УДК 343.3/.7

СУЩНОСТЬ КИБЕРПРЕСТУПНОСТИ КАК СОВРЕМЕННОГО ВИДА МОШЕННИЧЕСТВА
The essence of cybercrime as a modern type of fraud

О. Л. Альтшулер-Феррейра, преподаватель кафедры иностранных языков
Уральский юридический институт МВД РФ
(Екатеринбург, ул. Корепина, 66)

Рецензент: Б. А. Воронин, доктор юридических наук

Аннотация

В статье рассматривается феномен киберпреступности как нового явления и устанавливается его связь с преступлениями, подпадающими под понятие «мошенничество». Автор рассматривает перспективы данного феномена в изменяющихся социальных условиях с привлечением футурологических материалов современной фантастики.

Ключевые слова: киберпреступность, мошенничество, компьютеры, информационное общество.

Summary

The article examines the phenomenon of cybercrime as a new phenomenon and establishes its connection with crimes that fall under the concept of “fraud.” The author examines the prospects for this phenomenon in changing social conditions using futurological materials from modern science fiction.

Keywords: cybercrime, fraud, computers, information society.

Мошенничество в Интернете или кибермошенничество – это различные способы мошеннических действий, осуществляемых киберпреступниками в Интернете. Существует много вариантов мошенничества: через фишинговые сообщения, социальные сети, SMS-сообщения на сотовый телефон, звонки мошеннической технической поддержки, псевдоантивирусные программы и т. д. Основная цель этих вариантов мошенничества может варьироваться от кражи кредитных карт, перехвата пароля и имени пользователя до кражи персональных данных.

Ст. 159 УК РФ определяет мошенничество следующим образом: «Мошенничество это хищение чужого имущества или приобретение права на ичужое имущество путем обмана или злоупотребления доверием [].

Сайт антивируса Касперского определяет киберпреступность следующим образом: «Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов. Киберпреступления совершают частные лица и организации – от начинающих хакеров до слаженных группировок, которые используют продвинутые методики и хорошо подкованы технически» [1]. Зачастую киберпреступность граничит с мошенничеством – по сути, киберпреступление и есть разновидность мошенничества либо воровства, выполняемого при использовании современных технических средств. Киберпреступник

владеет этими средствами лучше своих жертв – это необходимое условие такого рода преступлений.

Это чаще всего не личное общение преступника с потерпевшим, преступник может вообще отбывать наказание за другое преступление, а коммуникация осуществляется через гаджеты. Граждане достаточно слабо владеют этой техникой, следовательно, она лежит вне опыта человека, при личном контакте он не отдал бы деньги мошеннику, но с легкостью переводит свои сбережения на «безопасный счет».

Преступники как правило представляются сотрудниками банка, что при личном контакте было бы также затруднительно.

Число схем такого мошенничества велико и все увеличивается.

В 2023 году в суд было передано дело о интернет-мошенничестве: двое жителей Екатеринбурга открыли в соцсетях шесть сайтов якобы интернет-магазинов предметов самообороны, приняли заказы и получили предоплату, товаров же отгружать не собирались. С июля по ноябрь 2022 года аферисты похитили более 2,2 млн рублей у 45 человек [8].

Наличные деньги уходят в прошлое, регулярные банковские транзакции совершают сегодня не работники банковской сферы, как в недавнем прошлом, а простые граждане самостоятельно, без личного обращения в банк.

Перспективы развития данной ситуации позволяет оценить обращение к жанру фантастики, писатели, работающие в нем, в первую очередь пытаются отследить, оценить и экстраполировать тенденции В 2022-м году вышел сборник фантастических рассказов «Время вышло. Современная русская антиутопия» [2] – первый же рассказ данного сборника «Аз Иванов. Выход в деньги» представляет новую концепцию «мыслящих денег»: валюта «азио», электронные деньги будущего, по мысли писателя А. Рубанова, это баллы, начисляемые гражданину за выполненный труд, то есть, по сути, трудодни. Деньги стремятся быть потраченными, поэтому накопление не предусмотрено: баллы списываются со счета в конце года и накопление их начинается сначала 1 января каждого года [2, с. 23]. Украсть такие деньги невозможно, и это кажется решением проблемы. С другой стороны, создается картина, напоминающая исторически известные в Советской России «трудодни». Такие «квазиденьги» исключают появление у граждан по-настоящему крупных сумм (что приводит на память мысли Карла Маркса об экспроприации трудящихся), так что, если автор прав, киберпреступность со временем полностью переместится в область государственных либо частных предприятий и финансовых организаций, каковые и станут мишенью киберпреступников будущего.

Тем не менее, сегодня техническая киберпреступность атакует финансовый сектор экономики, кибермошенники же сосредоточены на простых гражданах. Для справки: как подсчитали аналитики RTM Group, «в 2021 году общий ущерб от преступлений с использованием компьютерных технологий в России превысил 150 млрд рублей, через год он может достичь 165 млрд рублей» [6]. Аналитики оказались полностью правы, уже к середине 2023 года экономике *России* действиями *киберпреступности* уже был нанесён *ущерб* в 203,3 млрд руб., хотя цель подобного прогнозирования остается не до конца понятной [7].

Важным аспектом проблемы представляется возраст потерпевших – в среднем они старше 55 лет, значит можно сформулировать предварительную гипотезу, что молодежь менее подвержена риску оказаться жертвой кибермошенника, следовательно, проблема со временем решится сама собой. Однако по статистике молодежь чаще сталкивается с кибермошенниками, просто потому, что больше общается в киберпространстве.

Очевидно, рассчитывать на самостоятельное разрешение проблемы было бы безответственно, поэтому органы внутренних дел, и прежде всего полиция, принимают все возмож-

ные меры по предупреждению киберпреступлений. Меры эти носят преимущественно коммуникативный характер – собственно, речь идет о предупреждении граждан и о пропаганде бдительности.

Сфера пропаганды все время расширяется, включая уже и печатную продукцию, и стенды на улицах, в транспорте, в интернете и пр.

Выводы. Победить киберпреступность можно только усилиями всего общества путем формирования социального иммунитета к киберпреступности. Иммунитет этот должен включать бдительность в области финансов и готовность сотрудничать с органами внутренних дел как с главным защитником граждан от преступников нового типа [3, 4].

Библиографический список

1. Что такое киберпреступность? Защита от киберпреступности [Электронный ресурс] // Kaspersky. Режим доступа: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime/ (дата обращения: 19.11.2023).
2. *Рубанов А*. Аз Иванов. Выход в деньги // Время вышло. Современная русская антиутопия. М.: Альпина-нонфикшн, 2022. С. 23.
3. *Багрецов Д. Н*. Общественный порядок и коллективная безопасность как центральные идеологемы для консолидации общества и основа педагогической деятельности в гуманитарной сфере // Молодежь и наука. 2023. № 7.
4. *Багрецов Д. Н., Хомутникова Е. А., Копнина В. А., Капицкий В. Н*. Анализ теорий развития творческого потенциала студентов // Мир науки, культуры, образования. 2019. № 4 (77). С. 52-55.
5. Эксперты назвали низкую цифровую грамотность россиян причиной роста киберпреступности [Электронный ресурс] // Форбс. Режим доступа: https://www.forbes.ru/tekhnologii/455881-eksperty-sprognozirovali-rost-userba-ot-kiberprestupnosti-v-rossii-do-165-mlrd-rublej (дата обращения: 19.11.2023).
6. УК РФ Статья 159. Мошенничество [Электронный ресурс] // Консультант плюс. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdf64b7c9cfd62e90d7f55f9b5b7b72b755/ (дата обращения: 156.01.2024).
7. Потери от киберпреступности [Электронный ресурс] // Tadviser. Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D0%B8 (дата обращения: 15.01.2024).