Автономная некоммерческая общеобразовательная организация "Физтех-лицей"
(АНОО «Физтех-лицей» им. П.Л. Капицы)

XX научно-практическая конференция

«Старт в инновации»

Личный ассистент по безопасности в сети

Выполнил:
Севрюков Никита 9И
Руководитель:
Мерзляков Алексей Владимирович

Московская область, г. Долгопрудный

2021 г.

Содержание

Есть немало людей, озабоченных безопасностью атомных станций
и не пристегивающихся в машине.
Джордж Карлин

Цель, задачи, объект исследования, актуальность проблемы

Цель моей работы является создание адаптированного личного помощника для обеспечения банковской безопасности при работе в сети интернет и по телефону для людей, плохо разбирающихся в интернет-технологиях. Использование такого доступного помощника позволит понизить степень обмана населения и повысит уровень безопасности при использовании банковских карт.

Объектом исследования является безопасность при работе в сети интернет и во время разговора по телефону.

Для достижения поставленной цели я провел анализ новых способов мошенничества и уловок с банковскими картами, проанализировал меры безопасности, которые рекомендуют банки РФ при работе с онлайн-банкингом, и на основе этого анализа создал Telegram-бот (обучающий ассистент), который постарался адаптировать под более уязвимые для информационных мошенников слои населения.

Задачи:

-выяснить, какие существуют типы мошенничества с банковскими картами и личными персональными данными, а также выявить вновь образовавшиеся, в связи с эпидемией COVID-19, способы отбора денег у населения;

- проанализировать виды мошенничества, ожидаемые в 2021 году с целью предупреждения мошеннических действий;

-сформировать представление о банковской безопасности при работе с персональными данными и банковскими картами;

-оценить влияние человеческого фактора на банковскую информационную безопасность, с учетом увеличения объема финансовых интернет транзакций вне личного контакта участников и в случае интернет торговли;

- проанализировать существующие решения проблемы;

-разработать обучающий помощник (Telegram-бот) в части банковской безопасности для предотвращения случаев обмана населения.

Актуальность изучения новых способов мошенничества и создание обучающего помощника, помогающего выработать у человека «привычку» не давать информацию по карте, особенно возрастает с началом действия режима самоизоляции, поскольку в этот период активизируются мошенники, которые используют введенные ограничения в своих целях, чтобы незаконно завладеть денежными средствами населения.

Способы хищения денег с банковских карт

Самым распространенным способом мошенничества является **социальная инженерия** — методы обмана и введения клиентов в заблуждение с целью кражи денежных средств. По данным ЦБ, в первом полугодии 2020 года на нее пришлось 83,8% случаев от общего числа атак [1]. Традиционно мошенники звонят банковским клиентам под видом «службы безопасности банка» или «службы финансового мониторинга» и сообщают о том, что по карте якобы совершена подозрительная операция. Под предлогом спасения денежных средств они заставляют клиента совершить ряд действий, чтобы украсть деньги с его счета. Контактную и персональную информацию о клиентах злоумышленники получают, покупая «слитые» базы в даркнете или находят их там же в свободном доступе. Также для убедительности они могут звонить с подменных номеров банков. Далее схема мошенничества развивается по нескольким сценариям.

Мошенники выманивают платежные данные карты (16-значный номер, имя владельца, срок действия и трехзначный код на обратной стороне, а также код из СМС от банка) либо обманом узнают данные для входа в личный кабинет.

Иногда мошенники в процессе звонка просят установить на телефон специальное приложение якобы для лучшей защиты — им оказывается программа удаленного доступа и управления, с помощью которой можно зайти в личный кабинет онлайн-банка жертвы и перевести оттуда деньги на свой счет.

Также во время звонка мошенники убеждают своих жертв снять деньги в банкомате и зачислить их на специальный счет для «спасения средств». Некоторые злоумышленники, «заботясь» о клиенте, заказывали своим жертвам такси до ближайшего банкомата.

В последнее время стали появляться более сложные схемы: к звонкам от «банковских работников» добавились звонки от «правоохранительных органов», которые «подтверждают», что кто-то пытается украсть деньги клиента, поэтому их надо спасти путем перевода на «безопасный» счет.

Во время пандемии COVID-19 и перехода многих процессов в онлайн-формат мошенники особенно активизировались в интернете. Злоумышленники обещают интернет-пользователям крупную сумму выплаты, но перед этим просят заплатить небольшую «комиссию» либо осуществить «закрепительный платеж» (такой тип мошенничества называют **скамом**). Самыми распространенными видами таких преступлений в 2020 году, по данным «Лаборатории Касперского», стали рассылка сообщений на тему различных социальных выплат, в том числе связанных с коронавирусной инфекцией. Мошенники создают поддельные сайты банков, чтобы узнать данные для входа в личный кабинет. С января по ноябрь компания обнаружила почти 86 тыс. скам-ресурсов [2]. Злоумышленники активно пользуются технологией подмены номера. Чаще всего они указывают телефоны финансовых организаций, государственных учреждений или юридических лиц.

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — это некий вид получения злоумышленником секретной информации, при котором правонарушитель, используя средства социальной инженерии, «разводит» клиента на открытие своих личных данных. Такими данными могут быть номер и код банковской карты, номер телефона, логин и пароль от какого-либо сервиса и т.д. В основном, такой вид «ловли» используют чтобы получить доступ к онлайн-банкингу или кошельку жертвы в той или иной платежной системе и вывести средства на посторонние счета. На электронный адрес атакуемого приходит фишинг-письмо, которое, в первую очередь, влияет на эмоции получателя. Например, это может быть оповещение о большом выигрыше или же, наоборот, сообщение о взломе аккаунта с дальнейшим предложением перейти по фишинговой ссылке и ввести данные авторизации. Пользователь переходит на предоставленный ресурс и «отдает» свой

логин и пароль в руки мошенника, который, со своей стороны, достаточно быстро оперирует полученной информацией [3].

Вишинг — это одна из разновидностей фишинга, при котором также используются методы социальной инженерии, но уже с помощью телефонного звонка. На телефон поступает звонок от сотрудника банка, и оператор предупреждает, если прямо сейчас не будет предоставлена полная информация банковской карты ему по телефону, то карту заблокируют. Доверчивый пользователь, слыша подобную «угрозу» сразу же впадает в панику и может выдать все персональные данные вплоть до проверочного кода из SMS.

Также при вишинге может быть предложена выгодная покупка с огромной скидкой или озвучена информация о выигрыше в какой-либо акции.

Еще одним видом обмана посредством сервисов связи является **смишинг** (англ. smishing – sms+phishing). Данная преступная схема направлена на переход пользователем по вредоносной ссылке из SMS-сообщения. Смишинг-сообщение может иметь вид сообщения от известного банка, знакомой компании или быть просто оповещением о внезапном выигрыше в лотерею или в крупную акцию. В случае с SMS выявить подвох несколько сложнее, нежели при фишинге, т.к. сообщения небольшие и имеют меньше информации, помимо самой ссылки.

Скорее всего это будет предложение перейти по ссылке и ввести данные или же просто позвонить или отправить обратное сообщение, что понесет за собой некоторые затраты.

Недавно был придуман новый подвид фишинг-мошенничества – фарминг (англ. pharming), заключающийся в секретном перенаправлении пользователя на сторонние сайты. Особенность фарминга заключается в подмене настоящего сайта на мошеннический, позволяющий злоумышленнику завладеть конфиденциальными данными пользователя. Все это производится посредством использования кэша DNS на конечном устройстве пользователя или же на сетевом оборудовании провайдера. После подмены злоумышленнику остается только дождаться, когда клиент будет авторизоваться на определенном ресурсе и собрать все его данные. Вирус активирует свою деятельность только в момент перехода на интересующую страницу. Зачастую это касается онлайн-банкингов или иных платежных систем, через которые осуществляются денежные транзакции.

Чтобы защититься от фарминга нужно не только научиться узнавать жульнические письма, но и внимательно относиться к установке программного обеспечения.

Как уточнил глава Российской секции Международной полицейской ассоциации [4]:

- Ущерб от киберпреступности в России по итогам прошедшего года составил 69 млрд рублей. К концу 2021 года, вероятно, нас ограбят на 90 млрд рублей. То есть предполагается рост на 30%.

Мировой экономический кризис, вызванный пандемией коронавируса, вызвал волну новых видов мошенничеств и рост количества преступлений, совершаемых с использованием сети «Интернет». Одним из них является хищение средств граждан и организаций под видом сбора денег на благотворительные нужды (в помощь заболевшим коронавирусом и членам их семей, медицинским работникам и т.д.). Как правило, такие преступления совершаются посредством размещения призывов к оказанию помощи в мессенджерах и социальных сетях. Следующим видом является реализация товаров, якобы спасающих от заражения COVID-19, а также «вакцины» от этой инфекции. С начала января 2020 г. в сети «Интернет» по всему миру появились объявления о продаже средств от коронавируса. Основные новые способы мошенничества представлены в таблице ниже.

По данным банка Тинькофф из статьи Seldon News[5]:

Вернуть деньги, которые были украдены с помощью социальной инженерии, сложно, так как потерпевший добровольно подтверждает операции по своему счету и у банка есть основания отказать в возврате средств. Клиент может обратиться в банк с требованием заблокировать мошенническую операцию, но, как показывает практика, в подавляющем большинстве случаев в отсутствие документов, подтверждающих факт совершения мошеннических действий, банк, скорее всего, ответит отказом.

Человеческий фактор или проблемы с информационной безопасностью?

Цифровой мир прост, удобен и быстр. В 2020 году многие аспекты повседневной жизни серьезно изменились. Всеобщая «удаленка» и рекордная цифровизация большинства отраслей не могла изменить информационную безопасность. Банки всегда подвергались рискам, связанным с ошибками или мошенничеством, но в связи с пандемией COVID -19 перед банковской информационной безопасностью стоят особо сложные задачи, поскольку изощренность мошенников и возможности реализации обманных методов значительно расширились.

Социальная инженерия – это коммуникативное мошенничество, т.е. получение от жертвы в телефонном разговоре либо в процессе общения в различных чатах, соцсетях, электронных письмах и т. д. конфиденциальных данных (персональных, номеров и других параметров платежных карт, счетов, номеров и сканов документов и т. д). Затем на основании этих данных осуществляется попытка хищения активов потенциальной жертвы. Технологически банки уже предусматривают защиту, предполагающую участие клиента в процессе подтверждения операции (например, обязательная защита дистанционных карточных платежей 3D-Secure), либо эта защита требует ввода дополнительных кодов для подключения к Samsung Pay или Apple Pay, другим системам платежей со счета или карты. Поэтому вторым этапом мошенники стараются узнать коды или пароли, приходящие в сообщениях от банка.

Главный признак этих атак: убедить потенциальную жертву сообщить требуемые данные. Приемы злоумышленников опираются на три кита любого мошенничества: жадность, страх и, в ряде случаев, банальное невежество, когда клиенту либо обещают «на грош пятаков» или другие золотые горы, пугают его «вот сейчас все заблокируем», «сейчас или никогда», либо убедительно рассказывают какие-то фантастические истории. Люди так легко попадаются на удочку мошенников, потому что мошенники стараются максимально приблизить свое общение с жертвой к общению «клиент – банк». Фразы мошенников зачастую соответствуют стандартным скриптам банковских call-центров, а это уже располагает потенциальную жертву к диалогу. Это так называемая точка входа, через которую мошенники транслируют свои «сказки» для дальнейших махинаций с восприятием человека, подавляя тем самым критическое мышление объекта атаки.

И вот тут начинает срабатывать «человеческий фактор».

Как обычный человек за короткий промежуток времени попадает под влияние лица, совершенно ему неизвестного, принимая его за представителя банка, компании, государственного регулирующего органа, спецслужб и действует в полном соответствии с инструкциями злоумышленника? Мошенники добиваются нужной реакции от совершенно незнакомого человека и воруют активы без физического контакта с жертвой: путем убеждения при телефонном разговоре или в процессе переписки, обходя и различные методы дополнительной защиты.

Почему люди так легко попадаются на удочку мошенников, несмотря на постоянные напоминания банков о бдительности, различные сообщения в прессе и на телевидении?

Чаще всего жертвами мошенников становятся те, кто склонен верить в выдуманные истории о неизлечимых болезнях, потерянных документах и т. п., а также те, кто привык безоговорочно доверять официальным инстанциям – банкам, социальным отделам, службам безопасности. Люди пожилого возраста, социально незащищенные категории

населения, молодежь зачастую плохо воспринимают информацию, исходящую только от банков, ввиду ее сложности и больших объемов. В любой системе самым слабым звеном всегда является человек – не случайно именно на него методами социальной инженерии воздействуют мошенники. И исключить человеческий фактор из данного процесса полностью не представляется возможным, так как вне зависимости от внедренных технических мер подлинность транзакции в конечном итоге может подтвердить или опровергнуть только ее непосредственный создатель. И именно на него и направлена атака методами социальной инженерии. На мой взгляд, всех потребителей нельзя сделать специалистами и научить вычислять мошенников, но человеческий фактор необходимо минимизировать. В связи с тем, что полностью человеческий фактор исключить нельзя, банкам необходимо внедрять программы повышения осведомленности в области противодействия мошенничеству и в области информационной безопасности, с использование областных и федеральных каналов.

Анализ существующих решений проблемы

Что делают банки для обеспечения информационной безопасности?

Давайте разберем самые популярные способы, которыми пользуются наши банки, для защиты денег на банковских картах и счетах:

1. Наличие магнитной полосы – большинство современных пластиковых карт оснащены еще и чипом. Магнитной полосой практически уже никто не пользуется, но данная защита когда-то была актуальна и защищала информацию, хранящуюся на карте.
2. Чип – на данный момент является высокой степенью защиты и позволяет хранить информацию и реквизиты в зашифрованном виде.
3. CVC2 и CVV2 коды – данные коды обычно используются для проверки пользователя при покупке через интернет и на данное время без данной информации невозможно произвести покупку во многих интернет-магазинах.
4. 3D-Secure – данная технология также позволяет сохранить ваши деньги при оплате ли переводе средств через Интернет. И для завершения операции нужен специальный одноразовый код, который приходит к вам на мобильный телефон в виде СМС.
5. RFID на банковской карте – это технология бесконтактной оплаты или радиочастотные волны идентификации пользователя. С помощью данной технологии можно расплачиваться в магазине не вставляя карту в торговый терминал.

Однако злоумышленники могут с помощью мощного ридера прочитать и отсканировать информацию о карте и сделать перевод. RFID кражи не такие частые, но они набирают популярность и на западе все чаще у клиентов воруют реквизиты карты с помощью RFID-ридера.

Чаще всего злоумышленникам сообщают всю необходимую информацию сами люди, поскольку информация и все реквизиты для списания и перевода находятся на пластике: номер карты, имя, CVC2 и CVV2 код и срок действия. Зная всю эту информацию, можно сделать перевод средств.

3D Secure – это специализированный протокол защиты, который применяется пользователями банковских карт, чтобы платить за услуги через интернет. Благодаря технологии, банки и продавцы могут быть защищены от действий мошенников. При этом система не гарантирует, что средства владельца карты останутся в сохранности. Главный плюс защитной системы состоит в том, что вся вводимая человеком информация остается

только на сервере банка. В магазин, в котором пользователь покупал какую-то вещь, эти данные не попадают. Второе преимущество – это использование одноразового кода, высылаемого банком для подтверждения аутентификации. Однако именно этот плюс может превратиться в значительный минус. При помощи специализированных программ или банальных вирусов мошенники способны перехватить такие данные. Для этого достаточно однажды случайно поставить любое зараженное приложение на телефон и личный компьютер. Есть и второй недостаток – не каждый интернет-магазин желает подключать для себя 3D-Secure. Это не возбраняется и не преследуется по закону, так как система не является обязательной. Получается, что технологию 3D-Secure тоже можно обойти.

Какие технологии у нас не используются?

Очень простая технология, которая применяется на Западе уже много времени, а именно Индекс банковской карты. Индекс банковской карты – это почтовый индекс вашей прописки в момент оформления и регистрации карты в банке. Это дополнительный реквизит, который также используется при онлайн покупке.

Злоумышленник, который может своровать вашу карту, и зная все реквизиты, не сможет угадать ваш почтовый индекс. Конечно есть способы узнать и его, но это дополнительная защита, позволяет сохранить средства от злоумышленников.

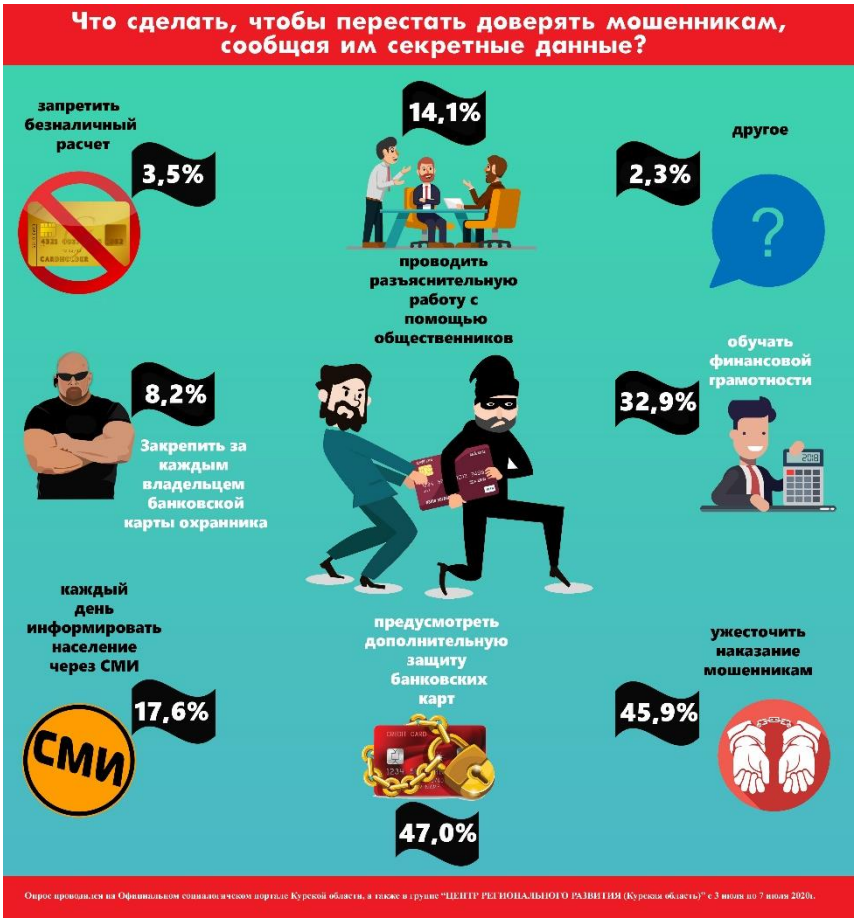
Также слабым звеном является использование нестойких паролей и низкое качество парольных комбинаций. На основании информации предоставленной поставщиком решений для менеджеров паролей NordPass из 275 699 516 паролей, которые оказались раскрыты при утечках данных в 2020 году, выяснилось, что только 44% из них были «уникальными». Наиболее популярными «слабыми» паролями остаются комбинации «123456», «123456789», «picture1», «пароль» и «12345678». Расшифровка каждого из них займет секунды. Статистика используемых российскими пользователями паролей значительно отличается от зарубежной. Российский список паролей на 50% состоит из расположенных рядом символов (1234567, qwerty и т.д.), тогда как западные пользователи больше склонны употреблять слова английского языка (password, love и т.д.).

Вероятность компрометации пароля из 4-х символов приблизительно равна 97%, а при условии использовании 9-символьного пароля этот показатель почти в 6 раз меньше и составляет примерно 17%. Эту проблему могло бы снизить внедрение несложных политик безопасности, не позволяющих применять пароли длиной менее 8-10 символов. Добавление правил о том, что пароль не должен содержать комбинации из соседствующих символов и символов одного регистра, позволяет существенно повысить уровень защиты доступа.

Крупнейшие банки и мобильные операторы из «большой четверки» нашли способ бороться с подмененными номерами, которые используют мошенники, чтобы звонить банковским клиентам под видом кредитной организации. Антифрод-платформы разработали Теле2, МТС, «МегаФон» и «ВымпелКом». Банки, среди которых Тинькофф Банк, ВТБ, Газпромбанк, Райффайзенбанк, Московский кредитный банк (МКБ) и МТС Банк, уже тестируют системы или собираются это делать [6].

По данным РБК газета от 05 февраля 2020 г. [7], банки и операторы связи объединили усилия для борьбы с новым видом мошенничества
Банки будут передавать операторам информацию о контактах с клиентами, которая поможет понять, кто им звонит: сотрудники банка или мошенники.
Операторы мобильной связи — «МегаФон», МТС и Tele2 — разработали специальное технологическое решение, которое позволяет банку в режиме реального времени получать информацию о любых подозрительных вызовах их клиентам.

По данным социологического опроса, который проводился на официальном социологическом портале Курской области [8], а также в группе «Центр регионального развития (Курская область)» были получены следующие результаты:



Из данных полученных при опросе видно, что большинство населения считает целесообразным обучение финансовой грамотности и ужесточение наказания за мошенничество.

В ЦБ РФ спрогнозировали самое популярное мошенничество в 2021 году. Летом или осенью стоит ожидать постепенного восстановления международных полетов, приостановленных из-за пандемии коронавируса. Вместе с оживлением турпотока могут активизироваться и мошенники. Как рассказал первый заместитель директора департамента информационной безопасности ЦБ Артем Сычев: «Всплеск мошенничества зависит от популярности того или иного направления и времени его открытия. Особое внимание аферистов всегда привлекают туристические направления, которые активно рекламируются. Мошенники, которые хотят заработать на туристах, действуют по одной и той же схеме, и разгадать ее несложно. Они играют на создании у потребителя ощущения привлекательности услуг по минимальной стоимости. Когда возникает ситуация с явно дешевыми билетами или с рейсами, которые на других сайтах не подтверждаются, то это один из показателей, что против вас работают мошенники», — предупредил Сычев, подчеркнув, что основная цель злоумышленников — завладеть данными платежных инструментов граждан [9].

Для размещения предупреждающей информации о действиях мошенников ЦБ рекомендует использовать способы, позволяющие достучаться не менее чем до 80% клиентов — физических лиц. Например, информировать клиентов в мобильных приложениях, на банковских сайтах, в соцсетях, в отделениях кредитных организаций и на экранах банкоматов при переводе или снятии наличных, а также организовать рассылки

СМС (не реже одного раза в квартал) и сообщать о рисках, когда клиенты звонят в call-центры. ЦБ также предлагает включить тему противодействия мошенничеству в наружную рекламу банков и в рекламные материалы на радио, телевидении и в СМИ [10].

На фоне постоянно выявляемых новых схем преступной деятельности в банкинге и платежной индустрии может быть эффективна работа на опережение, когда компетентные органы исследуют потенциальные угрозы и информируют банки о возможных новых рисках еще до того, как преступники начали использовать те или иные новые методы.

Личный обучающий ассистент по безопасности в сети

У банков, несомненно, есть технологические инструменты противодействия мошенничеству, но в отношении социальной инженерии они не особо эффективны из-за человеческого фактора – невозможно контролировать поведение и действия клиента, который сам сообщает злодеям всю информацию.

Изучив методы борьбы с мошенниками, имеющиеся на текущий момент, мне представляется целесообразным создание некой обучающей программы, в качестве которой я предлагаю Telegram-бот. Для людей, которые являются потенциальными жертвами, такая программа может быть настоящей «палочкой-выручалочкой». Личный ассистент способен помочь и научить как действовать в ситуациях, в которые мы попадаем в результате мошеннических действий. При этом я не ставлю задачей сделать из населения, пользующегося финансовыми услугами - специалистов. По моему мнению, необходимо сосредоточиться на устойчивом закреплении в мышлении пользователей - элементарных базовых принципов и простых навыков «цифровой гигиены» (на уровне привычки). Я считаю целесообразным, банкам при выдаче банковских карт и первой загрузке мобильных приложений проводить обучение при помощи таких программ, разработав их в соответствии со своими целями. Обучающие помощники воспринимаются проще и приносят больше пользы, чем просто слова, о том, что «не говорите ПИН-код».

У банков, несомненно, есть технологические инструменты противодействия мошенничеству, но в отношении социальной инженерии они не особо эффективны из-за человеческого фактора – невозможно контролировать поведение и действия клиента, который сам сообщает злодеям всю информацию.

СПИСОК ЛИТЕРАТУРЫ:

1. https://www.rbc.ru/finances/05/12/2020/ Чернышова Е. (20.12.2020 г.)
2. https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-proanalizirovala-naibolee-rasprostranyonnie-shemi-telefonnogo-i-onlain-moshennichestva-v-2020-godu (25.12.2020 г.)
3. https://rocit.ru/news/fraud-with-bank-cards (22.01.2021 г.)
4. https://newizv.ru/news/incident/15-02-2021/kibermoshenniki-za-god-ukrali-u-rossiyan-69-mlrd-rubley (21.02.2021 г.)
5. https://news.myseldon.com/ru/news/index/235685703 (24.02.2021 г.)
6. https://rg.ru/2021/02/14/kak-protivostoiat-kiberprestupnosti.html. Жданов Ю. (21.02.2021 г.).
7. https://www.rbc.ru/newspaper/2020/02/05 (24.02.2021)
8. http://соцпортал46.рф (24.02.2021 г.)
9. https://travel.rambler.ru/news/45856833-v-tsb-rf-sprognozirovali-samoe-populyarnoe-moshennichestvo-v-2021-godu/ (24.02.2021 г.)
10. https://www.rbc.ru/finances/24/02/2021/60366d769a79472e39a37fc1 (24.02.2021 г.)