DOI: 10.18287/2542-047X-2021-7-2-133-137

НАУЧНАЯ СТАТЬЯ

УДК 342.9

Дата поступления: 10.04.2021
рецензирования: 15.05.2021
принятия: 25.05.2021

Мошеннические действия с применением информационно-телекоммуникационных технологий в сфере мобильных интернет-приложений

К. И. Озеров
Московский университет МВД России имени В. Я. Кикотя, Москва, Российская Федерация
E-mail: ozerov.kir@yandex.ru

Аннотация: В статье рассматривается специфика совершения мошеннических действий в области мобильных Интернет-приложений. Затрагивается вопрос о безопасности официальных (App Store, Google Play) и неофициальных платформ по скачиванию пользовательских программ для различных целей. Приводятся примеры совершения мошенничеств, и демонстрируются негативные от них последствия. Раскрывается суть fleeceware-приложений и отмечаются плюсы и минусы операционных систем IOS и Android, которые являются технической базой в мобильных устройствах крупнейших фирм. Отмечается возрастная категория, которая в большей степени подвергается или может подвергаться незаконным действиям со стороны мошенников в сфере IT-технологий. Делается акцент на некоторые пробелы в техсистемах и законодательстве, при которых мошенник избегает уголовного преследования. Подтверждается высокая латентность подобной преступности по причине небольшого ущерба у жертв посягательства, если рассматривать каждого потерпевшего по отдельности, а также по причине сложно-структурности самого преступления. Предлагаются меры по недопущению мошеннических действий, связанных с онлайн-приложениями на мобильные устройства в отношении самого себя.
Ключевые слова: мошенничество; информационно-телекоммуникационные технологии; Интернет-приложения; мобильное устройство; вредоносное программное обеспечение; уголовная ответственность; киберсреда; киберугроза; киберпреступление.
Цитирование. Озеров К. И. Мошеннические действия с применением информационно-телекоммуникационных технологий в сфере мобильных интернет-приложений // Юридический вестник Самарского университета. 2021. Т. 7, № 2. С. 133–137. DOI: https://doi.org/10.18287/2542-047X-2021-7-2-133-137.
Информация о конфликте интересов: автор заявляет об отсутствии конфликта интересов.

Кирилл Игоревич Озеров – адъюнкт Московского Университета МВД России имени В.Я. Кикотя, 117437, Российская Федерация, г. Москва, ул. Академика Волгина, 12.

SCIENTIFIC ARTICLE

Submitted: 10.04.2021
Revised: 15.05.2021
Accepted: 25.05.2021

Fraudulent actions using information and telecommunications technologies in the field of mobile Internet applications

K. I. Ozerov
Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V. Y. Kikot, Moscow, Russian Federation
E-mail: ozerov.kir@yandex.ru

Abstract: the article deals with the specifics of committing fraudulent actions in the field of mobile Internet applications. The question of the security of official (App Store, Google Play) and unofficial platforms for downloading user programs for various purposes is raised. Examples of fraud are given and their negative consequences are demonstrated. The essence of "fleeceware"-applications is revealed and the pros and cons of the IOS and Android operating systems, which are the technical base in the mobile devices of the largest companies, are noted. There is an age category that is more exposed or may be exposed to illegal actions on the part of fraudsters in the field of IT technologies. In turn, the emphasis is placed on some gaps in those. systems and legislation in which the fraudster avoids criminal prosecution. The high latency of such crimes is confirmed due to the small damage to the victims of the assault, if we consider each victim separately, as well as due to the complexity of the crime itself. Measures are taken to prevent fraudulent actions related to online applications on mobile devices against yourself.
Key words: fraud; information and telecommunications technologies; Internet applications; mobile device; malicious software; criminal liability; cyber environment; cyber threat; cybercrime.
Citation. Ozerov K. I. *Moshennicheskie deistviya s primeneniem informatsionno-telekommunikatsionnykh tekhnologii v sfere mobil'nykh internet-prilozhenii* [Fraudulent actions using information and telecommunications technologies in

the field of mobile Internet applications]. *Iuridicheskii vestnik Samarskogo universiteta* [Juridical Journal of Samara University], 2021, vol. 7, no. 2, pp. 133–137. DOI: https://doi.org/10.18287/2542-047X-2021-7-2-133-137 [in Russian].
Information about the conflict of interests: author declares no conflict of interests.

© Ozerov K. I., 2021
Kirill I. Ozerov – adjunct of Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V. Y. Kikot, 12, Akademika Volgina Street, Moscow, 117437, Russian Federation.

Информационно-телекоммуникационные технологии стали важнейшим элементом жизнедеятельности человека XXI века. Представить свою повседневную деятельность без компьютера, сотового телефона или планшета затруднительно, в особенности когда на этих перечисленных устройствах нет подключенного Интернета.

Каждый человек вне зависимости от своего возраста и социального статуса в той или иной мере погружается в информационную среду, совершая электронные платежи, получая заработную плату на свою банковскую карточку.

В связи с глобализацией и широкой областью применения информационно-телекоммуникационных технологий преступность переходит в IT-сферу, где в настоящее время сосредоточено множество значимой информации, материальных ресурсов и других благ.

Злоумышленниками изобретаются вредоносные программы как для хищения материальных ценностей, так и для сохранения анонимности киберпреступника.

Под большую угрозу подпадают рядовые граждане, особенно те, которые не имеют специальных знаний и умений в информационной среде, юридические лица, в частности малый и средний бизнес, ибо нет возможности финансировать кибербезопасность, чтобы ее функционирование было на высоком уровне и способствовало предотвращению виртуальных атак с преступной стороны [1].

Особое внимание хотелось бы уделить «скаму», связанному с мобильными приложениями, требующими плату за полноценное пользование ими. «Скам» – это понятие, означающее жульничество, мошенничество, надувательство, очень часто употребляется при упоминании дистанционных мошенничеств.

На платформах Google Play и App Store, которые принадлежат крупнейшим мировым компаниям Apple, Samsung, Sony, Huawei, Xiaomi и др. существуют пользовательские приложения для решения самых разных задач.

Из них, подавляющее большинство составляют развлекательные онлайн-игры на всевозможные тематики, затем приложения для «ускорения» своего устройства, антивирусные программы для предотвращения вторжения вредоносного «софта» – понятие, используемое в сфере информационных технологий, обозначающее программное обеспечение, фото-, видеоредакторы и др.

Мы с точностью можем утверждать, что любой пользователь мобильного устройства, оснащенного Интернетом и широким спектром функций, обращался к вышеперечисленным приложениям и замечал, что есть категория платных приложений, которые заранее предполагают внесение денежных средств за скачивание, и бесплатных.

Проводя исследование, мы осуществили опрос, который подтвердил факт наличия высокотехнологичных мобильных устройств у граждан, имеющих операционные системы IOS или Android (в большинстве случаев). Также было доказано, что практически каждый обращался к платформам App Store или Google Play для скачивания приложений. Из 20 опрошенных, где возрастная категория варьировалась от 10 до 65 лет, у всех были смартфоны и флагманы крупнейших мировых брендов: Apple, Samsung, Xiaomi, Huawei. 19 из 20 граждан обращались к Интернет-платформам для скачивания самых разных приложений.

Опираясь на элементарную психологию человека, мошенники придумали другой формат, они изобрели fleeceware-приложения, которые дают более широкие возможности пользователям, оформив месячную, недельную или годовую подписку на полную версию скаченной программы.

Работает это следующим образом. Видя платное приложение, скорее всего, мы обойдем его стороной. Но, когда скачивание той или иной программы не предполагает никаких финансовых затрат, пользователь заинтересован в ее полноценной работе, находит подходящие функции в ней, непосредственно просмотрев рекламный видеоролик.

Скачав приложение, владелец мобильного устройства замечает, что обещанные атрибуты приложения неполноценны, на часть из них наложена блокировка, некоторых вовсе нет. В свою очередь модераторы такого софта предоставляют возможность использовать весь функционал, но уже за определенную плату. Плата за «приоритетные» функции такой программы или онлайн-игры небольшая, примерно 30$ в неделю, 50$ в месяц или же 100$ в год.

Тем самым модераторы завлекают пользователей подобных приложений оформлять годовую подписку, ведь это очень «выгодное» предложение.

Почему люди соглашаются на предложение о покупке подписки на определенный срок? Все очевидно, мошенники урезают количество функций в бесплатной версии и предлагают «пробный период», который уже предполагает соглашение на приобретение подписки. Данный период варьируется от 3 до 7 дней, за это время пользователь имеет возможность протестировать все «закрытые» функции приложения.

Соответственно, в силу бурных рабочих дней, домашних хлопот человек забывает о наличии

оформленной подписки, которая подразумевает пробный период в N-м количестве дней, и тот промежуток времени, который пользователь выбрал для дальнейшей работы в данном приложении (неделя, месяц, год). Денежные средства начинают списываться по истечении пробного периода без уведомления пользователя, спасти его могут только оповещения онлайн-банка или SMS-уведомления от оператора связи, которые зачастую отключены.

Лица, занимающиеся мошенническими действиями, заблаговременно создают некачественные, низкопробные приложения, обещая клиенту широкий спектр функций, который он может получить за оформление соглашения по пользованию, имея пробный период. Человек, понимая, что при наличии пробного периода денежных средств он лишиться не может, заранее зная о расторжении соглашения по использованию полной версии по истечению пробного периода, оформляет подписку без всякой предосторожности, а по причине плохого качества представленных функций он удаляет программу с мобильного устройства, забывая про нее.

Пользователи мобильных телефонов или планшетов не осведомлены о том, что подписку нужно прекращать в самом приложении или в настройках своего устройства, в разделе «платежи», «подписки» и др. Соответственно, человек из-за своей нерасторопности теряет денежные средства месяцами, а порой даже годами при фактической неактивности.

Это юридическая лазейка для злоумышленников, за которую, по сути, невозможно привлечение к уголовной, административной или иной ответственности, ведь физическое лицо самостоятельно идет на заключение договора по представлению функционала внутри софта и не расторгает его путем отмены подписки, а лишь удаляет приложение.

Fleeceware-приложения – это пробел в законодательстве, где у людей «похищают денежные средства легальным способом».

Бывают же случаи, когда кибермошенники «злоупотребляют» незаконными действиями, помимо денежных средств, получаемых с подписок от граждан, они завладевают реквизитами банковских карт, через которые были оформлены такие подписки.

Чаще всего для обеспечения безопасности в сфере информационных технологий в части банковских переводов и электронных платежей, используют «сайты-посредники» (OnePay, Webpay, E-pay и др.) для осуществления транзакций. Они являются второстепенными при совершении платежа, нажимая на иконку «Оплатить», пользователь автоматически переходит на подобный сайт, где уже нужно вводить реквизиты банковской карты и код с SMS-сообщения для подтверждения покупки.

Зачастую, оформляя подписку внутри приложения, мы не сталкиваемся с автоматическим переходом на «сайт-посредник». Это происходит в трех основных случаях:

1) приложение принадлежит крупнейшей компании, где не нужны никакие гаранты по оформлению подобной сделки, само имя организации говорит за себя и гарантирует безопасность процедуры;

2) приложение новое, находится на стадии развития, и отсутствует достаточное количество активов, чтобы придерживаться безопасной процедуры по электронному внесению денежных средств;

3) приложением владеют кибермошенники, которые имеют умысел на получение ваших личных данных и реквизитов банковской карты для совершения хищения денежных средств и в иных целях.

Отметим, что Apple уходит от «сайтов-посредников» и оплат «лично в руки» создателям того или иного софта. Они тщательно проверяют каждую онлайн-игру, программу на факт содержания в них вредоносного программного обеспечения, а затем дают допуск автору на размещение своего приложения на платформе App Store, которая и выступает тем самым гарантом при осуществлении платежей, и все транзакции проходят через нее. Но все это не исключает факта существования и работы fleeceware-приложения.

Вадим Галеев в 2019 году на международном форуме International Cybersecurity Congress заявил: «Взлом IOS (Apple) на Darknet стоит порядка $ 2 млн, когда взломать любое мобильное устройство, имеющее операционную систему Android, стоит порядка $ 100. IOS гораздо безопаснее, компания Apple заботится о кибербезопасности своих пользователей» [2].

Сложно не согласиться, ведь «взломанных», «пиратских» приложений на Iphone практически не существует, а скачать программу на Iphone через сторонние сайты почти невозможно, ибо встроенное программное обеспечение, поддерживающее безопасность устройства, блокирует подобные процедуры. Если говорить о гаджетах, на которых установлена операционная система Android, то «пиратские» приложения встречаются даже на Google Play, о чем мы поговорим далее.

Вернемся к «сайтам-посредникам», пользователи мобильных устройств на операционной системе Android могут сталкиваться с ними внутри приложения, а также, как мы описали по пунктам выше, бывают платы и вне его, ибо Google Play не всегда поддерживает систему встроенных покупок и более лояльно относится к допуску на свою платформу игровых приложений и иных инструментов.

Минус операционной системы Android – возможность скачивания приложения не с официальных ресурсов, с потусторонних, вредоносных сайтов. Поэтому, возвращаясь к 3 пункту, понимаем, что посредством установки подозрительных приложений мы имеем риск передать в руки киберпреступников все свои личные данные и стать жертвой хищения денежных средств.

Соответственно, в рассмотренном случае не будет спора насчет незаконности содеянного и потребуется квалификация подобных мошеннических актов по статьям Особенной части Уголовного кодекса Российской Федерации, а оперативно-розыскным подразделениям следует применять специальные организационно-тактические меры с использованием техоборудования для раскрытия подобных преступлений.

Существует еще одна схема, когда модераторы приложений увеличивают плату за пользование подпиской или добавляют дополнительные пакеты функций, рассчитывая на невнимательность клиента.

Также стоит затронуть проблемные стороны онлайн-игр как одной из категорий интернет-приложений. В большинстве своем, играми на мобильном устройстве увлекаются лица в возрасте от 5 до 30 лет. Основная угроза исходит от Cheat-программ (cheat – в переводе с англ. «жульничество, обман»; используется для упрощения прохождения игры или для изменения игрового процесса, например: игроку предоставляются бесконечные виртуальные денежные средства или нескончаемое количество жизней). Эти программы по своей сути имеют вредоносное составляющее, так как изменяют игровые процессы, дав возможности игроку, которые нереальны по сюжету игры, увеличивая превосходство над другими (происходит внедрение вредоносного ПО, посредством которого игра взламывается).

Подобными вредоносными программами, как показывает практика, пользуются лица от 10 до 18 лет, где игроки до 14 лет вовсе не осознают, что, оформляя покупку «чит-программы» через банковскую карту своих родителей, они рискуют получить неблагоприятные последствия.

Так, за прошлый год количество скачиваний мошеннических вредоносных приложений, связанных с игрой Minecraft превысило 5 млн, что принесло колоссальный ущерб заинтересованным в этом лицам.

«Мошенническая схема рассчитана на тех, кто скачивает приложение, не обращая внимания на написанное мелким шрифтом. Именно поэтому жертвами злоумышленников рискуют стать дети, поскольку, скачивая дополнительный контент для Minecraft, они могут не прочитать или не понять условия, которые они принимают, устанавливая приложение. Мы призываем наших клиентов сохранять бдительность при загрузке любых приложений от неизвестных разработчиков и всегда внимательно изучать отзывы пользователей и соглашения об оплате перед тем, как оформить подписку», – отмечает Ондржей Дэвид, руководитель группы анализа вредоносных программ в Avast [2].

Таким образом, для недопущения мошеннических действий в области мобильных приложений рекомендуем соблюдать следующие меры:

– скачивать приложения с официальных сайтов;

– обращать внимание на отзывы к приложению, их количество и содержание, если преобладающее большинство негативные, то лучше воздержаться хотя бы от оформления подписки. Существуют и «накрученные» положительные оценки и отзывы, в основном это видно, когда скачивания приложений по количеству раз гораздо меньше, чем оценок. Также они зачастую слишком примитивные, порой одинаковые по смыслу или текстовки;

– не вводить реквизиты своей банковской карты внутри подозрительного приложения, делать все через «сайты-посредники» или же по встроенным покупкам на платформах App Store, Google Play;

– избегать взломанных, «пиратских» программ;

– писать жалобы и обращаться в службу техподдержки той или иной платформы для проверки подозрительного приложения;

– вести контроль за своими детьми в целях несовершения ими самостоятельных платежей в том или ином приложении.

Выполняя представленные требования, вы сохраните собственную безопасность на просторах Интернета и в сфере информационно-телекоммуникационных технологий, не допустив совершения мошеннических действий в отношении себя и своих близких.

Библиографический список

1. Надежин Н. Н. Предпринимательский риск в гражданских правоотношениях // Безопасность бизнеса. 2019. № 4. С. 17–21. URL: https://elibrary.ru/item.asp?id=38524008.

2. Международный конгресс по кибербезопасности. URL: https://icc.moscow/ru. (дата обращения: 10.12.2020).

3. Портал «Хакер». URL: https://xakep.ru/2020/11/12/minecraft-fleeceware/ (дата обращения: 17.11.2020).

4. Батоев В. Б. Оперативно-розыскное противодействие мошенническим действиям с использованием информационно-телекоммуникационных технологий // Расследование преступлений: проблемы и пути их решения. 2018. № 4 (22). С. 144–149. URL: https://elibrary.ru/item.asp?id=37371038.

5. Богданов А. В., Ильинский И. И., Хазов Е. Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С. 15–20. DOI: http://doi.org/10.24411/2687-0185-2020-10004.

6. Гужаева В. А., Прокофьева Е. В., Прокофьева О. Ю. Преступность в сети Интернет: криминологические характеристики / В. А. Гужаева, Е. В. Прокофьева, О. Ю. Прокофьева // Вестник экономической безопасности. 2019. № 4. С. 111–114. DOI: http://doi.org/10.24411/2414-3995-2019-10225.

7. Любан В. Г., Молянов А. Ю., Хазов Е. Н. Распространенные способы мошенничеств в сфере информационно-телекоммуникационных технологий // Вестник Московского университета МВД России. 2019. № 1. С. 190–194.

DOI: http://doi.org/10.24411/2073-0454-2019-10047.

8. Озеров И. Н. Организация раскрытия и расследования преступлений: учебное пособие. Белгород: БелЮИ МВД РФ. 2007. 176 с.

9. Озеров И. Н., Черкасова Е. А., Капустина И. Ю. Допустимость доказательств в уголовном судопроизводстве: сущность и значение // Проблемы правоохранительной деятельности. 2013. № 2. С. 67–70. URL: https://elibrary.ru/item.asp?id=20929540.

10. Смольянинов Е. С., Воронин М. Ю. Проблемы реализации уголовной политики по противодействию преступлениям в сфере высоких технологий // Вестник РГГУ. Серия «Экономика. Управление. Право». 2018. № 3 (13). С. 134–141. DOI: http://doi.org/10.28995/2073-6304-2018-3-134-141.

References

1. Nadezhin N. N. *Predprinimatel'skii risk v grazhdanskikh pravootnosheniyakh* [Entrepreneurial risk in civil relationships]. *Bezopasnost' biznesa* [Business Security], 2019, no. 4, pp. 17–21. Available at: https://elibrary.ru/item.asp?id=38524008 [in Russian].

2. *Mezhdunarodnyi kongress po kiberbezopasnosti* [International Cybersecurity Congress]. Available at: https://icc.moscow/ru (accessed 10.12.2020) [in Russian].

3. *Portal «Khaker»* [Portal «Hacker»]. Available at: https://xakep.ru/2020/11/12/minecraft-fleeceware (accessed 17.11.2020) [in Russian].

4. Batoev V. B. *Operativno-rozysknoe protivodeistvie moshennicheskim deistviyam s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologii* [Operative-investigative counteraction to fraudulent actions using information and telecommunication technologies]. *Rassledovanie prestuplenii: problemy i puti ikh resheniya* [Investigation of Crimes: Problems and Solution], 2018, no. 4 (22), pp. 144–149. Available at: https://elibrary.ru/item.asp?id=37371038 [in Russian].

5. Bogdanov A. V., Il'inskiy I. I., Khazov E. N. *Kiberprestupnost' i distantsionnoe moshennichestvo kak odna iz ugroz sovremennomu obshchestvu* [Cybercrime and remote fraud as one of the threats to modern society]. *Kriminologicheskii zhurnal*, 2020, no. 1, pp. 15–20. DOI: http://doi.org/10.24411/2687-0185-2020-10004 [in Russian].

6. Gauzhaeva V. A., Prokof'eva E. V., Prokof'eva O. Yu. *Prestupnost' v seti Internet: kriminologicheskie kharakteristiki* [Crime on the Internet: criminological characteristics]. *Vestnik ekonomicheskoi bezopasnosti* [Vestnik of economic security], 2019, no. 4, pp. 111–114. DOI: http://doi.org/10.24411/2414-3995-2019-10225.

7. Lyuban V. G., Moljanov A. Yu., Khazov E. N. *Rasprostranennye sposoby moshennichestv v sfere informatsionno-telekommunikatsionnykh tekhnologii* [Disseminated ways of frauds in the field of information-telecommunication technologies]. *Vestnik Moskovskogo universiteta MVD Rossii* [Vestnik of Moscow University of the Ministry of Internal Affairs of Russia], 2019, no. 1, pp. 190–194. DOI: http://doi.org/10.24411/2073-0454-2019-10047 [in Russian].

8. Ozerov I. N. *Organizatsiya raskrytiya i rassledovaniya prestuplenii: uchebnoe posobie* [Organization of disclosure and investigation of crimes: textbook]. Belgorod: BelYuI MVD RF, 2007, 176 p. [in Russian].

9. Ozerov I. N., Cherkasova E. A., Kapustina I. Y. *Dopustimost' dokazatel'stv v ugolovnom sudoproizvodstve: sushchnost' i znachenie* [The admissibility of evidence in criminal proceedings: essence and significance]. *Problemy pravookhranitel'noi deyatel'nosti* [Problems of law-enforcement activity], 2013, no. 2, pp. 67–70. Available at: https://elibrary.ru/item.asp?id=20929540 [in Russian].

10. Smolyaninov E. S., Voronin M. Yu. *Problemy realizatsii ugolovnoi politiki po protivodeistviyu prestupleniyam v sfere vysokikh tekhnologii* [Problems of implementation of the criminal policy on combating high-tech offenses]. *Vestnik RGGU. Seriya «Ekonomika. Upravlenie. Pravo»* [RSUH/RGGU Bulletin. «Economics. Management. Law» *Series*], 2018, no. 3 (13), pp. 134–141. DOI: http://doi.org/10.28995/2073-6304-2018-3-134-141 [in Russian].