В настоящее время робототехника используется практически во всех областях промышленности, космоса, медицины др. Возможно, в ближайшем будущем роботы упростят нашу жизнь, сделают ее проще и легче. Робототехника совершенствуется с каждым годом, а это значит, что языки программирования для создания кодов для этих роботов также обновляются.

1. Алексеевский, П.И. Робототехническая реализация модельной практико-ориентированной задачи об оптимальной беспилотной транспортировке грузов / П.И. Алексеевский, О.В. Аксенова, В.Ю. Бодряков // Информатика и образование. ИНФО. - 2018. - № 8. - С. 51-60.
2. Бешенков, С. А. Использование визуального программирования и виртуальной среды при изучении элементов робототехники на уроках технологии и информатики / С.А. Бешенков, М.И. Шутикова, В.Б. Лабутин // Информатика и образование. ИНФО. - 2018. - № 5. - С. 20-22.
3. Иванов, А. А. Основы робототехники : учеб. пособие для студентов вузов... / А.А. Иванов. - М. : Форум, 2012. - 222 с. : ил., схем., табл. - (Высшее образование). - Библиогр.: с. 220. - Сер. указ. на обороте тит. л. - ISBN 978-5-91134- 575-4.
4. Шутикова, М.И. Использование робототехнического оборудования на платформе Arduino при организации проектной деятельности обучающихся / М.И. Шутикова, В.И. Филиппов // Информатика и образование. ИНФО. - 2017. - № 6. - С. 31-34.

Гочияева М.Д., Джуккаева З.А.
Безопасность онлайн-покупок

*Северо-Кавказская государственная академия
(Россия, Черкесск)*

doi: 10.18411/trnio-12-2021-73

Аннотация

Электронные платежи стали неотъемлемой частью современной жизни. Очевидно, что это наиболее перспективный вид расчетов с точки зрения новых бизнес-возможностей, а также удобства и простоты для пользователя. Системы электронных платежей можно разделить на: системы онлайн-банкинга; системы моментальных платежей; электронные платежные системы.

Ключевые слова: безопасность, онлайн-покупки, электронные платежи, закон, защита, Интернет.

Abstract

Electronic payments have become an integral part of modern life. Obviously, this is the most promising type of calculations in terms of new business opportunities, as well as convenience and simplicity for the user. Electronic payment systems can be divided into: online banking systems; instant payment systems; electronic payment systems.

Keywords: security, online shopping, electronic payments, law, protection, Internet.

Развитие современных технологий и глобального Интернета привело к резкому увеличению количества безналичных платежей и онлайн-платежей за покупки. Это выгодно, потому что вам не нужно тратить время и силы в дороге, вы можете изучить продукт и купить его в один клик. Пандемия коронавируса дала дальнейшее развитие системе безналичных расчетов, в связи, с чем проблема безопасности онлайн-покупок стала очень актуальной.

Несмотря на преимущества, у покупок в Интернете есть и недостатки. Во-первых, вас могут обмануть мошенники. Во-вторых, реальный продукт может быть намного хуже, чем его виртуальное световое изображение. Целью исследования является разработка рекомендаций по безопасности при совершении покупок в Интернете.

Безопасность онлайн-транзакций интересует не только держателей карт, но и банки, рынки, интернет-магазины и платежные системы, которые разрабатывают новые, более совершенные и дорогие средства защиты онлайн-платежей и защиты от мошенничества. Все участники сделки рискуют своими деньгами, а бизнес, банки, системы и рынки также рискуют своей репутацией.

Как же происходит процесс платежа?

В каждом процессе оплаты участвуют несколько сторон. Одна сторона - это лицо, выполняющее операцию. Другая сторона - это интернет-магазин или торговая площадка, предлагающая товары или услуги. Среди них банк-эмитент и банк-эквайер. Первый - это тот, кто дал вам карту с деньгами на вашем счету. Второй - это банк, который выполняет эту финансовую операцию. В некоторых случаях один и тот же банк может играть роль эмитента и эквайера. Не менее важными участниками операции являются международные платежные системы и провайдеры услуг, осуществляющие операцию.

Сделав покупку в интернет-магазине и нажав кнопку «Оплатить», вы перейдете на страницу формы оплаты и заполните необходимую информацию. Кроме того, платежная система (поставщик услуг) передаст все ваши данные банку-эквайеру, который обслуживает этот интернет-магазин. Банк-эквайер передаст информацию банку-эмитенту, который выпустил и выпустил вам карту. Он проверяет информацию о вас, о карте, наличие на ней денежных средств, иногда спрашивает разрешение у Покупателя по технологии 3-D Secure. Затем он разрешает (или не разрешает) выполнить операцию, передает данные в платежную систему, платежная система отправляет их в магазин, и покупатель получает уведомление о том, что операция завершена.

Каждый, кто участвует в операции в Интернете, несет ответственность за безопасность операции. Ответственные банки, интернет-магазины и платежные системы постоянно совершенствуются и придумывают новые способы защиты себя и своих клиентов от потенциальных угроз. На сегодняшний день существует ряд протоколов и правил, которые вы, как прямой участник любой транзакции, должны знать и помнить каждый раз, когда совершаете онлайн-платеж.

SSL - это безопасный уровень Socked. Позволяет безопасно передавать зашифрованную информацию от пользователя на сервер. Стандарты PCI DSS (стандарт безопасности данных индустрии платежных карт). Эти стандарты информационной безопасности, разработанные международными платежными системами, защищают данные банковских карт. 3-D безопасная технология. Важным шагом защиты является проверка личности держателя карты в реальном времени, включая банк-эмитент. Обычно такая проверка осуществляется с помощью SMS. Системы защиты от мошенничества. Дословно переводится как «антифрод». Это системы платформ, которые оценивают финансовые транзакции в Интернете и могут обнаруживать проблемы. Развитие минимальных навыков для обеспечения онлайн-безопасности - основа современной финансовой грамотности, которую должны соблюдать все пользователи Интернета.

Правила, которым нужно следовать:

Подключите интернет-банк и СМС-оповещение. Это позволит вам отслеживать операции в режиме реального времени.

Не используйте подозрительные сайты. Адрес защищенного сайта должен начинаться с <https://>. Также рядом с адресной строкой должна быть иконка в виде закрытого замка. Это показывает, что вы имеете дело с ответственным продавцом и ваши данные будут передаваться в зашифрованном виде.

Используйте 3-D Secure — авторизацию платежа по СМС, при этом обращайте внимание на назначение платежа, которое приходит в СМС от банка вместе с проверочным кодом.

Ищите на сайте надпись Verified by Visa или MasterCard Securecode — в зависимости от того, какой платежной системой вы пользуетесь. Сайты, которые размещают у себя такие

логотипы, будут соответствовать стандартам PCI DSS и/или использовать технологию 3-D Secure.

Не сообщайте данные своей банковской карты другим людям: ни банковским служащим, ни работникам интернет-магазинов.

Если интернет-магазин вызывает у вас подозрение, используйте платежные системы Apple Pay, PayPal или другие. В этом случае вам не нужно будет делиться данными своей банковской карты.

Совершайте покупки с устройств, на которых установлена антивирусная защита. Каждое новое обновление содержит встроенные антивирусы, поэтому необходимо вовремя обновлять все свои гаджеты.

Не пользуйтесь для оплаты зарплатной или кредитной картой. Откройте для этих целей вторую карту в том же банке. Особенно это касается тех платёжных систем и интернет-магазинов, к которым вы хотите привязать карту.

Приобретайте товары популярных брендов на зарекомендовавших себя интернет-площадках, лучше всего, уже знакомых вам. Если сайт для вас нов, вас должно насторожить любое обстоятельство из списка ниже: слишком низкая цена; отсутствие в интернете отзывов о сайте; отсутствие на сайте адреса компании, которой принадлежит сайт, и других контактных данных; переадресация на подозрительные сайты, не имеющие отношения к магазину.

Если вы столкнулись с чем-то из перечисленного, то вы с вероятнее всего перед вами мошенники, цель которых — реквизиты вашей банковской карты. Если остались сомнения, проверьте сайт на <https://www.whois.com/whois/>. Если поймёте, что сайт существует всего несколько дней, — это точно мошенники. Избегайте предоплаты. По возможности оплачивайте товар курьеру при получении и только после того, как проверите покупку. Это обезопасит вас, особенно при покупке товаров с частных страниц в соц. сетях (Instagram, VK, WhatsApp)

Что делать, если деньги все-таки украли?

Заблокируйте карту. Если с карты списали деньги без вашего ведома, позвоните в банк и заблокируйте карту. Номер горячей линии банка указан на оборотной стороне карты.

Опротестуйте операцию. В тот же день, когда вы получили уведомление о незаконной операции обратитесь в отделение банка. Запросите выписку по счету и напишите заявление о несогласии с операцией, которую не совершали.

Обратитесь в полицию. Расследованием преступлений в интернете занимается Бюро специальных технических мероприятий (БСТМ) МВД России. Подайте заявление в территориальное учреждение БСТМ. Можно просто написать заявление в отделение полиции по месту жительства. Чем быстрее вы это сделаете, тем больше шансов найти преступников и вернуть деньги.

При совершении покупок в Интернете шансы встретить преступников в Интернете во много раз выше, чем в оффлайновом мире. Мошенники не упускают возможности и всеми возможными способами пытаются обманым путем привлечь деньги - они делают фейковые сайты, похожие на известные интернет-магазины, используют социальную инженерию, спам в электронной почте, SMS и всевозможные другие методы. Узнав обо всех правилах оплаты и методах безопасности при совершении покупок в Интернете, вы сможете максимально обезопасить себя в области онлайн-платежей.

1. Безопасность в платежах: [Электронный ресурс]. – Электрон. дан. – URL: <https://1prime.ru/business/20200816/831913299.html/> (Дата посещения 17.11.21).
2. Безопасные покупки в интернете [Электронный ресурс]. – Электрон. дан. – URL: <https://fincult.info/article/bezopasnye-pokupki-v-internete/> (Дата посещения 18.11.21).
3. Безопасность в интернете: как защитить свои платежи – Электрон. дан. – URL: <https://www.forbes.ru/finansy-i-investicii/346943-bezopasnost-v-internete-kak-zashchitit-svoi-platezhi> (Дата посещения 18.11.21).