

pISSN 2073-2872
eISSN 2311-875X

Экономическая безопасность

КОМПАЕНС-КОНТРОЛЬ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КОМПАНИЙ В СФЕРЕ ЭЛЕКТРОННОЙ ТОРГОВЛИ

Вилена Анатольевна ЯКИМОВА ^{a,*},
Виктор Сергеевич РАДОМСКИЙ ^b

^a кандидат экономических наук, доцент кафедры финансов,
Амурский государственный университет,
Благовещенск, Российская Федерация
vilena_yakimova@mail.ru
<https://orcid.org/0000-0001-5866-5652>
SPIN-код: 4477-4930

^b кандидат физико-математических наук,
генеральный директор ООО «КОМП»,
Москва, Российская Федерация
vitek1715@yandex.ru
ORCID: отсутствует
SPIN-код: 4097-2740

* Ответственный автор

История статьи:

Рег. № 259/2021
Получена 10.05.2021
Получена в
доработанном виде
26.05.2021
Одобрена 11.06.2021
Доступна онлайн
16.08.2021

УДК 657.6

JEL: F23, G32, M42

Ключевые слова:

цифровая экономика,
электронный бизнес,
электронная торговля,
ИТ-риски,
информационная
система, система
внутреннего
комплаенс-контроля

Аннотация

Предмет. Организационно-методические вопросы системы внутреннего комплаенс-контроля для предприятий, специализирующихся в области электронной торговли.

Цели. Совершенствование организации и методики внутреннего комплаенс-контроля с учетом особенностей бизнес-процессов и ИТ-рисков для предприятий электронной торговли.

Методология. Исследование базируется на применении методов анализа и обобщения, группировки, систематизации, риск-ориентированного, системного и бизнес-процессного подходов.

Результаты. В процессе исследования разработана пятикомпонентная система комплаенс-контроля, определены ее принципы и функции для обеспечения экономической безопасности предприятий, реализующих продукцию на основе электронной коммерции. Предлагаются комплаенс-процедуры, направленные на снижение ИТ-рисков и учитывающие особенности бизнес-процессов предприятий электронной торговли.

Область применения. Результаты исследования могут быть использованы в ходе формирования надежной и эффективной комплаенс-системы предприятий электронной торговли в целях предотвращения экономических правонарушений и преступлений.

Выводы. Комплаенс-контроль в сфере электронной торговли является механизмом, направленным на выявление и контроль комплаенс-рисков для безопасного функционирования

предприятий, важных для обеспечения потребностей жизнедеятельности населения. Установлено, что базовым элементом системы комплаенс-контроля является информационная система, которая должна обеспечивать защиту от IT-рисков, а процедуры контроля могут быть разделены на общие и прикладные.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2021

Для цитирования: Якимова В.А., Радомский В.С. Комплаенс-контроль как инструмент обеспечения экономической безопасности компаний в сфере электронной торговли // *Национальные интересы: приоритеты и безопасность*. – 2021. – Т. 17, № 8. – С. 1491 – 1518.
<https://doi.org/10.24891/ni.17.8.1491>

Комплаенс-контроль как самостоятельный вид контрольной деятельности, направленной на предупреждение и выявление фактов нарушения законодательства, является неотъемлемым элементом рыночной экономики и государственной политики в области обеспечения экономической безопасности общества. В основу стратегии национальной безопасности государства положена концепция устойчивого развития экономических систем, провозглашенная международными организациями (ООН, ОЭСР). Устойчивое развитие становится стратегическим приоритетом и достигается при обеспечении экономического роста и стабильного улучшения качества жизни населения, сохранения окружающей среды для будущих поколений. В устойчивой экономике важное значение приобретает сбалансированное состояние производства и потребления, экспорта и импорта и т.п. С 2020 г. распространение коронавирусной инфекции (COVID-19) привело к росту дистанционных форм взаимодействия в сфере розничной торговли, что активизировало переход многих предприятий от традиционных рынков к электронным, внедрение цифровых информационных технологий и формирование новых социально-экономических отношений в обществе.

Одним из факторов, сдерживающих развитие электронного бизнеса, являются риски потери и искажения финансовой информации в IT-среде, рост случаев финансового мошенничества, что вызывает необходимость разработки и внедрения мер по обеспечению экономической безопасности предприятий. Электронная торговля, как составная часть активно развивающегося электронного бизнеса, имеет свои особенности, которые необходимо принимать во внимание при формировании системы внутреннего контроля (далее – СВК). В научных трудах ряд отечественных ученых исследуют тенденции и проблемы развития электронного бизнеса (С.Ю. Ревина [1], Р.Р. Салихова [2], Т.Н. Беляцкая [3], М.С. Романцов [4], Г.Г. Медведев, Б.С. Касаев [5], Л.Г. Никитюк, О.Г. Тимчук [6]), внутренний контроль в сфере традиционной торговли (Ж.А. Аксенова, О.В. Ищенко,

В.П. Леошко [7]), методы и процедуры комплаенс-контроля как формы СВК (А.А. Николаева [8], Д.А. Чирков [9], Ж.А. Кеворкова, Н.Г. Сапожникова [10]). Однако вопросы организации СВК для компаний в сфере электронного бизнеса являются недостаточно изученными, а традиционные процедуры контроля в торговых организациях не позволяют предотвратить весь комплекс IT- и комплаенс-рисков, которым подвержена информационная система.

Возникновению электронной коммерции (*e-commerce*) в 1970-х гг. способствовали разработки в области электронных платежных средств (EFT) и систем электронного обмена данными (EDI), которые обеспечили возможность обработки различных типов транзакций: от финансовых до коммерческих. О тенденциях развития в России условий цифрового экономического пространства свидетельствует как рост числа хозяйствующих субъектов, вовлеченных в электронный бизнес, так и рост объема продаж в интернет-торговле (рис. 1).

До 2019 г. наблюдался положительный рост трансграничной интернет-торговли, в 2020–2021 гг. обозначилось заметное сокращение объемов экспорта в связи с закрытием границ и замедлением доставки товаров. Приоритетным направлением интернет-торговли стали продажи на внутреннем рынке. В структуре интернет-торговли преобладают одежда и обувь (в 2020 г. – 31,6%), цифровая и бытовая техника (21,5%). При этом рост интернет-магазинов способствовал развитию систем потребительского онлайн-кредитования и электронных платежных систем [1].

Категория «электронная торговля» в научной литературе взаимосвязана со схожими понятиями «электронная экономика», «электронный бизнес», «электронная коммерция», «интернет-торговля». Наиболее широкое понятие «электронная экономика» означает «техносоциальную распределенную систему производства, обмена и конечного потребления материальных благ, имеющих разную степень электронно-информационного компонента» [3].

Так, М.С. Романцов [4], Г.Г. Медведев, Б.С. Касаев [5], Л.Г. Никитюк, О.Г. Тимчук [6] определили электронный бизнес как совокупность технических и организационных форм совершения финансовых и торговых транзакций с использованием электронных систем. А.А. Назаров, В.И. Иванова [11] приводят следующее определение: электронная торговля – это коммерческие сделки, в которые вовлечены как организации, так и физические лица, при условии, что эти сделки связаны с передачей и обработкой цифровой информации, включая текстовые, звуковые и визуальные данные, получаемые из открытых или закрытых сетей. Таким образом, отличительным признаком и фактором оптимизации является

электронная форма сделок, информационные и цифровые средства коммуникации между производителем и потребителем благ.

В цифровой экономике видоизменяется модель бизнеса в направлении выхода предприятия на глобальные рынки сбыта с помощью интернет-технологий, что позволяет достичь за короткий период времени эффекта масштаба и сократить транзакционные издержки. Экономический эффект достигается с помощью ускорения обмена информацией, оперативного реагирования на запросы покупателей и их удовлетворения за счет широты ассортимента, возможности приобретения уникальных товаров. В качестве преимуществ электронной торговли отмечается создание и накопление ритейл-данных, применение режима офлайн-продаж [12], гибкая ценовая политика, электронный документооборот [2], реализация функции отслеживания заказа в пути, цифровизация логистических систем, услуги фулфилмент-операторов, которые обеспечивают приемку, хранение, обработку, доставку товара [13]. Предприятия электронной торговли быстро создают и доставляют товары, получают конкурентные преимущества за счет удовлетворения индивидуальных потребностей, расширения географических рынков сбыта, масштабных рекламных мероприятий и отлаженной маркетинговой системы.

Информационные технологии в бизнесе позволяют собирать, агрегировать, анализировать большие потоки информации, обеспечивать ее точность и надежность, хранить электронные документы в неограниченном объеме, осуществлять быстрый поиск и выдачу по требованию любому заинтересованному пользователю. Получили распространение инструменты управления цепочками поставок, автоматизации работы с партнерами (e-SCM) и взаимоотношения с клиентами (e-CRM) [14]. Интернет-магазин интегрирован с системами складского и бухгалтерского учета, торговыми системами, а для крупных корпораций – с ERP-системами, позволяющими планировать ресурсы и интегрировать бизнес-процессы электронного бизнеса. Комплексные интернет-ориентированные системы позволяют осуществлять сервисное обслуживание, анализировать спрос и цены на рынке и управлять каналами доставки.

Таким образом, особенности электронной торговли, отличающие ее от традиционной торговли, заключаются в следующем:

- 1) взаимодействие между участниками торгового процесса, оформление сделок осуществляется в цифровом формате;
- 2) непрерывность работы, постоянная доступность и возможность оформления заказа в любое время суток;
- 3) массовость однотипных торговых и электронных платежных операций;
- 4) отсутствие упорядоченной географической сети поставок;

- 5) широкая возможность использования электронных средств платежа: банковские переводы, электронные деньги, мобильные платежи, наличный расчет при курьерской доставке, наложенный платеж при почтовой доставке;
- 6) необходимость обеспечения сохранности и защиты товара в момент его доставки до потребителя;
- 7) обработка и передача информационных ресурсов составляют значительную часть бизнес-процессов, а управление и контроль базируется на принципе самоорганизации в автоматическом режиме;
- 8) маркетинг и продвижение товаров на рынок, предполагающие активное применение скидок, акций;
- 9) традиционная и электронная форма активов, прав собственности.

Электронный рынок не может развиваться устойчиво, когда существуют риски обмана, злоупотребления доверием, роста экономических правонарушений, фактов мошенничества и т.п. Как показывает статистика, наряду с ростом объемов интернет-торговли возрастают и факты мошенничества с применением электронных средств платежа (рис. 2).

Количество уголовно наказуемых преступлений в 2019 г. увеличилось в несколько раз, а именно – с 95 до 710, одновременно возросло и число наказаний в виде штрафов и лишения свободы. На рис. 3 приведена динамика правонарушений в сфере торговли.

В торговле по видам правонарушений лидируют нарушения порядка ценообразования, что вызывает необходимость применения процедур антимонопольного комплаенса. При этом в 2019 г. выявлено большее количество правонарушений, связанных с реализацией без применения контрольно-кассовой техники (ККТ), что обусловлено повышением эффективности мер и процедур контроля, направленных на предотвращение фактов нелегальных продаж в рознице.

Таким образом, Интернет, выступая средой общего пользования, не только дает широкие возможности и условия для развития бизнеса на основе информационного взаимодействия субъектов, но несет в себе информационные риски, не свойственные традиционной торговле. Большинство авторов (Н.В. Быстрова, К.А. Максимова [15], Л.Г. Никитюк, О.Г. Тимчук [6], Р.Р. Салихова [2]) в качестве проблем развития электронной торговли отмечают низкий уровень надежности информационных систем, безопасности в Интернете при осуществлении коммерческих сделок, отсутствие контроля за соблюдением норм и регулирования взаимоотношений между участниками электронной коммерции,

неразвитость нормативно-правовой базы, мошенничество в целях подорвать имидж компании.

Контроль, обеспечивающий экономическую безопасность в электронной торговле, является сложным механизмом. В европейских странах злоупотребления в электронном бизнесе пресекаются за счет использования специальных электронных алгоритмов для выявления фактов нарушения законодательства, а в случае трансграничной торговли используется обмен данными между национальными системами администрирования НДС [16]. Системы государственного контроля за кибермошенничеством и защитой информации в электронном виде нельзя назвать в полной мере эффективными. В то же время традиционные процедуры внутреннего контроля торговых предприятий охватывают только проверку аналитического учета движения денежных средств, выявление фактов хищений на складах, проверку соблюдения графика документооборота, применения ККТ, ведения фискальной памяти и замены накопителей [7]. Для электронной торговли перечисленных процедур становится недостаточно в силу особенностей деятельности и возможных угроз экономической безопасности. При этом А.А. Коваль, А.Д. Левашенко [17] справедливо отмечают, что предприятия электронной торговли должны обеспечивать безопасность онлайн-платежей, защиту персональных данных потребителей, цифровых активов, точность и надежность учетных данных, а также соблюдение нормативно-правовых актов в сфере торговых и финансовых отношений.

Роль СВК компаний в сфере электронной торговли заключается в обеспечении экономической безопасности, что предполагает защиту электронного бизнеса от факторов случайного и преднамеренного воздействия, которые могут нанести ущерб деловой репутации, имиджу партнера, потребителям продукции и информационной системе, которая поддерживает развитие розничной торговли. В систему контроля для полного решения всех задач должна быть встроена функция комплаенса. Большинство авторов в качестве преимуществ комплаенса указывают на повышение эффективности деятельности, увеличения конкурентоспособности, стоимости бизнеса и доверия со стороны рынка и всех заинтересованных сторон [8–10, 18]. Б.С. Батаева, В.А. Черепанова [19] справедливо отмечают, что комплаенс-контроль снижает риск существенного финансового убытка или потери репутации в результате несоблюдения бизнес-правил поведения, установленных в деловой среде.

Комплаенс-контроль представляет собой наиболее эффективную систему снижения комплаенс-рисков, связанных с возникновением у компании юридической ответственности различных форм (административной, дисциплинарной, материальной, гражданско-правовой и уголовной) и соответствующих видов санкций, материальных и финансовых потерь,

утраты доверия контрагентов, репутации и прекращения бизнеса [8]. Внутренний комплаенс-контроль важен для мониторинга и оценки соблюдения действующего законодательства и стандартов, которые для компаний электронного бизнеса являются недостаточно проработанными. В ходе контроля определяется состояние объектов контроля, фактические данные сопоставляются с плановыми, выявляются причины отклонений, которые могут сформировать угрозы экономической безопасности и повлечь рост криминализации торговой сферы.

Формирование системы внутреннего контроля компаний, действующих в сфере электронной торговли, должно быть основано на выделении особенностей информационной системы, а также форм и методов внутреннего контроля. В электронной коммерции взаимосвязанными элементами единой СВК являются информационные системы, внутриорганизационные бизнес-процессы, поддерживающие транзакции, межорганизационные процессы и системы в интернет-среде. Взаимосвязанное выполнение функций всех элементов комплаенс-системы позволяет эффективно реализовать информационно-коммуникационные задачи. Бизнес-процессы электронной торговли являются уникальными и формируют цифровые связи между участниками процесса, позволяют реагировать на изменения в IT-среде. Бизнес-процессный подход для предприятий электронной торговли развит в научных трудах А.А. Назарова, В.И. Ивановой [11], И.А. Шишкина, В.Л. Хацкевича, Л.Д. Хацкевича [20]. Для формирования СВК на предприятиях электронной торговли выделены основные бизнес-процессы (рис. 4).

Объектами контроля становятся как информационные ресурсы, базы и хранилища данных, IT-технологии, цифровые активы, так и бизнес-процессы, которые обеспечивают перемещение и преобразование ресурсов. Продавец, размещая на интерактивном веб-сайте информацию о товарах и услугах, предлагает пользователям ознакомиться с ассортиментом и ценами, различными формами оплаты, при этом организует доставку и обязан контролировать расчеты с покупателем. Согласно п. 13 постановления Правительства РФ от 31.12.2020 № 2463¹, договор считается заключенным с момента выдачи продавцом покупателю кассового или товарного чека либо иного документа, подтверждающего оплату товара, а продавец предоставляет оферту. Доставка может быть курьерской (подтверждается накладной) или почтовой (имеется больший риск порчи и

¹ Об утверждении Правил продажи товаров по договору розничной купли-продажи, перечня товаров длительного пользования, на которые не распространяется требование потребителя о безвозмездном предоставлении ему товара, обладающего этими же основными потребительскими свойствами, на период ремонта или замены такого товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих обмену, а также о внесении изменений в некоторые акты Правительства Российской Федерации: постановление Правительства РФ от 31.12.2020 № 2463.

хищения товара, который ложится на организацию-продавца), либо со склада продавца.

В современных условиях оплата за товар может производиться посредством электронных платежей, что требует заключения с обслуживающим банком договора интернет-эквайринга, регистрации продавца в ЭПС, заключения договора с агентством, которое будет переводить электронные деньги. Для переводов электронных денег используются электронные кошельки. В законе «О НПС»² определены лимиты остатков электронных денежных средств в корпоративных кошельках (не свыше 600 тыс. руб.). Предприятия электронной торговли могут применять мобильные переводы – SMS-сообщения, USSD-команды, технологии бесконтактной оплаты (NFC) или приложения мобильного банкинга. Также возможна оплата товара при доставке в почтовом отделении при получении товара, когда работник почтовой службы переводит платеж на адрес продавца.

Бизнес-риски, присущие электронной торговле и формирующие угрозы экономической безопасности, представляется возможным сгруппировать следующим образом:

- 1) возникновение внутреннего и внешнего мошенничества (злоупотребление активами, использование электронных платежных систем, невыполнение требований законодательства в электронном бизнесе, мошенничество со стороны покупателей, удаленные или локальные хакерские атаки на ИТ-ресурсы);
- 2) технические риски, риски, связанные с особенностями строения системы обработки данных: неточность данных, технические сбои, неисправность аппаратного обеспечения, отсутствие целостности компьютерной системы;
- 3) системные ошибки (в алгоритме, классификаторах, справочных системах), неспособность произвести модификации в системах или программах, когда это необходимо, несовершенство защиты информации;
- 4) риск случайной гибели, порчи товара при транспортировке в результате несоблюдения условий хранения, противоправных действий или стихийных бедствий;
- 5) риск невыполнения договорных обязательств и отказа от сделки;

² О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 22.12.2020).

- 6) неправильное проведение операций или управление в процессе построения отношений с заказчиками, искажение информации при вводе пользователем;
- 7) ненадлежащий контроль за сохранностью данных операционного учета, несанкционированный доступ к данным и отсутствие конфиденциальности, что может привести к ненадлежащим модификациям данных или цифровых активов;
- 8) несвоевременность ввода данных в программу по независящим причинам (большие расстояния, исправления из-за «человеческого фактора» стороны, отправившей документ).

Угрозы экономической безопасности в электронной торговле могут привести к разрушению аппаратно-программных средств и технологий обработки учетных данных, потере и недоступности информационных данных, которые отражаются в бухгалтерском учете и необходимы для формирования финансовой отчетности. Высокая скорость осуществления сделок в интернет-торговле обуславливает необходимость усиления принципа непрерывности мониторинга, интегрированности приемов и методов контроля, актуализации в связи с постоянным совершенствованием средств обхода СВК и кибератаками. Уточненные функции внутреннего контроля для предприятий электронной торговли представлены в *табл. 1*.

На *рис. 5* представлен проект СВК, элементы которой учитывают особенности компаний в сфере электронной торговли.

Контрольная среда формирует общую атмосферу предприятия электронной торговли и принятия сотрудниками функций контроля, в связи с чем важной составляющей должна выступать политика экономической и информационной безопасности. Учитывая требования к формированию контрольной среды, должны быть четко распределены обязанности между владельцами бизнес-процессов и ИТ-службой. В надежной комплаенс-системе владельцы бизнес-процессов отвечают за выполнение функциональных требований, применение сервисов, а ИТ-службы – за автоматизацию и настройку функций, процедур, осуществление контроля в целях обеспечения целостности приложений.

В *информационной системе* происходит формирование широкой базы данных на основе процедур обработки, регистрации и аккумуляции операций и сделок, поэтому от надежности ее функционирования напрямую зависит операционное обслуживание клиентов, полнота и достоверность бухгалтерской отчетности.

Информационные системы, формируя совокупность информационного, технического, программного, технологического и организационного обеспечения (ИТ-бизнес-процессы, ИТ-приложения и ИТ-инфраструктура),

связывают все объекты в технологическую цепочку сбора информации и обеспечивают доступ к информации для анализа и управления. Система электронной торговли представляет собой пользовательскую систему, содержащую прикладную программу, способ передачи данных, программное обеспечение для обмена данными. Для управления бизнес-процессами используются IT-приложения, к которым относятся технические ресурсы, а именно стандартное или специализированное программное обеспечение, используемое для реализации всех процессов и функционирования IT-системы. Автоматизированные системы управляют процессами сбора информации из внутренних и внешних источников, дистанционного доступа потребителей к информации, обработки и хранения электронных документов, ведения учета, анализа и составления отчетности. С помощью автоматизации документооборота сокращаются расходы, снижается риск потери документов, ошибочной адресации, фальсификации платежных документов (табл. 2).

Международный стандарт CobiT «Контрольные объекты для информационных и смежных технологий» обязывает при оценке информационной системы учитывать стадию ее зрелости (рис. 6), а также соответствие критериям целостности, актуальности, своевременности. Выполнение перечисленных требований составляет базу функционирования IT-системы электронной торговли. В информационной системе происходит генерирование бизнес-операций, выгруженных с веб-сайта, обработка с помощью внутренних систем учета, контроля и управления. Система автоматизированного учета должна отвечать требованиям полноты и точности обработки, систематизации информации, своевременности признания в учете доходов и расходов, оценки всех торговых операций, состояния запасов и сохранности данных.

На этапе ввода и принятия информации к обработке важно, чтобы все данные были введены клиентом, информация о заказе и клиенте была подлинной, отсутствовали ошибки и дублирование заказов. Проверка функционирования информационной системы сводится к оценке выполнения функции, введенных записей, процедур ввода, обработки и вывода данных, действия программного управления, возможности отслеживания транзакций и проверке соблюдения законодательства.

Основу СВК составляют контрольные действия, целью выполнения которых является предупреждение и управление IT- и комплаенс-рисками. Для выбора способов контроля необходимо идентифицировать и ранжировать IT-риски по степени их критичности, то есть с точки зрения угроз и проявления факторов риска. Под *фактором комплаенс-риска* следует понимать способ воздействия на информационную систему, который может привести к нарушению целостности, конфиденциальности или иных свойств системы, что, в свою очередь, угрожает уязвимостью

всей СВК по отношению к факторам ошибок и умышленным вмешательствам мошенников. Ценность контрольной процедуры определяется величиной ущерба, наносимого в случае нарушения безопасности экономической системы в ситуации действий злоумышленников. При планировании комплаенс-контроля необходимо спрогнозировать финансовые потери и выделить места, слабые с точки зрения информационной защищенности. Система комплаенс-контроля в электронной торговле должна быть направлена на обеспечение экономической безопасности путем соблюдения следующих основных принципов:

- наличие и соблюдение правил авторизации, аутентификации, конфиденциальности, целостности, ограничения доступа к данным и доступности информации. Основными инструментами обеспечения безопасности являются брандмауэр, антивирусная защита (защита веб-сервера и сервера бэк-офиса), шифрование для защиты от несанкционированного доступа неавторизованными пользователями, мониторинг, протоколирование электронной передачи данных для идентификации потерь или потери информации о транзакциях, программное обеспечение для обнаружения атак, идентификация и проверка получателя данных, обеспечение безопасности веб-сайтов для невозможности внесения изменений в структуру и содержание сайта, резервное копирование. Аутентификация представляет собой проверку подлинности и инициирование участников транзакции с помощью процедуры авторизации (защита с помощью системы паролей) и цифровой подписи;
- обеспечение сохранности транзакций: полнота, точность, достоверность зарегистрированной и обрабатываемой информации (проверка соответствия записей, предотвращение дублирования или пропуска операций, гарантия принятия условий доставки и кредитования при выполнении заказа, защита от отказа одного из участников в совершении сделки после принятия договорных условий, предотвращение неполной обработки и возможность уточнения условий сделки для обеспечения регистрации всей необходимой информации, распределение информации о сделке в единой сети и хранение, резервирование зарегистрированных записей);
- согласование процессов, интегрируемых в единой информационной системе компании для обеспечения полноты и точности обработки информации о сделках, хранение данных, своевременное признание выручки от продажи, идентификация спорных сделок;
- поддержание процедур контроля в условиях постоянных экономических и информационно-технических изменений.

Система комплаенс-контроля при реализации электронных транзакций должна включать два уровня контроля (рис. 7).

Первый уровень комплаенс-контроля внедряется в интерфейс системы пользователя и осуществляется перед или во время отправки информации о сделке. Процедуры контроля первого уровня должны включать проверку подлинности данных о пользователе, полноты данных, отсутствия признаков фальсификации. На первом уровне проверяется соблюдение требований аутентичности, конфиденциальности, целостности и эффективности сделки. Проверенная информация поступает на интернет-сайт продавца, где должна быть верифицирована на соблюдение требования полноты, точности, достоверности и своевременности (второй уровень). На втором уровне осуществляется защита входящих и исходящих данных, контроль полноты, отсутствия сбоев и потери информации, ошибок пользователей. Информация проверяется на соответствие принципам точности, своевременности обработки и одобрения участниками сделки.

В СВК должны использоваться организационные, технические и технологические средства контроля. Цель применения организационных средств заключается в обеспечении надежности и безопасности системы управления ИТ-рисками, технических средств – в использовании процедур и методов контроля для защиты ИТ-активов. Технологические (операционные) средства используются для контроля непрерывности и обеспечения долгосрочности функционирования системы, а также всех созданных цифровых активов (резервное копирование информации). В табл. 3 представлены предлагаемые процедуры для реализации комплаенс-контроля предприятий электронной торговли.

Процедуры внутреннего контроля подразделяются на общие и прикладные. Общий контроль, осуществляемый в целях обеспечения бесперебойной и непрерывной работы предприятия электронной торговли, предусматривает контроль компьютерных систем (главного компьютера, системы «клиент – сервер», рабочих мест конечных пользователей и т.д.). Общие меры контроля включают проверку полноты, точности, достоверности данных об электронных продажах, авторизации и разделения обязанностей. Необходимо организовать контроль за изменением программного обеспечения, ограничением доступа к нему и базам данных, реализации новых версий прикладных систем и резервирования, восстановления данных [21].

Контроль ИТ-систем должен осуществляться в целях обеспечения защиты данных от угрозы потери в случае неполадок оборудования и системных сбоев. Информационная система должна гибко реагировать на изменения нормативно-законодательной базы, обеспечивать архивирование баз данных, передачу данных с использованием каналов связи, выполнение

процедур мониторинга. Прикладной контроль направлен на проверку правильности обработки и регистрации данных в системе, умений и навыков работы с программой.

Прикладные средства контроля позволяют исключить арифметические и логические ошибки обработки данных, обобщения, систематизации и регистрации первичной информации. Необходимо организовать контроль за исправительными записями, которые могут ввести в заблуждение, проверить в таких участках обоснованность продаж и расходов, надлежащее оформление и полноту документирования, права доступа к учетным записям. Ручные приемы контроля целесообразно применять в случае проверки подозрительных и сомнительных бизнес-операций, в крупных суммах, требующих особого контроля со стороны контрольно-надзорных органов.

Таким образом, предлагаемая система внутреннего комплаенс-контроля призвана нейтрализовать влияние рисков нарушения законодательства и несоблюдения принципов и стандартов в сфере торговли и безопасности информационных систем. СВК включает информационную систему, процессы и процедуры контроля, направленные на обеспечение защиты от внутреннего и внешнего вмешательства, несанкционированного доступа, что гарантирует достоверность и надежность данных учета и бухгалтерской отчетности, а также защиту потребителей от случаев мошенничества в электронном бизнесе.

Таблица 1**Уточнение функций СВК в электронной торговле****Table 1****The clarification of internal control functions in e-commerce**

Традиционные функции внутреннего контроля	Уточненные функции внутреннего контроля в электронной торговле
Оценка рациональности <i>плановых</i> решений, соответствие <i>плановых</i> решений принятым установкам и ориентирам	Выявление резервов и направлений электронного бизнеса, прогноз развития внешней электронной среды бизнеса, оценка потенциала IT-технологий
Контроль за выполнением принятых <i>плановых</i> решений для достижения необходимых результатов	Анализ реализации бизнес-проектов и использования бизнес-аналитики для стратегического планирования. Автоматизация контроля для эффективности обработки электронных транзакций
Контроль за наличием и движением <i>имущества</i> , рациональности использования ресурсов согласно нормам, соответствие выданных и полученных обязательств, целесообразностью и законностью операции	Оценка достоверности электронной информации о движении товаров, выполнении договорных обязательств, состояния складских запасов, контроль за состоянием и выполнением обязательств, рациональность товародвижения и схем логистики, контроль сохранности товаров на всех этапах движения заказа
Оценка информации о <i>результатах</i> выполнения управленческих решений	Подготовка цифровой информации и контроль принимаемых управленческих решений в электронной торговле
Проверка соответствия принятых управленческих решений, выявление отклонений от намеченных целей, корректировка при необходимости	Выработка рекомендаций по совершенствованию деятельности, оценка результативности работы IT-служб
Управление рисками (анализ и разработка методов снижения)	Управление IT-рисками в информационной системе электронной коммерции

Источник: авторская разработка

Source: Authoring

Таблица 2**Матрица «Бизнес-процесс предприятия электронной торговли – Принципы экономической безопасности в IT-системе»****Table 2****The matrix – Business Process of E-Commerce Enterprise – Principles of Economic Security in the IT system**

Бизнес-процесс	Конфиденциальность	Полнота (целостность)	Аутентификация	Авторизация	Невмешательство третьих лиц
Заключение договора с поставщиком, закупка товаров	–	+	+	–	+
Складирование	–	+	–	–	+
Создание веб-сайта, опубликование на сайте каталога и подробной информации о товаре	+	+	–	+	+

Оформление и размещение заказа	+	+	+	–	+
Подтверждение и оплата заказа	+	+	+	–	+
Уведомление об отправке и доставка заказа, подтверждение получения	+	+	+	+	+

Источник: авторская разработка

Source: Authoring

Таблица 3

Группировка процедур комплаенс-контроля компаний в сфере электронной торговли по объектам и факторам риска

Table 3

The grouping of compliance control procedures in e-commerce businesses by target and risk factor

Объект контроля	Фактор IT- и комплаенс-риска	Процедуры контроля
Наличие документооборота и взаимодействия между отделами	Некорректный и (или) несвоевременный ввод данных в программу, риск хищений в результате потери или фальсификации документов	Оценка заключенных договоров на соответствие условиям движения документов внутренним регламентам, положению об информационной безопасности, инструкциям и т.п. Оценка соблюдения графика бумажного и электронного документооборота, проверка своевременного прохождения всех этапов документооборота, наблюдение за движением документов. Проверка наличия всех необходимых подписей на документах, в том числе ЭЦП
Права доступа к программам	Случайное или умышленное искажение данных в результате некорректного распределения прав доступа	Проверка правильности разграничения обязанностей по вводу данных в программу и текущему контролю. Проверка наличия у лиц права доступа к программам, на установление изменений и замен. Проверка информационной поддержки и безопасности в отношении прав доступа к программам, их изменение, санкционирование. Проверка применения локальной сети, аппаратных и программных средств для разграничения доступа
Информационная поддержка и безопасность	Риск ошибок, использование устаревшего законодательства, неверных настроек программ, нарушения целостности и	Проверка наличия и полноты Положения об информационной безопасности, ознакомление с ним сотрудников. Применение программного обеспечения, позволяющего своевременно устранять попытки несанкционированного доступа. Оценка соблюдения законодательства

	безопасности, стороннего вмешательства и фактов мошенничества, кибератак	и стандартов в сфере интернет-торговли, бухгалтерского и налогового законодательства. Проверка соответствия информации о ценах на сайте и в заказах, правомерности применения системы скидок и акций. Соответствие веб-сайта целевым установкам, оценка дизайна сайта, его особенностей навигации. Наличие и функционирование программы восстановления коммерческих операций, применение способов защиты от сбоев. Обеспечение конфиденциальности применяемых кодов и паролей, невозможности применения ЭЦП другим лицом. Контроль за обеспечением безопасного хранения и обработки данных, предотвращение их передачи третьим лицам, наличие письменного согласия на обработку персональных данных. Контроль идентификации электронных платежей и защита информации, соблюдения правил электронных платежных систем. Проверка обнаружения и определения фактора ошибок в IT-системе, идентификации подозрительных сделок. Оценка своевременности поддержки и обновления программных продуктов, их бесперебойного функционирования. Проверка наличия системы криптографической и антивирусной защиты информации. Проверка возможности программы «не пропускать» оформление заказа и платежа без заполнения всех необходимых реквизитов. Оценка взаимосвязи с потенциальными потребителями, поиск посетителей сайта, определение «ненадежных» покупателей. Оценка соблюдения правил осуществления персонифицированных платежей Закону о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Проверка целостности информации о бизнес-операциях
Применение средств автоматизированного контроля	Ошибки, сомнительные бухгалтерские записи, умышленные искажения в программе	Автоматизированный контроль непроведенных документов. Минимизация слабоконтролируемых операций (введенных вручную, корректировок). Проверка соблюдения дат, хронологической последовательности торговых операций. Проверка соблюдения контрольных соотношений с помощью программных средств. Автоматическое обнаружение и исправление ошибки прикладными средствами контроля. Контроль правильности расчетов с помощью процедур программных проверок.

		Применение программных методов аутентификации и авторизации. Работа контрольных модулей систем и самодиагностика программных средств
Ввод и обработка информации	Некорректный ввод информации	Проверка отсутствия дублирования данных. Оценка точности и полноты при хранении информации и передачи между компонентами информационной системы. Проверка правильности ввода и обработки информации
Мониторинг за состоянием АИС	Отсутствие или затруднение в проведении мониторинговых процедур	Оценка порядка внесения изменения в базы данных, их санкционирования. Оценка уязвимости системы от внутренних и внешних угроз. Проверка периодичности осуществления контроля за полнотой и своевременностью ввода информации. Анализ протоколов действий в IT-системе
Квалификация операционных работников	Риск некорректного ввода и обработки данных. Затруднения обработки данных при изменениях документов, бизнес-операций	Подготовка, повышение квалификации и самообучение сотрудников программным продуктам. Наличие пользовательской, методической, технической документации для работы в IT-системе. Ознакомление сотрудников с изменениями, вносимыми в программный продукт. Консультирование работников по вопросам использования программного обеспечения
Контроль экспорта-импорта информации	Риск существенного искажения данных в случае потери информации или несвоевременной выгрузки данных	Оценка периодичности загрузки/выгрузки данных. Установление лиц, ответственных за загрузку/выгрузку данных, их права и компетентность. Применение типовых механизмов для загрузки/выгрузки данных. Проверка внесения изменений в загруженные/выгруженные данные, выявление причин корректировок. Проверка наличия контроля за загрузкой/выгрузкой и сверкой данных между компонентами программ. Проверка на конец отчетного периода соответствия между обмениваемыми данными. Оценка корректности периода и настроек при загрузке/выгрузке данных, соответствие между данными

Источник: авторская разработка

Source: Authoring

Рисунок 1

Динамика интернет-торговли России на внутреннем и трансграничном рынках в 2010–2021 гг.

Figure 1

Online trade trends in Russia in the domestic and cross-border markets, 2010–2021



Примечание. 2021 г. – прогнозное значение.

Источник: составлено авторами по данным Ассоциации компаний интернет-торговли (АКИТ). URL: <http://akit.ru>

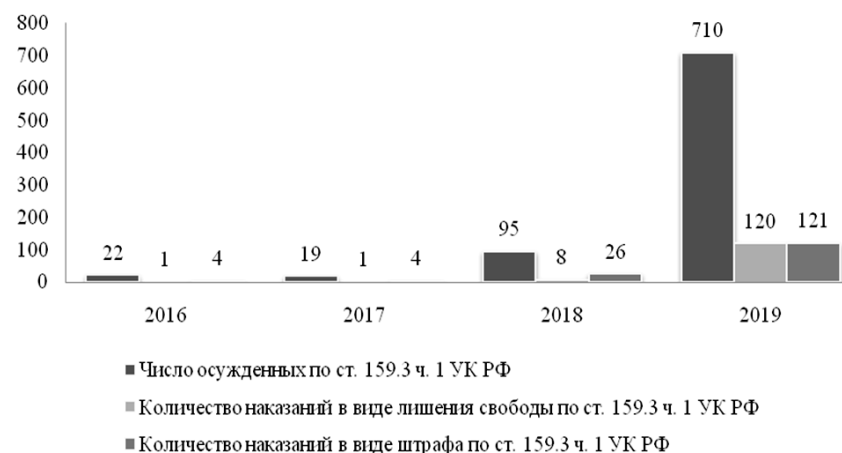
Source: Authoring based on Association of Internet Trade Companies (AITC). URL: <http://akit.ru> (In Russ.)

Рисунок 2

Мошенничество в системе использования электронных средств платежа в России, 2016–2019 гг.

Figure 2

Fraud in electronic means of payment in Russia, 2016–2019



Источник: Судебная статистика РФ. URL: <http://stat.апи-пресс.рф/>

Source: Russian Judicial Statistics. URL: <http://stat.апи-пресс.рф/> (In Russ.)

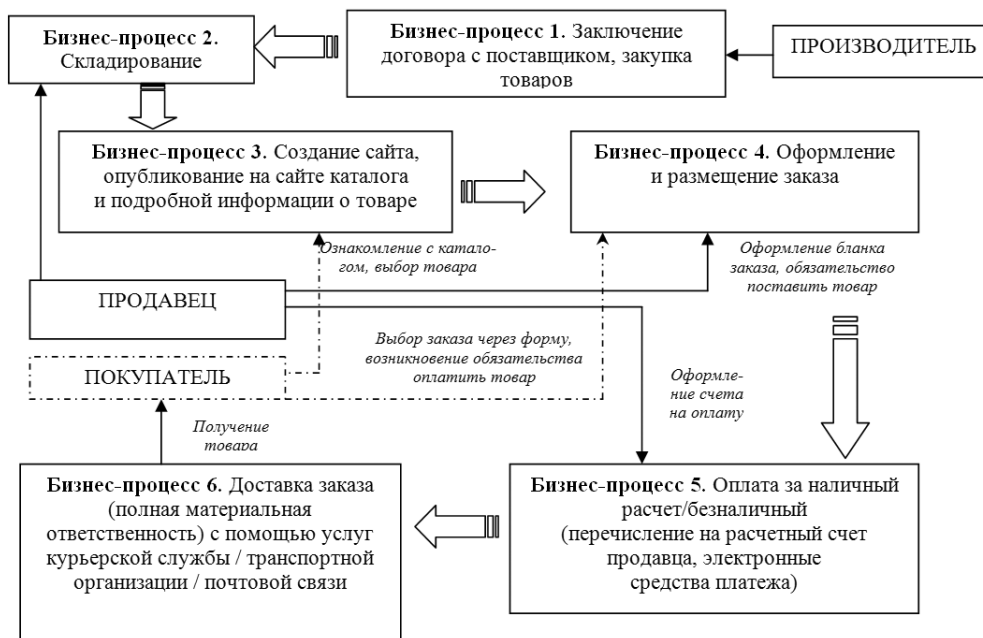
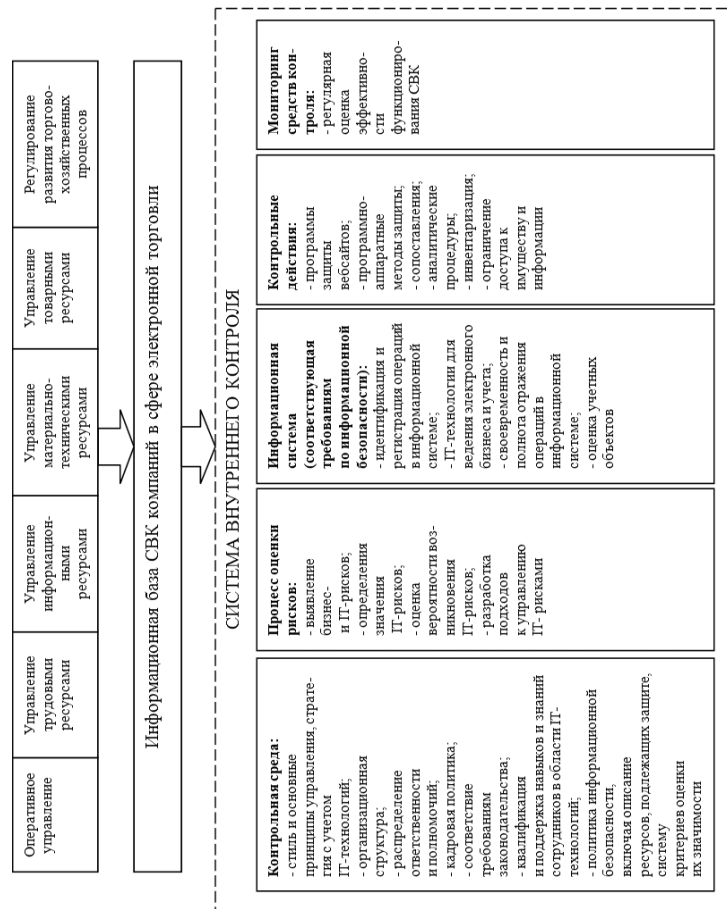
Рисунок 3**Динамика штрафных санкций, налагаемых на предприятия торговли в 2016–2019 гг.****Figure 3****Trends in penalties imposed on trade enterprises, 2016–2019***Источник:* Судебная статистика РФ. URL: <http://stat.api-пресс.рф/>*Source:* Russian Judicial Statistics. URL: <http://stat.api-пресс.рф/> (In Russ.)**Рисунок 4****Бизнес-процессы в сфере электронной торговли (B2C)****Figure 4****Business processes in electronic commerce (B2C)***Источник:* авторская разработка*Source:* Authoring

Рисунок 5
Система внутреннего комплаенс-контроля компаний электронной торговли
Figure 5
The internal compliance control system for e-commerce businesses



Источник: авторская разработка

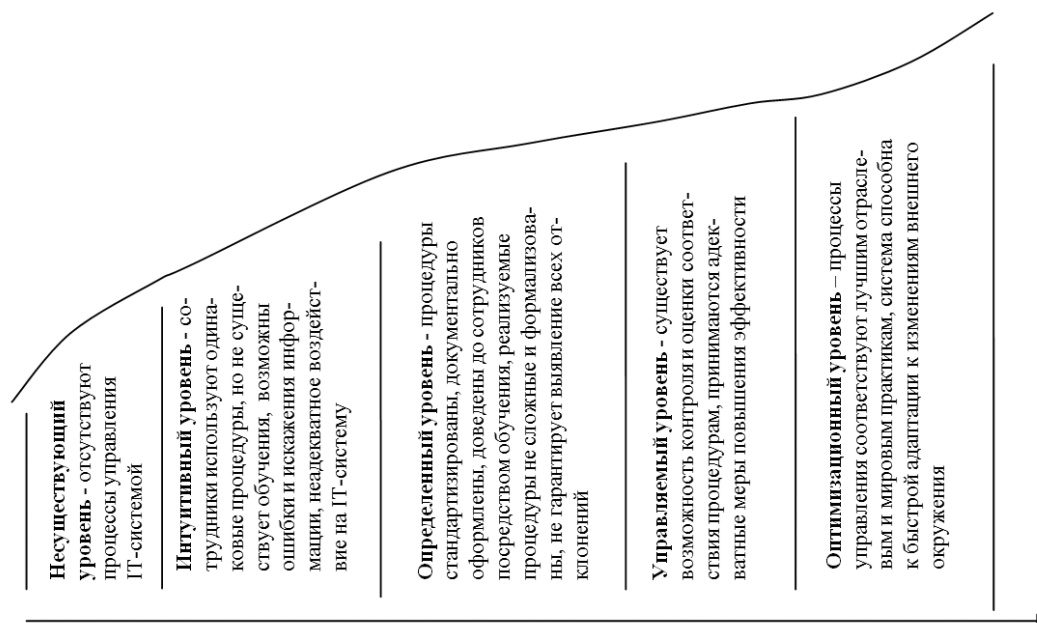
Source: Authoring

Рисунок 6

Информационная система компаний электронной торговли по стадиям зрелости

Figure 6

The information system of e-commerce businesses by maturity



Источник: авторская разработка

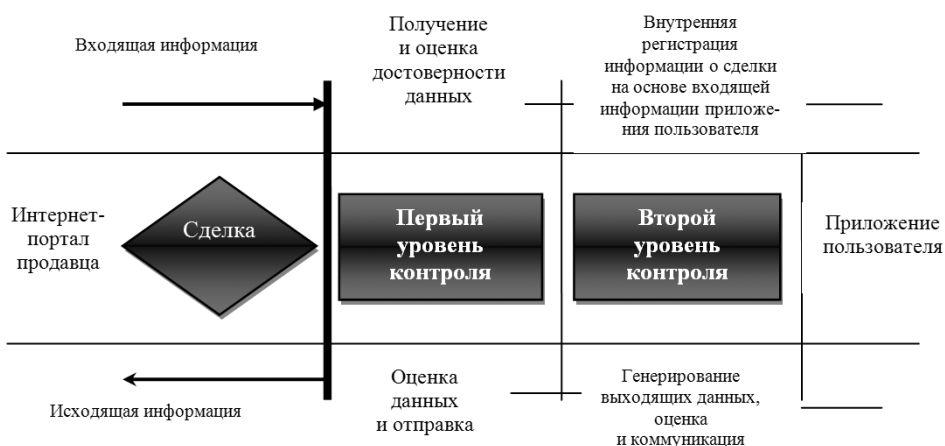
Source: Authoring

Рисунок 7

Процедуры внутреннего комплаенс-контроля сделок в электронной торговле

Figure 7

Internal compliance control procedures for e-commerce deals



Источник: авторская разработка

Source: Authoring

Список литературы

1. *Ревина С.Ю.* Тенденции и перспективы российской электронной коммерции // Вестник РУДН. Сер. Экономика. 2017. Т. 25. № 4. С. 487–497. URL: <https://doi.org/10.22363/2313-2329-2017-25-4-487-497>
2. *Салихова Р.Р.* Сущность, факторы и проблемы развития электронной торговли в России // Вестник экономики, права и социологии. 2020. № 2. С. 34–38. URL: <https://cyberleninka.ru/article/n/suschnost-factory-i-problemy-razvitiya-elektronnoy-torgovli-v-rossii/viewer>
3. *Беляцкая Т.Н.* Экосистема электронных рынков и факторы, ее определяющие // Научно-технические ведомости СПбГПУ. Экономические науки. 2017. Т. 10. № 6. С. 9–17. URL: <https://doi.org/10.18721/JE.10601>
4. *Романцов М.С.* Тенденции развития электронного бизнеса в России // Социально-экономические явления и процессы. 2017. Т. 12. № 4. С. 43–48. URL: <https://cyberleninka.ru/article/n/tendentsii-razvitiya-elektronnogo-biznesa-v-rossii/viewer>
5. *Медведев Г.Г., Касаев Б.С.* К вопросу развития электронного бизнеса в России // Инновации и инвестиции. 2018. № 4. С. 206–209.
6. *Никитюк Л.Г., Тимчук О.Г.* Роль электронной коммерции в развитии инновационной экономики // Вестник НГУЭУ. 2018. № 3. С. 180–193. URL: <https://cyberleninka.ru/article/n/rol-elektronnoy-kommertsii-v-razviti-innovatsionnoy-ekonomiki/viewer>
7. *Аксенова Ж.А., Ищенко О.В., Леошко В.П.* Особенности ведения внутреннего контроля в торговой организации // Вестник Академии знаний. 2019. № 3. С. 31–35.
8. *Николаева А.А.* Реализация комплаенс-функции в промышленности // Известия Санкт-Петербургского государственного экономического университета. 2016. № 1. С. 126–130. URL: <https://cyberleninka.ru/article/n/realizatsiya-komplpaens-funksii-v-promyshlennosti/viewer>
9. *Чирков Д.А.* Основы развития комплаенс-контроля в кредитных организациях // Экономика и бизнес: теория и практика. 2019. № 12-3. С. 141–144. URL: <https://doi.org/10.24411/2411-0450-2019-11536>
10. *Кеворкова Ж.А., Сапожникова Н.Г.* Концептуальные положения комплаенс как формы внутреннего контроля в экономических субъектах // Учет. Анализ. Аудит. 2020. Т. 7. № 2. С. 6–16. URL: <https://doi.org/10.26794/2408-9303-2020-7-2-6-16>

11. *Назаров А.А., Иванова В.И.* Электронная торговля как инструмент повышения качества взаимодействия государства, бизнеса и общества // *Oeconomia et Jus*. 2016. № 2. С. 1–8.
URL: <https://cyberleninka.ru/article/n/elektronnaya-torgovlya-kak-instrument-povysheniya-kachestva-vzaimodeystviya-gosudarstva-biznesa-i-obschestva/viewer>
12. *Филин С.А., Шуай Лю.* Управление электронными сетевыми структурами в торговле (на примере КНР) // *Национальные интересы: приоритеты и безопасность*. 2018. Т. 14. Вып. 11. С. 2116–2129.
URL: <https://doi.org/10.24891/ni.14.11.2116>
13. *Самусев Н.С., Павлова Е.И.* Организация доставки грузов для интернет-торговли с учетом возвратов // *Государственное и муниципальное управление. Ученые записки*. 2019. № 3. С. 78–84. URL: <http://upravlenie.uriu.ranepa.ru/wp-content/uploads/2019/09/78-84-1.pdf>
14. *Устинова Н.Г.* Цифровая экономика и предпринимательство: вопросы взаимодействия // *Вестник СГСЭУ*. 2019. № 3. С. 32–37.
URL: <https://cyberleninka.ru/article/n/tsifrovaya-ekonomika-i-predprinimatelstvo-voprosy-vzaimodeystviya/viewer>
15. *Быстрова Н.В., Максимова К.А.* Электронная коммерция и перспективы ее развития // *Инновационная экономика: перспективы развития и совершенствования*. 2018. Т. 1. № 7. С. 86–90.
16. *Погорлецкий А.И.* Налогообложение трансграничных операций электронной коммерции: особенности, проблемы и возможности // *Вестник Томского государственного университета. Экономика*. 2019. № 46. С. 229–250. URL: <https://doi.org/10.17223/19988648/46/16>
17. *Коваль А.А., Леващенко А.Д.* Защита потребителей в электронной торговле // *Российский внешнеэкономический вестник*. 2018. № 7. С. 99–104. URL: <https://cyberleninka.ru/article/n/zaschita-potrebiteley-v-elektronnoy-torgovle/viewer>
18. *Якимова В.А.* Обоснование роли комплаенс-контроля общественно значимых организаций с позиции институциональной экономической теории // *Вестник Пермского университета. Сер. Экономика*. 2017. Т. 12. № 4. С. 542–560. URL: <https://doi.org/10.17072/1994-9960-2017-4-542-560>
19. *Батаева Б.С., Черепанова В.А.* Перспективы развития комплаенса как средства улучшения корпоративного управления в российских компаниях // *Экономика. Налоги. Право*. 2017. Т. 10. № 5. С. 30–36.
URL: <https://cyberleninka.ru/article/n/perspektivy-razvitiya-komplaensa-kak-sredstva-uluchsheniya-korporativnogo-upravleniya-v-rossiyskih-kompaniyah/viewer>

20. *Шишкин И.А., Хацкевич В.Л., Хацкевич Л.Д.* Электронный бизнес и менеджмент интернет-проектов // *Современные технологии обеспечения гражданской обороны и ликвидации последствий чрезвычайных ситуаций*. 2016. № 12. С. 134–137.
URL: <https://cyberleninka.ru/article/n/elektronnyy-biznes-i-menedzhment-internet-proektov/viewer>
21. *Якимова В.А.* Оценка внутреннего контроля расчетов с персоналом по оплате труда в условиях применения аудируемым лицом автоматизированной информационной системы // *Международный бухгалтерский учет*. 2016. Т. 19. Вып. 22. С. 27–43.
URL: <https://cyberleninka.ru/article/n/otsenka-vnutrennego-kontrolya-raschetov-s-personalom-po-oplate-truda-v-usloviyah-primeneniya-avtomatizirovannoy-1/viewer>

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

pISSN 2073-2872
eISSN 2311-875X

Economic Security

COMPLIANCE CONTROL AS A MECHANISM FOR ENSURING THE ECONOMIC SECURITY OF BUSINESSES IN E-COMMERCE

Vilena A. YAKIMOVA ^{a,*},
Viktor S. RADOMSKII ^b

^a Amur State University (AmSU),
Blagoveshchensk, Russian Federation
vilena_yakimova@mail.ru
<https://orcid.org/0000-0001-5866-5652>

^b OOO KOMP,
Moscow, Russian Federation
vitek1715@yandex.ru
ORCID: not available

* Corresponding author

Article history:

Article No. 259/2021
Received 10 May 2021
Received in revised
form 26 May 2021
Accepted 11 June 2021
Available online
16 August 2021

JEL classification:

F23, G32, M42

Keywords: digital
economy, e-business,
e-commerce, IT risk,
information system,
internal compliance
control system

Abstract

Subject. The article focuses on organizational and methodological issues of internal compliance control in e-commerce businesses.

Objectives. We refine the design and technique of internal compliance control for e-commerce businesses.

Methods. The study relies upon methods of analysis and generalization, grouping, systematization, risk-based, systems and business process approaches.

Results. We devised the five-component compliance control system, determined its principles and functions ensuring the economic security of e-commerce businesses. We suggest conducting compliance procedures intended to mitigate IT risks and accounting for the specifics of e-commerce business processes.

Conclusions and Relevance. In e-commerce, compliance control serves for identifying and monitoring compliance risks, ensuring safe operations of businesses, which is vital for people. The information system for IT risk protection was found to underlie compliance control, while control procedures can be classified into general and applied. The findings can be used to set up a reliable and effective compliance system for e-commerce businesses in order to prevent economic abuses and crime.

© Publishing house FINANCE and CREDIT, 2021

Please cite this article as: Yakimova V.A., Radomskii V.S. Compliance Control as a Mechanism for Ensuring the Economic Security of Businesses in E-Commerce. *National Interests: Priorities and Security*, 2021, vol. 17, iss. 8, pp. 1491–1518.
<https://doi.org/10.24891/ni.17.8.1491>

References

1. Revinova S.Yu. [Russian e-commerce: Trends and prospects]. *Vestnik RUDN. Ser. Ekonomika = RUDN Journal of Economics*, 2017, vol. 25, no. 4, pp. 487–497. (In Russ.)
URL: <https://doi.org/10.22363/2313-2329-2017-25-4-487-497>
2. Salikhova R.R. [Essence, factors and problems of electronic commerce development in Russia]. *Vestnik ekonomiki, prava i sotsiologii = The Review of Economics, the Law and Sociology*, 2020, no. 2, pp. 34–38.
URL: <https://cyberleninka.ru/article/n/suschnost-factory-i-problemy-razvitiya-elektronnoy-torgovli-v-rossii/viewer> (In Russ.)
3. Belyatskaya T.N. [Ecosystem of electronic markets and its determinants]. *Nauchno-tekhnicheskie vedomosti SPbGPU. Ekonomicheskie nauki = St. Petersburg State Polytechnical University Journal. Economics*, 2017, vol. 10, no. 6, pp. 9–17. (In Russ.) URL: <https://doi.org/10.18721/JE.10601>
4. Romantsov M.S. [Tendencies of development of electronic business in Russia]. *Sotsial'no-ekonomicheskie yavleniya i protsessy = Socio-Economic Phenomena and Processes*, 2017, vol. 12, no. 4, pp. 43–48.
URL: <https://cyberleninka.ru/article/n/tendentsii-razvitiya-elektronnogo-biznesa-v-rossii/viewer> (In Russ.)
5. Medvedev G.G., Kasaev B.S. [On the development of e-business in Russia]. *Innovatsii i investitsii = Innovation and Investment*, 2018, no. 4, pp. 206–209. (In Russ.)
6. Nikityuk L.G., Timchyuk O.G. [The role of e-commerce in the development of innovative economy]. *Vestnik NGUEU = Vestnik NSUEM*, 2018, no. 3, pp. 180–193. URL: <https://cyberleninka.ru/article/n/rol-elektronnoy-kommertsii-v-razvitii-innovatsionnoy-ekonomiki/viewer> (In Russ.)
7. Aksenova Zh.A., Ishchenko O.V., Leoshko V.P. [Features of conducting internal control in a trade organization]. *Vestnik Akademii znanii = Academy of Knowledge Bulletin*, 2019, no. 3, pp. 31–35. (In Russ.)
8. Nikolaeva A.A. [The implementation of the compliance function in the industry]. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta = Bulletin of Saint Petersburg State University of Economics*, 2016, no. 1, pp. 126–130. URL: <https://cyberleninka.ru/article/n/realizatsiya-komplpaens-funktsii-v-promyshlennosti/viewer> (In Russ.)
9. Chirkov D.A. [Basics of the development of compliance control in credit organizations]. *Ekonomika i biznes: teoriya i praktika = Economy and Business: Theory and Practice*, 2019, no. 12-3, pp. 141–144. (In Russ.)
URL: <https://doi.org/10.24411/2411-0450-2019-11536>

10. Kevorkova Zh.A., Sapozhnikova N.G. [Conceptual provisions of compliance as a form of internal control in economic entities]. *Uchet. Analiz. Audit = Accounting. Analysis. Auditing*, 2020, vol. 7, no. 2, pp. 6–16. (In Russ.)
URL: <https://doi.org/10.26794/2408-9303-2020-7-2-6-16>
11. Nazarov A.A., Ivanova V.I. [E-commerce as a way to improve the quality of interaction between the State, business and society]. *Oeconomia et Jus*, 2016, no. 2, pp. 1–8. URL: <https://cyberleninka.ru/article/n/elektronnaya-torgovlya-kak-instrument-povysheniya-kachestva-vzaimodeystviya-gosudarstva-biznesa-i-obschestva/viewer> (In Russ.)
12. Filin S.A., Shuai Lyu [Management of electronic network structures in trade: Evidence from the People's Republic of China]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2018, vol. 14, iss. 11, pp. 2116–2129. (In Russ.)
URL: <https://doi.org/10.24891/ni.14.11.2116>
13. Samusev N.S., Pavlova E.I. [Organization of goods delivery supply chains in online trade considering return of goods]. *Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski = State and Municipal Management. Scholar Notes*, 2019, no. 3, pp. 78–84. URL: <http://upravlenie.uriu.ranepa.ru/wp-content/uploads/2019/09/78-84-1.pdf> (In Russ.)
14. Ustinova N.G. [Digital Economy and Entrepreneurship: Problems of Interaction]. *Vestnik SGSEU = Bulletin of Saratov State Socio-Economic University*, 2019, no. 3, pp. 32–37.
URL: <https://cyberleninka.ru/article/n/tsifrovaya-ekonomika-i-predprinimatelstvo-voprosy-vzaimodeystviya/viewer> (In Russ.)
15. Bystrova N.V., Maksimova K.A. [Electronic commerce and prospects for its development]. *Innovatsionnaya ekonomika: perspektivy razvitiya i sovershenstvovaniya = Innovative Economy: Prospects for Development and Improvement*, 2018, vol. 1, no. 7, pp. 86–90. (In Russ.)
16. Pogorletskii A.I. [Taxation of cross-border e-commerce transactions: Features, problems and opportunities]. *Vestnik Tomskogo gosudarstvennogo universiteta. Ekonomika = Tomsk State University Journal of Economics*, 2019, no. 46, pp. 229–250. (In Russ.)
URL: <https://doi.org/10.17223/19988648/46/16>
17. Koval' A.A., Levashenko A.D. [Consumer protection in electronic commerce]. *Rossiiskii vneshneekonomicheskii vestnik = Russian Foreign Economic Bulletin*, 2018, no. 7, pp. 99–104.
URL: <https://cyberleninka.ru/article/n/zaschita-potrebiteley-v-elektronnoy-torgovle/viewer> (In Russ.)

18. Yakimova V.A. Substantiation of a compliance control of socially significant organizations on the institutional theory basis. *Vestnik Permskogo universiteta. Ser. Ekonomika = Perm University Herald. Economy*, 2017, vol. 12, no. 4, pp. 542–560. (In Russ.)
URL: <https://doi.org/10.17072/1994-9960-2017-4-542-560>
19. Bataeva B.S., Cherepanova V.A. [Compliance as a means of improving corporate governance in Russian companies and its development prospects]. *Ekonomika. Nalogi. Pravo = Economics, Taxes & Law*, 2017, vol. 10, no. 5, pp. 30–36. URL: <https://cyberleninka.ru/article/n/perspektivy-razvitiya-komplaensa-kak-sredstva-uluchsheniya-korporativnogo-upravleniya-v-rossiyskih-kompaniyah/viewer> (In Russ.)
20. Shishkin I.A., Hatskevich V.L., Hatskevich L.D. [Electronic business and internet project management]. *Sovremennye tekhnologii obespecheniya grazhdanskoi oborony i likvidatsii posledstviy chrezvychaynykh situatsii = Modern Civil Defence and Emergency Technologies*, 2016, no. 1-2, pp. 134–137. URL: <https://cyberleninka.ru/article/n/elektronnyy-biznes-i-menedzhment-internet-proektov/viewer> (In Russ.)
21. Yakimova V.A. [Assessing the internal controls over payroll settlements using the automaed data processing by the auditee]. *Mezhdunarodnyi bukhgalterskii uchet = International Accounting*, 2016, vol. 19, iss. 22, pp. 27–43.
URL: <https://cyberleninka.ru/article/n/otsenka-vnutrennego-kontrolya-raschetov-s-personalom-po-oplate-truda-v-usloviyah-primeneniya-audiruemym-litsom-avtomatizirovannoy-1/viewer> (In Russ.)

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.