет лишь то, что они покорно выполнили все указания неизвестных

лиц исключительно при телефонном общении и лишились крупной суммы денег, самостоятельно снятой со своих счетов или оформленных в кредит.

Анализ информационного контента представлен схожими событиями правонарушений, но подчас они дополняются тем, что мошенники использующие доверие граждан, побуждают их не только совершать самопереводы, но и привлекать новых жертв, становиться соучастниками следующей криминальной схемы.

Обязательным условием для успешного проведения мошеннической схемы является выполнения жертвой нескольких условий, а именно – постоянно поддерживать телефонный разговор, не сообщать об угрозе хищения средств близким, сотрудникам финансовых учреждений и правоохранительных органов, не отказываться от выполнения указаний, поступающих от неизвестных, а самое главное – не проверять реальность угрозы хищения и не устанавливать личность неизвестных, которые предлагают «спасти» сбережения. Учитывая то, что жертвами преступления становятся граждане из различных социальных слоев населения, возрастных групп, имеющий различный уровень дохода, суммы накоплений, в разной степени владеющих информационными технологиями, использующими различного уровня сложности информационно-коммуникационные абонентские устройства связи, считаем необходимым организовать профилактику с применением официальных средств массовой информацией, обращением медийных персон и представителей органов власти.

В настоящее время данный вид преступлений динамично меняет способы совершения правонарушений, однако орудиями преступления по – прежнему выступают информационные системы и технологии. Согласимся с Долговой Н.В. в части заключения ее исследования о неготовности населения к цифровизации. Именно высокие темпы внедрения в нашу жизнь новых информационно-коммуникационных технологий и устройств связи, отсутствие обучения принципам личной информационной безопасности и защите

персональных данных приводят к ошибкам и создают благоприятные условия для преступников.

В целях разработки Программы социальной превенции необходимо знакомить население с понятием информационной безопасности и цифровой гигиены. Для этого считаем нужным привлекать сотрудников, обеспечивающих регистрацию на портале государственных услуг и работников финансовых организаций, как первичное звено, участвующее в оформлении и выдаче банковских карт (платежных средств) и реквизитов для доступа к счетам.

Также немаловажным будет организация профилактических бесед от младшего к старшему, так как молодежь более подготовлена к работе с информационными технологиями и сможет доступным языком пояснить родственникам угрозы от передачи кодов неизвестным, которые получены лично Вами.

Для наглядной агитации считаем действенным организовать конкурс постеров и плакатов для курсантов ведомственных образовательных учреждений и студентов юридических факультетов. В целях повышения эффективности методов борьбы с цифровыми преступлениями предлагаем организовать конкурс на изготовление социальных видеороликов и аудиозаставок для использования в общественных местах, на транспорте, в которых лаконично и доступно пояснять об опасности передачи личной информации неизвестным.

Следует помнить, что все активные действия, которые привели к потере денежных средств, жертвы совершают сами. Никакой реальной угрозы при обращении от неизвестных по телефону не исходит. Для проверки данной информации необходимо и достаточно прервать входящий звонок, инициированный неизвестными и самостоятельно обратиться в службу безопасности банка.

20 февраля 2024 г. Всероссийский центр изучения общественного мнения (далее - ВЦИОМ) представил результаты мониторингового опроса россиян, посвященного телефонному мошенничеству.

«В ходе февральского опроса 67% россиян признались, что за последние полгода-год получали фейковые звонки, тогда как еще в 2021 г. о таком опыте могли рассказать чуть больше половины наших сограждан (57%, +10 п.п. за три года). Согласно данным ВЦИОМ определен ряд причин, по которым злоумышленники отдают предпочтение телефонным звонкам, одна из наиболее очевидных — в ходе разговора гораздо проще, чем в обезличенных СМС-рассылках, расположить к себе потенциальную жертву, а если повезет — выманить заветную информацию и опустошить банковский счет.

Согласно полученным результатам, главный критерий выбора потенциальной жертвы — место проживания. Наиболее подвержены телефонному мошенничеству жители обеих столиц: с ним сталкивались 85% москвичей и петербуржцев (в том числе 81% получали звонки от мошенников, 26% — СМС-сообщения), тогда как в сельской местности с телефонными аферистами имели дело 57% наших сограждан: 55% получали звонки, каждый десятый — СМС (10%).

В качестве основополагающего вывода нашего исследования считаем нужным Организовать государственное исследование на постоянной основе для проведения социального мониторинга о влиянии цифровизации населения.

Список литературы

1. Авакьян С.А. Информационное пространство знаний, цифровой мир и конституционное право // Конституционное и муниципальное право. 2019. № 7. С. 26.

2. Жданов Ю.Н., Овчинский В.В. Киберполиция XXI века. Международный опыт / под ред. С.Е. Кузнецова. – М.: Международные отношения, 2020. – 288 с.

3. Оценка цифровой готовности населения России [Текст]: докл. к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / Н. Е. Дмитриева (рук. авт. кол.), А. Б. Жулин, Р. Е. Артамонов, Э. А. Титов; Нац. исслед. ун-т «Высшая школа экономики». — М.: Изд. дом Высшей школы экономики, 2021. — 86 с.

4. Правовое обеспечение социальной справедливости в условиях цифровизации: сборник материалов Всероссийской научно-практической конференции с международным участием / отв. Ред. Т.А. Сошникова. – Москва: Изд-во Московского гуманитарного университета, 2020. – 402 с.

5. Смушкин А.Б. Концепция дистанционной криминалистики: монография / под ред. докт. юрид. наук, проф. В.Б. Вехова. – М.: Юрлитинформ, 2024. – 256 с.

6. Субботина Л.Ю. Что понимать под состоянием безопасности личности // Ярославский психологический вестник. 2021. № 3 (51). С. 37-42.

7. Официальный сайт «Российская газета» (URL: https://rg.ru/2023/03/03/v-2022-godu-telefonnye-moshenniki-pohitili-bolee-14-mlrd-rublej.html). Дата обращения: 21.02.2024.

8. Официальный сайт ВЦИОМ. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring?utm_source=Rambler&utm_medium=finance&utm_campaign=transitio// Дата обращения: 21.02.2024).