УДК 004.056.5

Д.А. Саяков, ***daniyar.sayakov@yandex.ru***
Национальный исследовательский ядерный университет «МИФИ», г. Москва

АНАЛИЗ ВОЗМОЖНОСТИ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ БАНКОВСКИХ КАРТ ОТ АТАК В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Обосновывается актуальность в связи с фишинговыми атаками на пользователей. В 2022 году количество фишинговых атак заметно выросло. В связи с этим требуются новые подходы к обеспечению безопасности пользователей. В данной статье предлагается использование генератора случайных чисел для создания CVV — кодов, действующих во время сеанса оплаты.

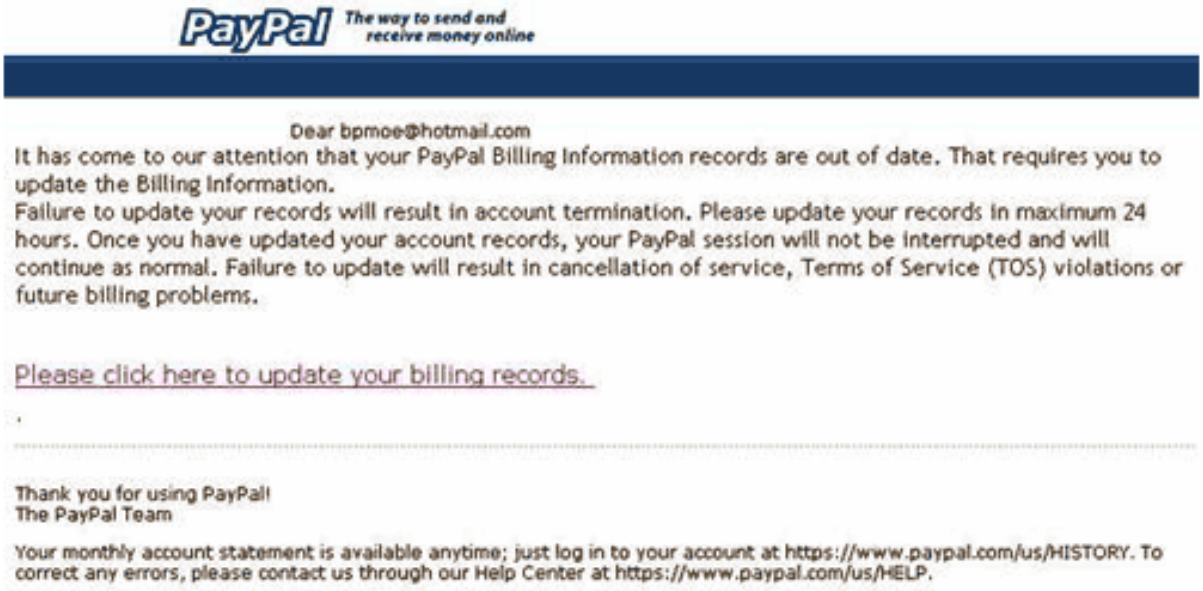
Ключевые слова: безопасность банковских карт, CVV— код, генерация случайных чисел, фишинг, веб-скимминг, социальная инженерия, атаки на банковские карты, данные пользователей

Введение

На сегодняшний день имеется множество атак на пользователей с целью кражи их личных данных, к таким атакам относятся: фишинг, социальная инженерия и веб-скимминг. Разберемся же с этими атаками и их особенностью.

Фишинг — это вид интернет-мошенничества, целью которого является завладение идентификационными данными как отдельных пользователей, так и всех потребителей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации. [1]

Фишинг представлен в виде пришедших на почту поддельных уведомлений от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут представляться различные. Это может быть утеря данных, поломка в системе и прочее, применяются методы социальной инженерии, как: «если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован», «если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль». [2]


PayPal The way to send and receive money online

Dear bpmoe@hotmail.com
It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information.
Failure to update your records will result in account termination. Please update your records in maximum 24 hours. Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

Please click here to update your billing records.

Thank you for using PayPal!
The PayPal Team

Your monthly account statement is available anytime; just log in to your account at https://www.paypal.com/us/HISTORY. To correct any errors, please contact us through our Help Center at https://www.paypal.com/us/HELP.

Рисунок 1– Фишинговое письмо с требованием пройти по ссылке и обновить свои данные в системе PayPal

Рисунок 2 – Фишинговое письмо с требованием пройти по ссылке и обновить свои данные в системе Federal Credit Union

Веб-скимминг – это термин, описывающий кражу учетных данных и конфиденциальной платежной информации у посетителей скомпрометированных веб-сайтов. [2]

Термин веб-скимминга произошел от слова «скимминг», который используется для описания физического взлома устройств кассовых терминалов и банкоматов путем помещения в них скрытого устройства для кражи информации о кредитной карте.

Рисунок 3 – Пример установки устройства для считывания данных карт на терминал

Рост числа атак с использованием веб-скимминга в Интернете в последние годы вызывает все больше страха у индустрии электронной коммерции. EAST подчеркивает, что большинство таких атак в последнее время были безуспешными — общие потери, связанные с такими инцидентами, составили всего около €136 000 евро. [2]

EUROPEAN PAYMENT TERMINAL CRIME STATISTICS - SUMMARY						
ATM Malware & Logical Attacks	2018	2019	2020	2021	2022	% +/- 21/22
Total reported Incidents	157	140	202	52	31	-40%
Total reported losses	€0.45m	€1.09m	€1.24m	€0.70m	€0.14m	-80%
Terminal Related Fraud Attacks	2018	2019	2020	2021	2022	% +/- 21/22
Total reported Incidents	13,511	18,217	6,523	5,969	10,141	+70%
Total reported losses	€247m	€249m	€218m	€198m	€200m	+1%
ATM Related Physical Attacks	2018	2019	2020	2021	2022	% +/- 21/22
Total reported Incidents	4,549	4,571	3,722	3,947	3,728	-6%
Total reported losses	€36m	€22m	€22m	€10m	€11m	+10%
Source: European Association for Secure Transactions (EAST)						

Рисунок 4 – Статистика, составленная EAST

Великий комбинатор Остап Бендер чтил Уголовный кодекс. Банальному грабежу он предпочитал психологические уловки, чтобы жертвы его обаяния добровольно отдавали ключи от квартир, где деньги лежат. Позже для таких махинаций придумали название – социальная инженерия.

Социальная инженерия – это метод получения конфиденциальной информации, не ограничивающийся и преступными действиями. В наше время социальная инженерия стала реальным инструментом, который используют компании для увеличения продаж, улучшения обслуживания, улучшения пользовательского опыта и многих других целей.

Одним из главных аспектов социальной инженерии является понимание психологических особенностей людей, что помогает специалисту максимально эффективно воздействовать на целевую аудиторию. Однако это не должно подразумевать манипуляцию, ведь главная цель заключается в создании взаимовыгодных контактов.

Социальная инженерия может быть применена к любой сфере, включая маркетинг, политику и социальную работу. Важно понимать, что наша миссия состоит в том, чтобы защищать интересы людей, а не нарушать их права. [3]

По статистике, в большинстве случаев люди теряют свои сбережения не потому, что их счета взламывают хакеры. Владельцы банковских карт чаще всего сами сообщают мошенникам их полные реквизиты, включая номер, срок действия, трехзначный CVV/CVC-код, а также пароли и коды из СМС, которые банки присылают для подтверждения операций.

«Если вы сами передали мошеннику секретные данные,
банк не обязан компенсировать похищенное.» [4]

Рассмотрение работы атаки фишинга

Фишинговые сайты, как правило, живут недолго (в среднем — 5 дней). Так как антифишинговые фильтры довольно быстро получают информацию о новых угрозах, фишерам приходится регистрировать все новые и новые сайты. Внешний же вид их остается неизменен — он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники.

Зайдя на поддельный сайт, пользователь вводит в соответствующие строки свой логин и пароль, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, в худшем — к электронному счету. Но не все фишеры сами обналичивают счета жертв. Дело в том, что обналичивание счетов сложно осуществить практически, к тому же человека, который занимается обналичиванием, легче засечь и привлечь мошенников к

ответственности. Поэтому, добыв персональные данные, некоторые фишеры продают их другим мошенникам, у которых, в свою очередь, есть отработанные схемы снятия денег со счетов. [6]

Заполучить данные пользователя – полбеды, большая же проблема — это обналичить и легализовать такой доход. Если от фишинг-атаки можно избежать наказания, то за легализацию уже нет. В развивающихся странах четко отработана система противодействия отмывания денег и финансирования терроризма. Практические многие финансовые институты могут потребовать от клиента справку с указанием источника его дохода. Также развивается система противодействия отмывания денег и финансирования терроризма в сфере оборота криптовалют. Поэтому, чтобы не рисковать, многие мошенники продают данные пользователей третьим лицам либо используют сложные схемы для придания законности дохода, а также применяют схемы с «денежными мулами».

Рассмотрение работы атаки веб-скимминга

British Airways, Ticketmaster, Discount Mugs, Adverline, FilaUK, Amerisleep и Umbro Brazil, Cleor, Macy's, Puma, Forbes, The Guardian, Garmin, Sweaty Betty, Снежная королева, Nyx Cosmetic, LaRoche Posay, Vichy, Redken, UrbanDecay, Kiehl’s, Pandora, Togas,Canon,Nespresso,Converse, Google Analytics, корзины Amazon S3 – это наиболее популярные взломанные интернет-магазины и сервисы за последнюю пару лет!

Скрипты, использующиеся в веб-скимминге, обычно используют такой метод, как обфускация. Это приведение с помощью различных программ или вручную исполняемого кода к виду, сохраняющему его функциональность, но затрудняющему анализ и понимание алгоритмов работы.

Помимо обфускации, злоумышленники могут использовать в своих скриптах метод «запутывания», то есть размещения пары строк вредоносного кода среди сотен строк обычного незараженного кода.

Большинство операций по внедрению скиммера выполняется двумя способами:

- ✓ Прямой взлом веб-сайта или пакета веб-сайтов путем подбора учетных данных администратора (так называемые **атаки методом перебора**) или с **использованием известных уязвимостей нулевого дня** для размещения вредоносных js-файлов на веб-сайте.
- ✓ Атака с помощью цепочки подстановки **путем взлома одного стороннего кода поставщика и изменения исходного сценария для доставки вредоносного фрагмента кода** с исходным кодом на все веб-сайты с использованием зараженного стороннего сценария.

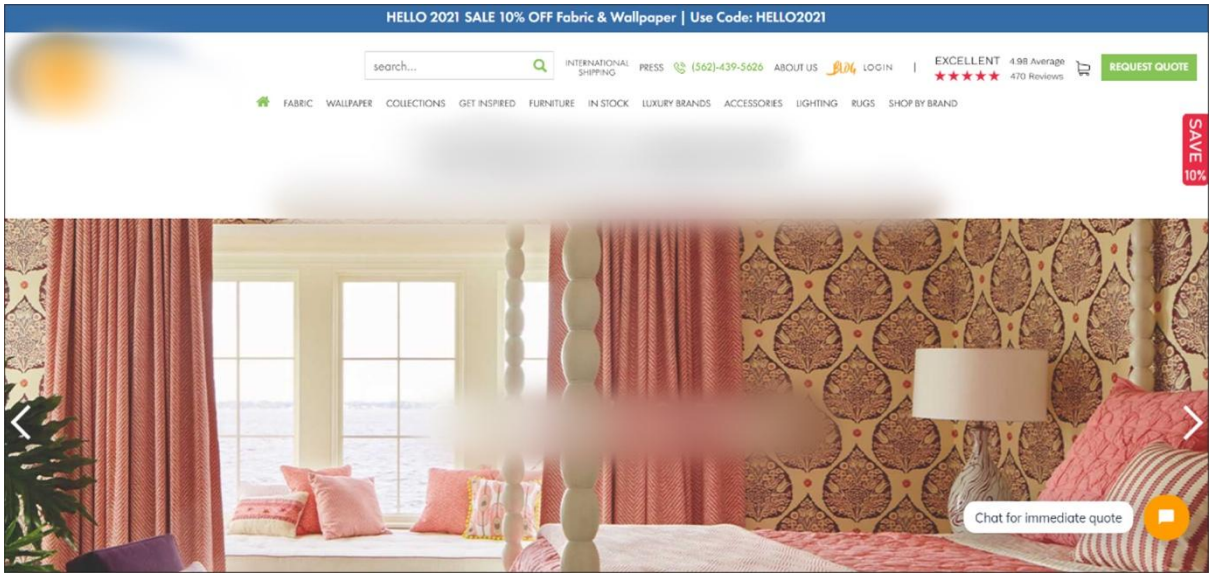


Рисунок 5 – Главная страница скомпрометированного сайта

Рисунок 6 – Вредоносный код

Рисунок 7 – Частичная деобфускация вредоносного кода

✓ Строки **«outerWidth», «innerWidth», «outerHeight», «Firebug»** – проверяют наличие открытых инструментов разработчика, чтобы специалистам по безопасности было труднее обнаружить вредоносную активность на сайте;

✓ **«find»** используется для поиска в формах определенных элементов, которые представляют из себя строки **«-card-number», «-card-cvc», «-card-expirity», «cc_owner»**;

✓ **«POST»** – это метод для отправки некоторого файла.

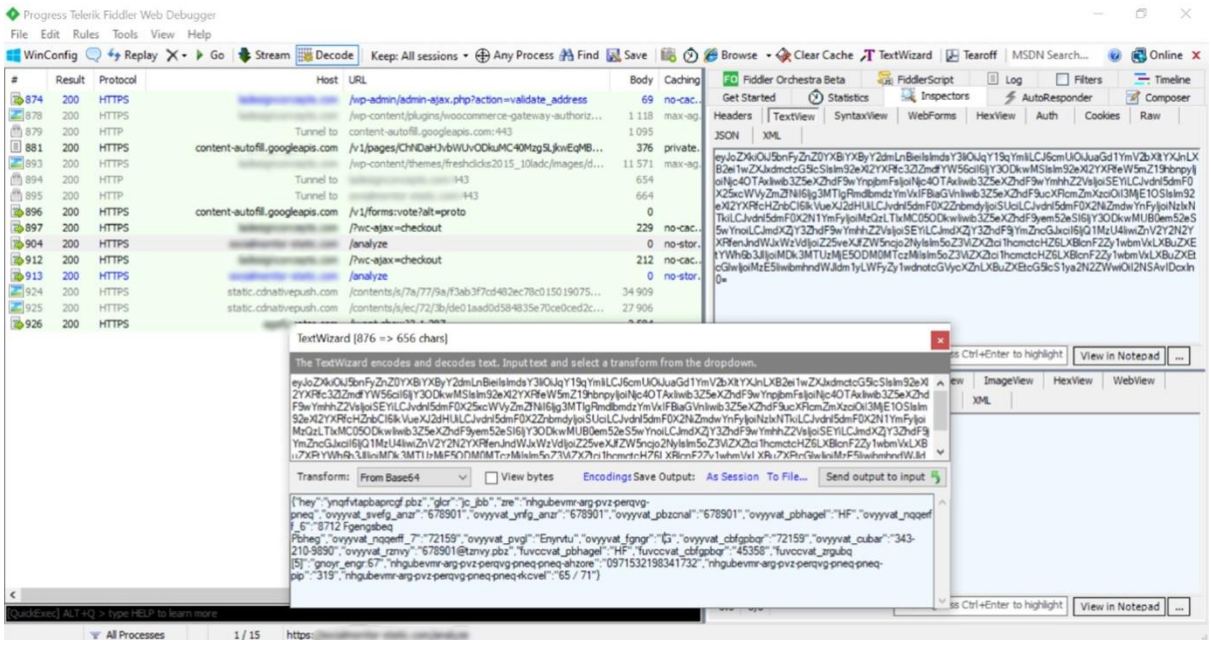


Рисунок 8 – Произведение оплаты с заведомо ложными данными для проверки их отправки на адрес злоумышленников

Рассмотрение работы и способов атаки социальной инженерии

Даже самые умные и осторожные люди иногда попадаются на крючок к махинаторам. Ниже представлены самые распространенные психологические уловки, которые используют мошенники:

1. Вызвать доверие. Мошенники представляются официальными организациями, чтобы усыпить бдительность людей и украсть их деньги. Они используют фишинговые сайты и информационные базы, а также социальные сети, чтобы узнать больше о своих жертвах. Достаточно небольшой информации, чтобы начать разговор и обмануть людей, поэтому нужно быть предельно осторожным и не доверять личные данные незнакомым людям.
2. Подделывание телефонного номера, документов и сайтов. Данный способ тесно связан с фишинговой атакой, спам-рассылкой и веб-скимингом. Подделываются оригинальные сайты, отправляется письмо о выигрыше в лотерее и другое.
3. Запугивание потерей денег. Обычно подобная атака требует подготовки, ведь полностью собранный и сконцентрированный человек вряд ли поверит телефонному звонку из банка. Данные атаки обычно проводятся посреди ночи, когда человек наиболее уязвим к сложным формулировкам, терминам, а также словам о том, что его счет подвергся атаке и нужны данные, чтобы обезопасить его.
4. Восстановление справедливости. Данный способ работает на людях, пострадавших от финансовых пирамид и афер. Мошенники предлагают "компенсации" для тех, кто потерял деньги на финансовых пирамидах, псевдолотереях и лохотронах. Чтобы получить эти "компенсации", людей убеждают указать полные реквизиты карты под предлогом оплаты "услуг юриста" или "комиссии за перевод денег", что может привести к повторному обману.
5. Использование дестабилизации в обществе. Мошенники активизируются во время катастроф и бедствий, следят за новостями и настроениями, адаптируются к ситуации и обманывают людей, выдавая себя за представителей Всемирной организации здравоохранения или авиакомпаний, рассылая СМС о несуществующих штрафах и предлагая проходить тест на коронавирус за деньги. Главная цель мошенничества – получить оплату "визита". [5]

Как работают современные платежные карты

Для оплаты товаров или услуг через Интернет платежная карточка не требуется. Достаточно знать всего-навсего три группы цифр (16+4+3):

— номер карты (16 цифр);

— срок действия: месяц и год (4 цифры);

— секретный CVV2- код (3 цифры на обратной стороне).

Каждая банковская карта имеет свой номер. Номер на карте может быть напечатан или эмбоссирован (выдавлен). В англоязычной документации он проходит как PAN (Primary Account Number). [9]

Номер карты регулируется двумя стандартами:

- международный стандарт ИСО/МЭК 7812-1 (выдает SWIFT);

- ГОСТ Р 50809-95 (выдает Ассоциация центров инжиниринга и автоматизации (Санкт-Петербург).

Действующий сейчас международный стандарт задает следующую структуру идентификационного номера пластиковой карты:

BBBBBBNNNNNNNNNNNNL,

где BBBBBB – идентификационный номер эмитента (БИН карты). Первая цифра всегда указывает на платежную систему пластиковой карты (например, 2 – Мир, 4 – Visa, 5 – Mastercard); [9]

NNNNNNNNNNNN – идентификационный номер пластиковой карты, выпущенной данным эмитентом, может быть длиной в 7, 10 или 13 цифр. В зашифрованном виде они обозначают тип карты (кредитная или дебетовая), регион, год выпуска и другую информацию, используемую при авторизации и прочих действиях в процессе совершения операций с карточкой; [9]

L – код Luhn (контрольная цифра, рассчитываемая из предыдущих цифр номера), необязательный и обычно присутствует только на картах с 13-значным номером. [7]

CVV-код – это трехзначный код для проверки подлинности вашей карты при оплате через Интернет и других видах операций. Код CVV можно найти на обратной стороне карты – это последние 3 цифры из семизначного числа рядом с местом для подписи, которые, как правило, визуально отделены от всего числа. [8]

Если карточка попадает в руки мошенников, переписать указанные 23 цифры можно за считанные секунды. Не говоря уже о ситуации физической утери, от которой не застрахован никто. На данный момент рекомендаций по безопасному обращению банковской карты имеется много: [9]

1. Проверять сайты. Рекомендуется не использовать и не оставлять данные карты на малоизвестных сайтах.
2. Всегда проверять службу, через которую проводится оплата, является ли это через стороннюю службу или через сам магазин.
3. Для защиты CVV-кода придумать свой способ шифрования. CVV2-код с карт Visa и Master стирать. Предварительно, конечно, где-то его продублировав. А для удобства оплаты счетов в Интернете написать ключ от кода фломастером (маркером) прямо на карточке. [9]

Рисунок 9 – Защищенная карточка

Восстановить CVV2- код легко. Составляем нехитрую формулу типа «плюс 4, 0, 4». Забиваем ее себе в память, а когда возникает надобность, быстренько прибавляем цифры формулы к цифрам ключа. [9]

Например:

1) Ключ, написанный фломастером, – 575.
2) Формула восстановления: +4, 0, 4.
3) Вычисляем:

5 + 4 = 9;
7 + 0 = 7;
5 + 4 =9.

Итого: CVV2- код – 979.

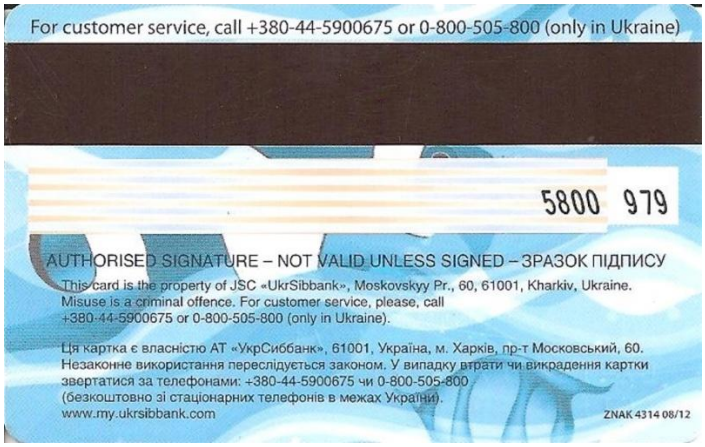


Рисунок 10 – Незащищенная карточка

Решение по защите банковских карт с помощью генератора случайных чисел

Как уже описано выше, для выполнения оплаты в онлайн–магазинах требуется указать номер карты, срок действия и CVV–код. Из трех групп цифр срок действия и номер карты не поддаются для случайной генерации, так как в них хранится информация о клиенте, типе карте и регионе. CVV– код можно заменить на возможность генерации случайным образом со сроком жизни для текущего сеанса. Данное решение позволит повысить безопасность и защиту от фишинговых атак, так как пользователь будет получать уведомление в виде поступающих к нему CVV– кодов для какой–либо транзакции.

Заключение

В результате проведенного анализа можно сделать вывод о том, что использование генератора случайных чисел может быть эффективным способом повышения безопасности пользователей банковских карт от атак в интернет–пространстве.

Литература

1. Что такое «фишинг» – . – URL: https://encyclopedia.kaspersky.ru/knowledge/what–is–phishing/ (дата обращения: 17.05.2023). Текст: электронный.
2. Спам и фишинг, что такое спам– . – URL: http://kk.convdocs.org/docs/index–39918.html (дата обращения: 09.06.2023)
3. Европейские банки теряют сотни миллионов евро из–за взлома банкоматов. – .– URL: https://www.securitylab.ru/news/537852.php (дата обращения: 17.05.2023). Текст: электронный.
4. Социальная инженерия. – . – URL:https://www.reg.ru/blog/chto–takoe–sotsialnaya–inzheneriya/ (дата обращения: 17.05.2023). Текст: электронный.

5. Социальная инженерия: почему люди сами отдают мошенникам деньги. – . – URL: https://fincult.info/article/sotsialnaya–inzheneriya–pochemu–lyudi–sami–otdayut–moshennikam–dengi/ (дата обращения: 17.05.2023). Текст: электронный.
6. Фишинг – .– URL: http://stud24.ru/information/fishing/134361–394246–page1.html. (дата обращения: 09.06.2023)
7. Номер банковской карты. – . – URL:https://www.banki.ru/wikibank/nomer_bankovskoy_kartyi/ (дата обращения: 17.05.2023). Текст: электронный.
8. Правила безопасного поведения в Интернете. – . – URL:http://bru.by/news/post/25162#:~:text=CVV%2Dкод%20–%20это%20трехзначный%20код,визуально%20отделены%20от%20всего%20числа. (дата обращения: 17.05.2023). Текст: электронный.
9. Безопасная платежная карта своими руками. – . – URL: https://habr.com/ru/articles/220025/#:~:text=Достаточно%20знать%20всего%2Dнавсего%20три,3%20цифры%20на%20обратной%20стороне). (дата обращения: 17.05.2023). Текст: электронный.