References

1. Social'noe polozhenie i uroven' zhizni naseleniya Respubliki Belarus': statistich. sb. / Nacional'nyj statisticheskij komitet Respubliki Belarus'. – Minsk, 2023. – 220 s.

УДК 138

ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

Д. А. Свибович
Научный руководитель: Т. В. Филиппова

Брестский государственный технический университет
Республика Беларусь, г. Брест, ул. Московская, 267
elb00318@g.bstu.by

В статье рассмотрены основные проблемы безопасности, с которыми сталкиваются как клиенты, так и поставщики в приложениях электронной коммерции. Без электронной коммерции отрасль не сможет эффективно работать на рынке. В связи с этим возникает необходимость проведения систематического обзора вопросов безопасности в индустрии электронной коммерции и выяснения, как различные платформы решают эти проблемы.

Ключевые слова: аутентификация, электронная коммерция, безопасность, угрозы, конфиденциальность.

MAJOR SECURITY THREATS IN E-COMMERCE

D. A. Svibovich
Scientific adviser: T. V. Filippova

Brest State Technical University
Republic of Belarus, Brest, Moskovskaya str., 267
elb00318@g.bstu.by

The article discusses the main security problems faced by both customers and suppliers in e-commerce applications. Without e-commerce, the industry will not be able to work effectively in the market. In this regard, there is a need to conduct a systematic review of security issues in the e-commerce industry and find out how different platforms solve these problems.

Keywords: authentication, e-commerce, security, threats, confidentiality.

Безопасность в электронной коммерции становится все более актуальной по мере перехода от традиционных покупок и транзакций к бизнесу, основанному только на кликах. Электронная коммерция быстро развивается на мировом рынке, и все же она сопряжена с риском того, что транзакции будут скомпрометированы, что в конечном итоге приведет к испорченной репутации и финансовым потерям. Основными проблемами безопасности, с которыми сталкиваются как потребители, так и поставщики, являются безопасность транзакций, конфиденциальность, системная безопасность и киберпреступность.

Действующее законодательство Республики Беларусь определяет электронную торговлю как оптовую, розничную торговлю, характеризующуюся заказом, покупкой, продажей

товаров с использованием информационных систем и сетей, и относит ее к одной из форм осуществления торговли наряду с комиссионной, посылочной, выездной и др. [1].

Электронная коммерция связывает клиентов и поставщиков через Интернет, когда они ведут деловые переговоры. Недавние исследования показали, что основным фактором, препятствующим успеху и дальнейшему росту электронной коммерции, является отсутствие безопасности.

Безопасность электронной коммерции – это защита активов электронной коммерции от несанкционированного доступа, использования, изменения или уничтожения. В электронной коммерции недостатки проявляются двумя различными способами. Одним из них является риск потери клиентом финансовой информации, а поставщиками услуг — убытков от мониторинга и плохой рекламы из-за этого [1].

Тремя существенными точками уязвимости в транзакции являются клиентская сторона, серверная сторона и канал связи.

При изучении литературы, были выявлены **пять основных аспектов безопасности**, которые необходимо сохранить, чтобы обеспечить желаемую безопасность платформ электронной коммерции [2].

1. *Конфиденциальность* рассматривается как фундаментальное право любого потребителя. Это способность контролировать условия, на которых осуществляется поиск и использование различной информации [1]. Любое копирование или чтение неавторизованной стороной приводит к потере конфиденциальности.

2. *Аутентификация* помогает определить, является ли тот или иной человек тем, за кого себя выдает. Для того, чтобы гарантировать подлинность предоставленных данных, транзакций и документов, необходимо обеспечить информационную безопасность. В электронной коммерции такое обеспечение дает возможность подтвердить то, что обе стороны являются теми, за кого себя выдают. Этот фактор также гарантирует, что конкретный пользователь является единственным, кому разрешено входить в учетную запись интернет-банкинга [2].

3. *Целостность* можно определить как надежность информации. Более конкретно это точность, согласованность и надежность информационного содержания, процессов и систем. Это означает гарантию, что данные, к которым осуществляется доступ или которые считываются, не были подделаны, изменены или повреждены с момента последнего авторизованного доступа.

4. *Отказ от ответственности* означает намерение человека не выполнить свои обязательства по контракту. Одна сторона транзакции не может отрицать получение транзакции, равно как и другая сторона не может отрицать ее отправку. Применительно к электронной коммерции — это отказ от продажи или покупки [3].

5. *Доступность* — это цель любой информационной системы сделать информацию доступной в любое время, когда она необходима. В данном исследовании это означает, что вычислительные системы, используемые для хранения и обработки информации, средства контроля безопасности и используемые каналы связи, используемые для доступа к ней, должны функционировать надлежащим образом.

Платформы электронной коммерции представляют собой системы высокой готовности. Их цель – постоянная доступность, предотвращение всех возможных перебоев в обслуживании.

Проблемы безопасности электронной коммерции

Четыре основные проблемы безопасности, с которыми сталкивается индустрия электронной коммерции, базируются на основе трех критериев: электронная платформа, владелец и ее пользователи.

1. Безопасность транзакций в электронной коммерции.

Безопасность транзакций в электронной коммерции относится к защищенной от мошенничества передаче денежной ценности от плательщика получателю платежа с помощью электронных средств, которые связывают обмениваемые данные с некоторой экономической ценностью реального мира.

Защита информации, доступной на платежной карте, является основной заботой с точки зрения клиента: следует поддерживать прозрачность транзакции; финансовая информация

не должна храниться после завершения транзакции и не должна раскрываться или продаваться третьим лицам [4].

Тремя основными игроками, которых необходимо учитывать при онлайн-транзакции, являются онлайн-продавец, страница электронной коммерции и восприятие плательщика. Характер обмена требует конфиденциальности и успех операции зависит от безопасности передачи данных. С точки зрения электронного бизнеса, для того, чтобы выжить, отношения между клиентом и поставщиком должны строиться на доверии. Не должно быть никакого беспокойства на протяжении всего процесса принятия решений и даже за его пределами.

2. Конфиденциальность в электронной коммерции.

Во-первых, клиенты обеспокоены повторным использованием их данных в несвязанных целях без их согласия, таких как передача третьим лицам. Во-вторых, потребители обеспокоены несанкционированным доступом к персональным данным из-за нарушений безопасности. Конфиденциальность должна рассматриваться с социальной, организационной, технической и экономической точек зрения, поскольку это законное право клиента [2].

3. Системная безопасность в электронной коммерции.

Безопасность системы зависит в основном от поставщика, и это касается сервера, доступности и безопасности базы данных. Чтобы платформа электронной коммерции служила своей цели, информация должна быть доступна все время. Злоумышленники, атакующие базы данных, изменяют системные ресурсы или получают доступ к системной информации без авторизации, либо сообщая логины или пароли, либо используя автоматический терминал, и изменяют, модифицируют или раскрывают информацию о продукте, информацию о потребителях и частную информацию, которая может нанести непоправимый ущерб бизнесу [1].

4. Киберпреступность в сфере электронной коммерции.

Киберпреступность в электронной коммерции — это, в основном, компьютерное преступление с целью умышленного причинения финансовых потерь, утечки данных либо прямого или косвенного риска репутации. Хакеры взламывают веб-серверы электронной коммерции, чтобы получить доступ к архивам транзакционной и личной информации, когда потребитель совершает онлайн-покупку [5].

На протяжении последних лет в Республике Беларусь наблюдается значительное увеличение количества регистрируемых преступлений. В 2015 году количество таких преступлений составляло 2440, а с начала 2023 года было совершено уже более 23 тысяч преступлений. За хищение с использованием компьютерной техники либо введение в компьютерную систему ложной информации грозит лишение свободы на срок до 3 лет. Если преступления совершены повторно или в группе – до 5 лет. Статья 349 УК Республики Беларусь предусматривает наказание в виде штрафа или ареста. Более серьезная ответственность (лишение свободы на срок до 2 лет) наступает, если несанкционированный доступ к информации был совершен из корыстной или другой личной заинтересованности.

Таким образом, безопасность транзакций электронной коммерции имеет решающее значение для постоянного успеха, а также для роста электронной коммерции. Это исследование выявило понимание того, что единой структуры, способной удовлетворить эти потребности в целом, пока нет. Исследование проливает свет на необходимость создания четкой системы безопасности для преодоления темной стороны электронной коммерции.

Список использованных источников:

1. О торговле [Электронный ресурс] : Закон Респ. Беларусь, 28 июля 2003 г., № 231-З // Эталон–Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2012

2. Агапов, А. В. Обработка и обеспечение безопасности электронных данных / А. В. Агапов, Т. В. Алексеева, А. В. Васильев. – М. : Синергия, 2012.

3. Старовойтова, Т. Ф. Электронный бизнес и коммерция / Т. Ф. Старовойтова. – М. : ТетраСистемс, 2009.

4. Исаев, Г. Н. Информационные системы в экономике / Г. Н. Исаев. – М. : Омега-Л, 2012.

5. Ахромов, Я. В. Системы электронной коммерции / Я. В. Ахромов. – М. : Оникс, 2018.
6. Абдеева. З. Р. Проблемы безопасности электронной коммерции в сети Интернет / З. Р. Абдеева // Проблемы современной экономики. – 2012.

References

1. O torgovle [Elektronnyj resurs] : Zakon Resp. Belarus', 28 iyulya 2003 g., № 231-Z // Etalon–Belarus' / Nac. centr pravovoj inform. Resp. Belarus'. – Minsk, 2012
2. Agapov, A. V. Obrabotka i obespechenie bezopasnosti elektronnyh dannyh / A. V. Agapov, T. V. Alekseeva, A. V. Vasil'ev. – M. : Sinergiya, 2012.
3. Starovojtova, T. F. Elektronnyj biznes i kommerciya / T. F. Starovojtova. – M. : Tetra-Sistems, 2009.
4. Isaev, G. N. Informacionnye sistemy v ekonomike / G. N. Isaev. – M. : Omega-L, 2012.
5. Ahromov, Ya. V. Sistemy elektronnoj kommercii / Ya. V. Ahromov. – M. : Oniks, 2018.
6. Abdeeva. Z. R. Problemy bezopasnosti elektronnoj kommercii v seti Internet / Z. R. Abdeeva // Problemy sovremennoj ekonomiki. – 2012.

УДК 338.12.017

МЕРОПРИЯТИЯ КОМПАНИИ DE BEERS ПО ФОРМИРОВАНИЮ ПРЕДПОЧТЕНИЙ ПОТРЕБИТЕЛЯ (НА ПРИМЕРЕ РЫНКА БРИЛЛИАНТОВ)[1]

П. С. Селиванова, В. В. Демьянкова, Д. А. Гринько
Научный руководитель: А. С. Сверлов, к. э. н., доцент

Белорусский государственный экономический университет
Республика Беларусь, г. Минск, Партизанский просп., 26
selivanovaps9679007@gmail.com

Эта научная статья исследует маркетинговую деятельность компании DE BEERS и ее влияние на формирование предпочтений потребителей на рынке бриллиантов. Она подчеркивает успешные маркетинговые стратегии DE BEERS, изменение традиций и повышение спроса на обручальные кольца с бриллиантами. Полученные результаты имеют значимость для маркетологов и предпринимателей, позволяя лучше понять потребительское поведение и стимулировать развитие рынка ювелирных изделий.

Ключевые слова: De Beers, «J. Walter Thompson», «N. W. Ayer & Son», алмазы, бриллианты.

ACTIVITIES OF DE BEERS COMPANY TO SHAPE CONSUMER PREFERENCES (BY THE EXAMPLE OF THE POLISHED DIAMOND MARKET)[2]

P. S. Selivanova, V. V. Demyankova, D. A. Grinko
Supervisor: A. S. Sverlov, Ph.D. in Economics, associate professor

Belarus State Economic University
The Republic of Belarus, Minsk, Partyzanski av., 26
selivanovaps9679007@gmail.com

[1] Подготовлены в рамках исследований, выполняемых в СНИЛ «Поиск» УО БГЭУ
[2]Prepared within the framework of the research carried out in SRL "Search" at BSEU