Международная электронная торговля: особенности регулирования розничного сектора

DOI: 10.24411/2072-8042-2020-10107

Елена Николаевна ТИМЧЕНКО,
Санкт-Петербургский государственный университет
(191123, Санкт-Петербург, ул. Чайковского, 62, ауд. 402)
кафедра мировой экономики - аспирант,
e-mail: timchenko-elena-2015@mail.ru

УДК 004.738.5 : 339
ББК 65.39
Т-419

Аннотация

В статье освещены особенности, оказывающие влияние на безопасность розничного сектора электронной коммерции, рассматриваются различные уровни регулирования данной сферы. Проведён обзор стандартов и нормативных актов по вопросам безопасности в информационной среде. Выделена проблема распределения ответственности в случае реализации киберугроз, исследуется поведение потребителей и их реакция на вызовы цифровизации. Показана необходимость комплексного подхода и международного сотрудничества для обеспечения безопасности глобального розничного рынка электронной коммерции и защиты интересов участников сделок.

Ключевые слова: безопасность, глобальный рынок, информационные технологии, электронная коммерция, электронная торговля, цифровизация.

International E-Commerce: Features of Retail Regulation

Elena Nikolaevna TIMCHENKO,
St Petersburg University (191123, St. Petersburg, Chaikovskogo st., 62, room 402)
Department of World Economy - Postgraduate Student,
e-mail: timchenko-elena-2015@mail.ru

Abstract

The article examines special aspects that affect the safety of the e-commerce sector, considers the various levels of regulation in this area. The standards and regulations on security in the IT environment are reviewed. The issue of responsibility distribution in the case of real cyber attacks is highlighted, consumer behaviour and their response to the challenges of digitalization are investigated. The necessity of an integrated approach and international cooperation to ensure the safety of the global e-commerce market and protect the interests of participants in transactions is substantiated.

Keywords: safety, global market, IT technology, e-commerce, e-trade, digitalization.

Вопросы безопасности в экономике активно стали рассматриваться с 30-х годов XX века[1]. Это было обусловлено необходимостью выхода из серьёзных кризисов, таких как Великая депрессия в США, Вторая мировая война и других[2]. Современные технологии предоставляют новые возможности для обеспечения безопасности в экономической сфере, но возникают и новые риски, не характерные для предыдущих этапов развития мирового хозяйства. При этом цифровая среда становится всё более популярной для проведения частных коммерческих сделок во всём мире.

Розничный рынок электронной коммерции включает следующие варианты проведения сделок: «Бизнес для Потребителя» (*B2C*), «Потребитель для Бизнеса» (*C2B*) и «Потребитель для Потребителя» (*C2C*). Существуют смешанные формы взаимодействия, например, «Бизнес для Бизнеса и для Потребителя» (*B2B2C*), когда фирма, работая через электронные каналы связи, предоставляет услуги и товары, как коммерческим компаниям, так и частным лицам. Также присутствует взаимодействие структур в категориях отношений «Государство для Потребителя» (*G2C*) и «Потребитель для Государства» (*C2G*). Они не часто имеют целью получение прибыли и представлены всевозможными электронными площадками сотрудничества правительства и граждан, но также требуют обеспечения высокого уровня безопасности для всех участников. Отдельного внимания заслуживают сделки «Машина для Машины» (*M2M*). Это специфический сценарий проведения транзакций, когда их инициаторами выступают так называемые «умные» устройства, самостоятельно связывающиеся друг с другом через Интернет для выполнения различных задач. Так как нередко они представляют интересы и оперируют данными частных лиц, этот тип взаимодействия также следует учитывать при рассмотрении вопросов безопасности пользователей.

Основная особенность розничного сектора электронной коммерции в том, что обычно физические лица не обладают профессиональными знаниями, чтобы самостоятельно в должной мере обеспечить защиту данных и как следствие — личную безопасность и сохранность денежных средств в глобальной цифровой среде. Оформляя заказ через удалённые каналы связи порой сложно убедиться в надёжности продавца, подлинности сайта, невозможно оценить качество и соответствие заявленным характеристикам товара до его получения. Стоит отметить, что в секторе *C2C* взаимодействие между покупателем и продавцом часто неофициально и не имеет документального подтверждения. При возникновении спорных ситуаций трудно доказать сам факт проведения сделки. Проблемы могут возникать и на этапе доставки материальных товаров, заказанных онлайн, например, если посылка повреждена при транспортировке или вовсе украдена. В отличие от коммерческих грузов такие отправления не всегда застрахованы, что создаёт трудности для возмещения ущерба.

Зарубежные учёные, со ссылкой на различные исследования, утверждают, что доверие является одной из важнейших предпосылок для успешной торговли[3]. Для поддержания благоприятных условий развития отрасли актуальной является задача глобального масштаба по обеспечению честной и максимально безопасной среды для всех участников рынка электронной коммерции. Решение этой задачи требует действий на всех уровнях регулирования.

РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УЧАСТНИКОВ РОЗНИЧНОГО РЫНКА ЭЛЕКТРОННОЙ КОММЕРЦИИ

Создание механизмов противодействия киберугрозам, а также разработка и реализация правил и законодательных актов, регулирующих отношения субъектов электронной коммерции и обеспечивающих безопасность электронных сделок, может осуществляться на различных уровнях.

Международными организациями формируются специализированные подразделения, исследующие процессы развития электронной коммерции, издаются рекомендательные документы. Например, в Европейском союзе (ЕС) с 25 мая 2018 года действует «Общий регламент о защите персональных данных в ЕС»[4]. В соответствии этим регламентом пользователи информационных услуг могут отслеживать, что происходит с их персональной информацией, и при желании удалять её. В результате такого нововведения многим компаниям пришлось изменить политику работы с данными пользователей в ЕС, а некоторые компании даже ушли с рынка ЕС. ЮНКТАД также освещает проблемы защиты прав потребителей в онлайн-среде[5]. Ежегодно рассчитывается «*B2C* индекс электронной коммерции», оценивающий возможности ведения деятельности в сегменте «*B2C*»[6]. Важный показатель при его расчёте — наличие защищённых серверов на 1 млн населения. Чем выше его значение, тем более благоприятными считаются условия для электронных сделок в стране.

На этапе становления систем управления информационной безопасностью (СУИБ) базовым и получившим широкое признание был Британский стандарт BS 7799, предназначавшийся для определения норм безопасности коммерческой деятельности, что с середины 90-х годов XX века стало особенно востребовано. Впоследствии были выпущены международные стандарты ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 и другие[7]. В них собраны лучшие мировые практики по управлению информационной безопасностью, предоставляются рекомендации для идентификации рисков, ведению документооборота, распределению ответственности, проведению аудита и т.д.

В России в этой области действуют государственные стандарты, а также проводится работа по их гармонизации с международными нормами. Примерами служат ГОСТ Р 53110-2008 «Система обеспечения информационной безопасности сети связи общего пользования. Общие положения», ГОСТ Р ИСО/МЭК ТО 15446-2008

«Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» и другие[8]. Различные аспекты защиты информации прописаны в Федеральном законе «Об информации, информационных технологиях и о защите информации»[9], в обновлённой в 2016 году «Доктрине информационной безопасности в РФ»[10] и других нормативных документах.

Многие страны проявляют заинтересованность в поиске союзников в вопросах обеспечения кибербезопасности. В 2012 году США и Австралия подписали документ о совместной работе в этой сфере[11]. В мае 2015 года Россия и КНР заключили соглашение по обеспечению международной информационной безопасности[12]. В 2020 году внесён проект соглашения между РФ и Узбекистаном о сотрудничестве в области обеспечения международной информационной безопасности[13], и это лишь некоторые примеры. Но нередко более открытому и продуктивному международному диалогу препятствует непродуманная либо агрессивная политика отдельных государств, что порождает формирование изолированных сегментов на глобальном рынке электронной коммерции, где часто концентрируются источники киберугроз.

Высокий уровень информационной защиты не менее важен и для коммерческих компаний. Международными платёжными системами разработаны собственные требования к информационной безопасности «Payment Card Industry Data Security Standard»[14] , контролирующие, чтобы каждый субъект, который хранит либо обрабатывает данные платёжных карт, делал это надёжным способом. Кроме того представители бизнеса вносят предложения о сотрудничестве с госорганами и международными организациями. В 2018 году под эгидой Всемирного экономического форума (ВЭФ) было подписано соглашение о создании Центра кибербезопасности, объединяющего представителей бизнеса и власти для обмена передовым опытом и совместной деятельности в области защиты данных[15].

Итак, власти большинства стран, международные организации, бизнес–структуры осознают значимость информационной безопасности для процессов развития мирового хозяйства в целом и розничного рынка электронной коммерции в частности. При этом важно учитывать ограниченные возможности частных пользователей по обеспечению собственной безопасности в цифровой среде. В отдельных случаях потребители могут самостоятельно застраховать некоторые виды рисков, присутствующие на рынке электронной коммерции. Но, как отмечают зарубежные авторы, в ряде государств, в частности в странах *Five Eyes* (Австралия, Канада, Новая Зеландия, Великобритания и США) и КНР, существует тенденция возлагать большую долю ответственности за обеспечение личной безопасности в информационной среде на конечных потребителей[16]. Изучение вопроса, справедлив ли такой подход, и как влияют киберугрозы на поведение пользователей, представляет интерес для исследователей.

БЕЗОПАСНОСТЬ И ПОВЕДЕНИЕ ПОТРЕБИТЕЛЕЙ НА РОЗНИЧНОМ РЫНКЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

При наличии различных мер защиты потребителей злоумышленники находят всё новые варианты преступных схем. Во многих случаях проблемой является несоблюдение пользователями элементарных правил: отсутствие антивирусных программ на электронных устройствах, создание простых паролей, открывающих доступ к важной информации, передача персональных банковских данных третьим лицам и прочее. Согласно проведённому в ЕС в 2017 году опросу Евробарометр, 87% респондентов считают киберпреступность угрозой безопасности ЕС, многие обеспокоены тем, что сами стали жертвами киберпреступлений: 69% обнаружили вредоносные программы на своих устройствах; 66% столкнулись с мошенничеством в сфере онлайн–банкинга и банковских карт. Для повышения безопасности пользователи предпринимают различные меры: 62% опрошенных поменяли пароли, 45% установили антивирусное программное обеспечение, при этом 12% сократили свои онлайн-покупки, а 10% вовсе отказалось от онлайн-банкинга[17].

Кроме того частные пользователи могут стать жертвами недобросовестной конкуренции. Сбор данных приобрёл тотальных характер, многие компании предоставляют разнообразные бесплатные сервисы, чтобы получить как можно больше информации о клиентах. Но как отмечает американский исследователь Э. Паризер: «Если Вы получаете нечто бесплатно, помните: Вы – не клиент. Вы – товар»[18]. Чем подробнее информация о каждом потребителе, тем эффективнее можно выстраивать бизнес. Всесторонний анализ данных грозит навязчивой рекламой, а в худшем случае эти данные могут стать инструментом манипуляции выбором пользователей либо вовсе попасть к злоумышленникам.

В 2019 году автором данной статьи был проведён опрос о поведении потребителей в условиях глобального распространения цифровых технологий. Название опроса «Информационная безопасность участников розничного рынка электронной коммерции». В нём приняли участие 225 респондентов различных возрастных групп и сфер деятельности. Было предложено ответить на пять вопросов с закрытыми вариантами ответов.

Таблица 1

Содержание опроса «Информационная безопасность участников розничного рынка электронной коммерции»

Укажите, пожалуйста, Ваш возраст	до 20 лет
	20-30 лет
	30-40 лет
	40-50 лет
	от 50 лет

Сталкивались ли Вы лично за предыдущий год со случаями мошенничества в Интернете либо по телефону?	да
	нет
Получали ли Вы персонализированные рекламные сообщения, основанные на Ваших предыдущих покупках и интернет–запросах?	да
	нет
Насколько важное значение Вы придаёте конфиденциальности личных данных?	спокойно оставляю в открытых источниках информацию о себе (паспортные данные, номера банковских карт, номер телефона, дату рождения, e–mail, домашний адрес и т.д.)
	ограничиваю доступ только к банковской информации, паспортным данным и другим наиболее важным документам
	стараюсь минимизировать распространение личных данных (не размещаю информацию в социальных сетях, никогда не заполняю анкеты для оформления карт лояльности в онлайн– и офлайн–магазинах, пользуюсь преимущественно наличными деньгами, отказываюсь от сбора биометрических данных и т.д.)
Станете ли Вы внимательнее относиться к обеспечению сохранности персональных данных?	нет, считаю, что в век цифровых технологий мир становится более открытым, и не имеет смысла скрывать информацию о себе
	задумаюсь над процессами трансформации экономики и общества, но вряд ли поменяю привычки
	да, рост информационных угроз обязывает относиться к персональным данным всё более внимательно

Источник: Составлено автором

По результатам опроса были получены следующие данные:

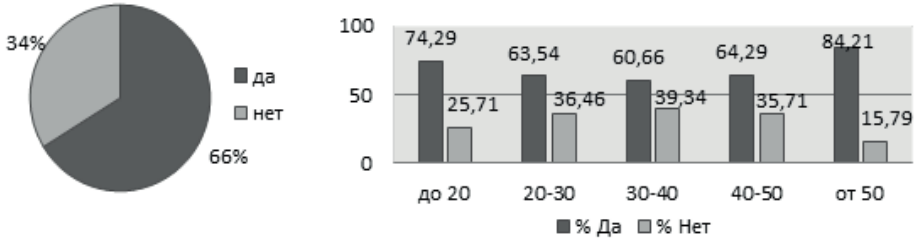

Рис. 1. Ответы на вопрос: «Сталкивались ли Вы лично за предыдущий год со случаями мошенничества в Интернете либо по телефону?» – общее распределение и распределение с учётом возраста, %

Источник: Составлено автором

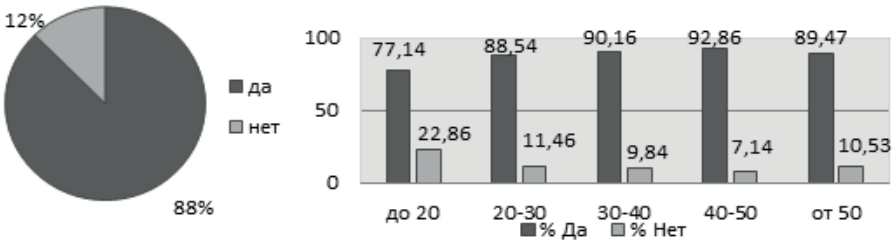

Рис. 2. Ответы на вопрос: «Получали ли Вы персонализированные рекламные сообщения, основанные на Ваших предыдущих покупках и интернет-запросах?» – общее распределение и распределение с учётом возраста, %

Источник: Составлено автором

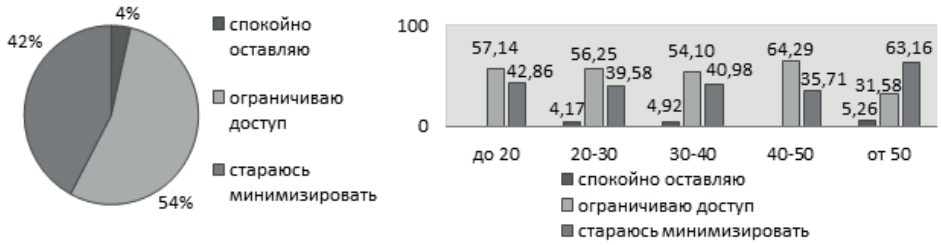

Рис. 3. Ответы на вопрос: «Насколько важное значение Вы придаёте конфиденциальности личных данных?» – общее распределение и распределение с учётом возраста, %

Источник: Составлено автором

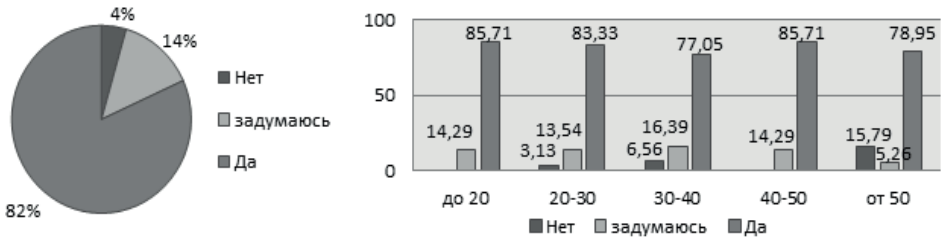

Рис. 4. Ответы на вопрос: «Станете ли Вы внимательнее относиться к обеспечению сохранности персональных данных?» – общее распределение и распределение с учётом возраста, %.

Источник: Составлено автором

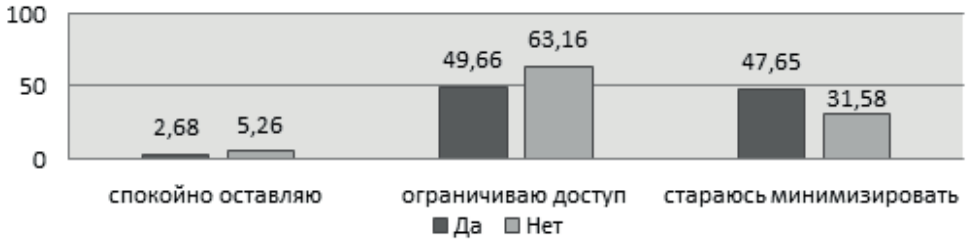

Рис. 5. Ответы на вопрос «Насколько важное значение Вы придаёте конфиденциальности личных данных?» в зависимости от того, сталкивался (да) либо не сталкивался (нет) респондент со случаями мошенничества в Интернете либо по телефону, %

Источник: Составлено автором

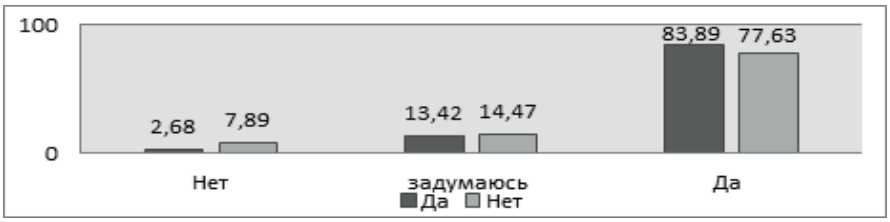

Рис.6. Ответы на вопрос «Станете ли Вы внимательнее относиться к обеспечению сохранности персональных данных?» в зависимости от того, сталкивался (да) либо не сталкивался (нет) респондент со случаями мошенничества в Интернете либо по телефону, %

Источник: Составлено автором

По результатам опроса выяснилось, что 66% процентов респондентов-участников розничного рынка электронной коммерции за предыдущий год сталкивались с тем или иным видом мошенничества. Это сопоставимо с данными Евробарометр, приведёнными ранее, согласно которым в Евросоюзе в 2017 году 66% опрошенных европейцев столкнулись с мошенничеством в сфере онлайн-банкинга и банковских карт. Следовательно, несмотря на развитие систем безопасности, масштабы угроз остаются на высоком уровне. Если рассмотреть результаты по группам, то видим, что чаще всего подвергаются рискам мошенничества пользователи старше 50 лет – 84% опрошенных. Это может быть связано с тем, что злоумышленники обычно рассчитывают на то, что люди старшего поколения имеют определённый уровень накоплений, более доверчивы и менее информированы о правилах информационной безопасности. На втором месте пользователи в возрасте до 20 лет – 74%, что по нашему мнению связанно с высокой активностью данной группы в цифровой среде – чем чаще человек использует цифровые сервисы, тем выше вероятность, что он столкнётся с деятельностью киберпреступников.

Персонализированная реклама знакома 88% опрошенных. При этом наименее охвачены такой рекламой респонденты в возрасте до 20 лет. Можно предположить, что это обусловлено меньшей финансовой самостоятельностью молодых людей, поэтому усилия компаний по продвижению товаров и услуг с помощью персонализированных предложений чаще предназначаются для людей финансово независимых. Кроме того имеет место различное понимание термина «персонализация». Но в любом случае даже для молодых людей этот показатель очень высок – 77%. Самый высокий уровень предложений, основанных на анализе поведения потребителей, у людей в возрасте от 40 до 50 лет – почти 93%. В целом это свидетельствует о масштабном анализе действий пользователей и ярко выраженной тенденции к предоставлению индивидуализированных товаров и услуг.

Большинство людей старается ограничивать доступ к наиболее важной информации – так поступают 54% опрошенных. Ещё более внимательно относиться к обеспечению сохранности персональных данных планируют 82% от общего числа респондентов.

В соответствии с результатами опроса наиболее внимательно к личным данным относятся люди в возрасте до 20 лет и 40-50 лет. Никто из них не ответил, что спокойно размещает информацию о себе в открытом доступе, и никто из них не ответил, что не имеет смысла скрывать информацию о себе.

Более 83% тех, кто сталкивался со случаями мошенничества, считают, что рост информационных угроз обязывает относиться к персональным данным всё более внимательно. Те, кто не сталкивался со случаями мошенничества, в меньшей степени стараются минимизировать распространение личных данных, по сравнению с теми, кто имел дело с мошенниками. Влияние киберугроз на поведение потребителей можно представить в виде диаграммы.

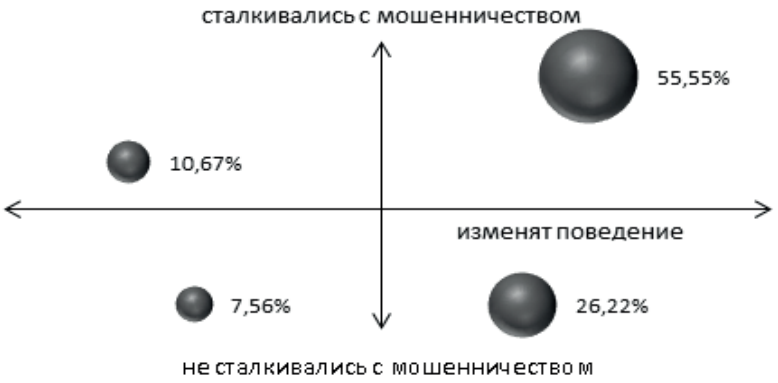

Рис. 7. Реакция пользователей на вызовы цифровизации
Источник: Составлено автором

Каждый пользователь основывается на предыдущем опыте, поэтому с одной стороны те, кто сталкивался с киберпреступниками, будет более бдительным и станет серьёзнее относиться к информационной безопасности, но с другой стороны подобные инциденты могут снижать доверие и интерес пользователей к электронным сделкам и замедлять развитие отрасли.

ЗАКЛЮЧЕНИЕ

Розничный сектор электронной коммерции является неотъемлемой составляющей цифровой экономики. Кроме угроз информационного характера в привычном понимании, таких как появление поддельных интернет-сайтов, атаки программ-вирусов, в электронной коммерции присутствуют и другие риски. К таким рискам относится недобросовестная конкуренция с использованием цифровых технологий, инсайдерские угрозы и прочее. Периодически возникают непредвиденные события, способные влиять на рост количества киберпреступлений. Ярким примером является эпидемия COVID-19[19]. Для обеспечения благоприятных условий развития отрасли необходим комплексный подход и использование передовых технологий. В настоящее время на всех уровнях регулирования ведётся активная работа для противодействия киберугрозам. К сотрудничеству приглашаются не только правительственные органы и международные организации, но и коммерческие компании, имеющие значительный опыт и способные внести вклад в борьбу с киберпреступлениями.

Анализ данных проведённого опроса подтвердил, что проявляющиеся информационные угрозы влияют на поведение потребителей. Для снижения негативного влияния киберпреступлений на развитие розничного сектора электронной коммер-

ции можно предложить разработать более выгодные и разнообразные (по сравнению с имеющимися на данный момент предложениями на рынке) условия страхования киберрисков для частных лиц. Также актуально пересмотреть принципы возмещение потерь от киберпреступлений и увеличить долю ответственности государства. И всем участникам рынка всегда следует помнить, что обеспечение безопасности – это непрерывный процесс, а не конечный результат.

ПРИМЕЧАНИЯ:

[1] Эрнесова Н.Э. Теоретические аспекты экономической безопасности // Вестник КРСУ. 2012. Т. 12. №11. С. 190–193.

[2] Цейковец Н.В. Концептуальные подходы к пониманию и обеспечению национальной экономической безопасности: научные теории и государственные стратегии // Журнал Новой экономической ассоциации. 2016. №1 (29). С. 129–157.

[3] Palak Gupta, Akshat Dubey. E-Commerce — Study of Privacy, Trust and Security from Consumer's Perspective. International Journal of Computer Science and Mobile Computing, 2016, vol. 5, no 6, pp. 224–232.

[4] Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физический лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation / GDPR // https://base.garant.ru/71936226/#friends

[5] Защита прав потребителей в сфере электронной торговли. Записка секретариата ЮНКТАД от 3 и 4 июля 2017 года // https://unctad.org/system/files/official-document/cicplpd7_ru.pdf

[6] UNCTAD B2C E–COMMERCE INDEX 2019 // https://unctad.org/system/files/official-document/tn_unctad_ict4d14_en.pdf

[7] ISO // https://www.iso.org/home.html

[8] Росстандарт. Федеральное агентство по техническому регулированию и метрологии // https://www.gost.ru/portal/gost/

[9] Об информации, информационных технологиях и о защите информации : федер. закон Рос. Федерации от 14 июля 2006 г. № 149–ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ. 2006. 29 июля.

[10] Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ от 5 декабря 2016 г. № 646

[11] Российский совет по международным делам. Блог по кибербезопасности// https://russiancouncil.ru/blogs/cyberrsmd/54/

[12] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности (Москва, 8 мая 2015 г.) // https://base.garant.ru/71032852/

[13] Проект Соглашения между Правительством Российской Федерации и Правительством Республики Узбекистан о сотрудничестве в области обеспечения международной информационной безопасности // http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=740402&dst=100007#01590619378042738

[14] Maintaining Payment Security // https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

[15] Сбер Банк // https://www.sberbank.ru/ru/press_center/all/article?newsID=9c2d6d45-aaf8-4805-b527-df0130a89a1b&blockID=1303&regionID=77&lang=ru&type=NEWS

[16] Karen Renaud, Craig Orgeron, Merrill Warkentin, P. Edward French. Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. Public Administration Review, 2020, vol. 00, iss. 00, pp. 1–13.

[17] State of the Union 2017: The Commission scales up its response to cyber-attacks // https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_3194

[18] Паризер Э. За стеной фильтров. Что Интернет скрывает от вас? / Эли Паризер ; пер. с англ. А. Ширикова. — М.: Альпина Бизнес Букс, 2012. — 304 с.

[19] Давыдов В.О. Спекуляция пандемией: как преступники используют кризис COVID–19 (по материалам доклада исполнительного директора Европол К. Де Боль «PANDEMIC PROFITEERING: HOW CRIMINALS EXPLOIT THE COVID–19» // Известия Тульского государственного университета. Экономические науки. — 2020. — №2. — 19–25.

БИБЛИОГРАФИЯ:

Давыдов В.О. Спекуляция пандемией: как преступники используют кризис COVID–19 (по материалам доклада исполнительного директора Европол К. Де Боль «PANDEMIC PROFITEERING: HOW CRIMINALS EXPLOIT THE COVID–19» // Известия Тульского государственного университета. Экономические науки. — 2020. — №2. — 19–25.

Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ от 5 декабря 2016 г. № 646

Защита прав потребителей в сфере электронной торговли. Записка секретариата ЮНКТАД от 3 и 4 июля 2017 года // https://unctad.org/system/files/official-document/cicplpd7_ru.pdf

Об информации, информационных технологиях и о защите информации : федер. закон Рос. Федерации от 14 июля 2006 г. № 149–ФЗ : принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ. 2006. 29 июля.

Паризер Э. За стеной фильтров. Что Интернет скрывает от вас? / Эли Паризер ; пер. с англ. А. Ширикова. — М.: Альпина Бизнес Букс, 2012. — 304 с.

Погорлецкий А.И. Налогообложение трансграничных операций электронной коммерции: особенности, проблемы и возможности // Вестник Томского государственного ун-та. Экономика. — 2019. — № 46. — С. 229–250. DOI: 10.17223/19988648/46/16. DOI: 10.17223/19988648/46/16

Погорлецкий А.И., Кешнер М.В. Косвенное налогообложение трансграничной электронной торговли: особенности национального и межгосударственного регулирования // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. — 2020. — 21. — № 1. — С. 256–280. DOI: 10.21684/2411-7897-2020-6-1-256-280

Проект Соглашения между Правительством Российской Федерации и Правительством Республики Узбекистан о сотрудничестве в области обеспечения международной информационной безопасности // http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=740402&dst=100007#01590619378042738

Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физический лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation / GDPR // https://base.garant.ru/71936226/#friends

Российский совет по международным делам. Блог по кибербезопасности// https://russiancouncil.ru/blogs/cyberrsmd/54/

Росстандарт. Федеральное агентство по техническому регулированию и метрологии // https://www.gost.ru/portal/gost/

Савинов Ю.А., Зеленюк А.Н., Тарановская Е.В. Использование технологии «блокчейн» в международной торговле // Российский внешнеэкономический вестник. — 2020. — №8. — С. 63–85.

Сбер Банк // https://www.sberbank.ru/ru/press_center/all/article?newsID=9c2d6d45-aaf8-4805-b527-df0130a89a1b&blockID=1303&regionID=77&lang=ru&type=NEWS

Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности (Москва, 8 мая 2015 г.) // https://base.garant.ru/71032852/

Эрнесова Н.Э. Теоретические аспекты экономической безопасности // Вестник КРСУ. — 2012. — Т. 12 — №11. — С. 190–193.

Цейковец Н.В. Концептуальные подходы к пониманию и обеспечению национальной экономической безопасности: научные теории и государственные стратегии // Журнал Новой экономической ассоциации. — 2016. — №1 (29). — С. 129–157.

ISO // https://www.iso.org/home.html

Karen Renaud, Craig Orgeron, Merrill Warkentin, P. Edward French. Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. Public Administration Review, 2020, vol. 00, iss. 00, pp. 1–13.

Maintaining Payment Security // https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

Palak Gupta, Akshat Dubey E-Commerce — Study of Privacy, Trust and Security from Consumer's Perspective // International Journal of Computer Science and Mobile Computing. — 2016. — Vol. 5 — Issue. 6. — P. 224–232.

State of the Union 2017: The Commission scales up its response to cyber-attacks // https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_3194

UNCTAD B2C E–COMMERCE INDEX 2019 // https://unctad.org/system/files/official-document/tn_unctad_ict4d14_en.pdf

BIBLIOGRAPHY:

Davy`dov V.O. Spekulyaciya pandemiej: kak prestupniki ispol`zuyut krizis COVID–19 (po materialam doklada ispolnitel`nogo direktora Evropol K. De Bol` «PANDEMIC PROFITEERING: HOW CRIMINALS EXPLOIT THE COVID–19» // Izvestiya Tul`skogo gosudarstvennogo universiteta. E`konomicheskie nauki. — 2020. — №2. — 19–25.

Doktrina informacionnoj bezopasnosti Rossijskoj Federacii : utv. Ukazom Prezidenta RF ot 5 dekabrya 2016 g. № 646

Zashhita prav potrebitelej v sfere e`lektronnoj torgovli. Zapiska sekretariata YuNKTAD ot 3 i 4 iyulya 2017 goda // https://unctad.org/system/files/official-document/cicplpd7_ru.pdf

Ob informacii, informacionny`x texnologiyax i o zashhite informacii : feder. zakon Ros. Federacii ot 14 iyulya 2006 g. № 149–FZ : prinyat Gos. Dumoj Feder. Sobr. Ros. Federacii 8 iyulya 2006 g. : odobr. Sovetom Federacii Feder. Sobr. Ros. Federacii 14 iyulya 2006 g. // Ros. gaz. 2006. 29 iyulya.

Parizer E`. Za stenoj fil`trov. Chto Internet skry`vaet ot vas? / E`li Parizer ; per. s angl. A. Shirikova. — M.: Al`pina Biznes Buks, 2012. — 304 s.

Pogorleczkij A.I. Nalogooblozhenie transgranichny`x operacij e`lektronnoj kommercii: osobennosti, problemy` i vozmozhnosti // Vestnik Tomskogo gosudarstvennogo un-ta. E`konomika. — 2019. — № 46. — S. 229–250. DOI: 10.17223/19988648/46/16. DOI: 10.17223/19988648/46/16

Pogorleczkij A.I., Keshner M.V. Kosvennoe nalogooblozhenie transgranichnoj e`lektronnoj torgovli: osobennosti nacional`nogo i mezhgosudarstvennogo regulirovaniya // Vestnik Tyumenskogo gosudarstvennogo universiteta. Social`no-e`konomicheskie i pravovy`e issledovaniya. — 2020. — 21. — № 1. — S. 256–280. DOI: 10.21684/2411-7897-2020-6-1-256-280

Proekt Soglasheniya mezhdu Pravitel`stvom Rossijskoj Federacii i Pravitel`stvom Respubliki Uzbekistan o sotrudnichestve v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti // http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=740402&dst=100007#01590619378042738

Reglament Evropejskogo Parlamenta i Soveta Evropejskogo Soyuza 2016/679 ot 27 aprelya 2016 g. o zashhite fizicheskij licz pri obrabotke personal`ny`x danny`x i o svobodnom obrashhenii takix danny`x, a takzhe ob otmene Direktivy` 95/46/ES (Obshhij Reglament o zashhite personal`ny`x danny`x / General Data Protection Regulation / GDPR // https://base.garant.ru/71936226/#friends

Rossijskij sovet po mezhdunarodny`m delam. Blog po kiberbezopasnosti// https://russiancouncil.ru/blogs/cyberrsmd/54/

Rosstandart. Federal`noe agentstvo po texnicheskomu regulirovaniyu i metrologii // https://www.gost.ru/portal/gost/

Savinov Yu.A., Zelenyuk A.N., Taranovskaya E.V. Ispol`zovanie texnologii «blokchejn» v mezhdunarodnoj torgovle // Rossijskij vneshnee`konomicheskij vestnik. — 2020. — №8. — S. 63–85.

Sber Bank // https://www.sberbank.ru/ru/press_center/all/article?newsID=9c2d6d45-aaf8-4805-b527-df0130a89a1b&blockID=1303&regionID=77&lang=ru&type=NEWS

Soglashenie mezhdu Pravitel`stvom Rossijskoj Federacii i Pravitel`stvom Kitajskoj Narodnoj Respubliki o sotrudnichestve v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti (Moskva, 8 maya 2015 g.) // https://base.garant.ru/71032852/

E`rnesova N.E`. Teoreticheskie aspekty` e`konomicheskoj bezopasnosti // Vestnik KRSU. — 2012. — T. 12 — №11. — S. 190–193.

Cejkovecz N.V. Konceptual`ny`e podxody` k ponimaniyu i obespecheniyu nacional`noj e`konomicheskoj bezopasnosti: nauchny`e teorii i gosudarstvenny`e strategii // Zhurnal Novoj e`konomicheskoj associacii. — 2016. — №1 (29). — S. 129–157.

ISO // https://www.iso.org/home.html

Karen Renaud, Craig Orgeron, Merrill Warkentin, P. Edward French. Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. Public Administration Review, 2020, vol. 00, iss. 00, pp. 1–13.

Maintaining Payment Security // https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

Palak Gupta, Akshat Dubey E-Commerce — Study of Privacy, Trust and Security from Consumer's Perspective // International Journal of Computer Science and Mobile Computing. — 2016. — Vol. 5 — Issue. 6. — P. 224–232.

State of the Union 2017: The Commission scales up its response to cyber-attacks // https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_3194

UNCTAD B2C E–COMMERCE INDEX 2019 // https://unctad.org/system/files/official-document/tn_unctad_ict4d14_en.pdf