УДК 346.5

Орлова Марина Гарръевна
Кандидат педагогических наук Доцент
Доцент кафедры «Экономическая теория и антикризисное управление»
Сибирский государственный университет путей сообщения
г. Новосибирск, Россия
formargar@mail.ru
Orlova Marina Garryevna
Candidate of of Pedagogical Sciences Associated Professor
Associate Professor of the Depart."Economic Theory and Crisis Management"
Siberian Transport University, Novosibirsk, Russia
formargar@mail.ru

ПРОБЛЕМА ЦИФРОВИЗАЦИИ СФЕРЫ КОМПЛАЕНС
THE PROBLEM OF DIGITALIZATION OF THE COMPLIANCE SPHERE

Аннотация. В статье рассмотрены аспекты цифрового комплаенса как эффективного инструмента экономической безопасности и управления рисками. Анализ формирования комплаенс-политики в российской бизнес-среде показал необходимость его дальнейшего развития и совершенствования. Изучение опыта обязательного применения цифрового комплаенса в финансовой сфере послужило поводом для сравнения успехов нефинансовых организаций по соблюдению требований регулятора. Предположение о дальнейшем проникновении цифрового комплаенса в нефинансовый сектор экономики подтверждается очевидными примерами применения цифровых инструментов в соответствии с Руководством по цифровому комплаенсу и Руководству должной осмотрительности для ответственного ведения бизнеса в различных сферах (ОЭСР). Предложены решения по цифровому комплаенсу для российских компаний с учетом направлений его реализации, которые могут быть автоматизированы. Проблема внедрения цифрового комплаенса сопряжена с требованиями регулятора и зависит от потенциала IT-разработчиков.

Ключевые слова: комплаенс, риски соответствия, законодательство, цифровые, технологии, автоматизация.

Abstract. The article discusses aspects of digital compliance as an effective tool for economic security and risk management. Analysis of the formation of compliance policy in the Russian business environment has shown the need for its further development and improvement. The study of the experience of mandatory application of digital compliance in the financial sector served as an occasion to compare the success of non-financial organizations in compliance with the requirements of the regulator. The assumption of further penetration of digital

compliance into the non-financial sector of the economy is confirmed by obvious examples of the use of digital tools in accordance with the Digital Compliance Manual and the Due Diligence Manual for Responsible Business in Various Fields (OECD). Solutions on digital compliance for Russian companies are proposed, taking into account the directions of its implementation, which can be automated. The problem of implementing digital compliance is associated with the requirements of the regulator and depends on the potential of IT developers.

Key words: compliance, compliance risks, legislation, digital, technology, automation.

В современных условиях распространения цифровых сервисов в различных сферах экономики особое значение приобретает соблюдение стандартов в области информационной безопасности и обеспечения сохранности личных данных. Инструментом, помогающим обеспечить соответствие регуляторным требованиям, является комплаенс. Однако проникновение современных цифровых технологий в эту сферу опережает соответствующую реакцию регулятора на использование потенциала цифры в своей контрольно-надзорной детальности [1].

Сфера комплаенс распространяется на финансовые и нефинансовые организации. Необходимость соответствия требованиям законодательства по противодействию легализации доходов, полученных преступным путем (115-ФЗ, 2001 г.) первыми испытали на себе финансовые организации, кроме того, комплаенс получил свое развитие именно в банковской сфере (1998 г.). Противодействие коррупции должны осуществлять все организации, независимо от целей деятельности, поэтому комплаенс стал проникать в различные сферы экономики, дифференцированно проявляясь в своих формах и методах [12]. Актуальность комплаенса подтвердилась после принятия поправок к закону РФ о конкуренции, что официально закреплено в соответствующем нормативном акте об антимонопольном комплаенсе (2020 г.). Предоставление отчетности регулятору со стороны фирм, участников рыночных операций было возложено на специальные подразделения по комплаенсу [3, 5, 12].

Анализ формирования комплаенс-политики в российской бизнес-среде выявил следующие факты [1,3,10].

1. Наличие «ручного» анализа финансовых операций, проводился в России в конце XX века. Это была основа комплаенса по определению соответствия или несоответствия требованиям регулятора. Элементы информатизации проявляли себя в части оформления (записи) «ручных» отчетов на электронный носитель в виде дискет или дисков. При этом процесс передачи таких отчетов занимал целые сутки. Но современные цифровые технологии проникают во все сферы человеческой жизни, и комплаенс не исключение.

2. Развитие информационных технологий, в т.ч. цифровых. Известно, что под цифровыми технологиями как правило понимается информационная технология, которая основана на методах шифрования, передачи, обработки и сохранения данных за относительно короткие отрезки времени. Технологические изменения информационной бизнес-среды стали драйвером проникновения IT-технологий в деятельность прежде всего финансовых организаций, которые стали предлагать цифровые продукты, мобильный банкинг и дистанционное обслуживание. Однако, Россия в этом вопросе уступила лидерство Китаю, который стремительно развивает сферу цифрового банкинга и готов полностью избавиться от бумажных денег к 2024 году.

3. Возрастающие требования регулятора. Банк России за последние десять лет (с 2012 г.) увеличил число своих требований к финансовым организациям примерно в восемь раз. За несоблюдение требований к финансовой отчетности и 115-ФЗ ежегодно отзывается около сотни лицензий. Для понимания этих требований и контроля за их соблюдением кредитные организации должны осуществлять большое количество комплаенс-операций по проверке бенефициарных собственников; оценке рисков обслуживания корпоративных клиентов, предотвращение сомнительных операций, транзитных схем и др. Без применения цифровых технологий финансовые организации не смогли бы обслуживать своих клиентов корректно требованиям.

4. Возрастающая роль комплаенс объединений. По оценкам экспертов Национальной Ассоциации Комплаенс (РФ) 2020 год стал знаковым в области цифровизации комплаенса, поскольку массовое внедрение IT-продуктов и постепенное превалирование электронного контроля над бумажным дало свои положительные результаты. Пришло осознание того, что ручной комплаенс-контроль в бизнесе – это дорогой метод, не исключающий комплаенс-рисков (ошибки по причине человеческого фактора, коррупция, коммуникации и др.) [5, 11]. Автоматизация является более эффективным и по итогу менее затратным методом контроля и предотвращения комплаенс-рисков [11]. За счет технология big data обработка больших массивов неструктурированной информации стало возможной и не в финансовой сфере: комплаенс-специалисты получили доступ к цифровым инструментам в других сферах экономики.

Таким образом, можно выделить 6 основных комплаенс-направлений в деятельности бизнеса, которые в современных условиях существовать просто не смогут без использования IT-технологий или цифровых инструментов [7, 8]:

1) проверка контрагентов на честность и прозрачность (оценка финансовой устойчивости, выявление партнерских и репутационных рисков);
2) обеспечение работы «Горячей линии» для информирования и обратной связи с целевыми аудиториями;
3) трудовые отношения и внутренние регламенты;

4) проверка партнеров и контрагентов на присутствие в санкционных списках [12];

5) выявление конфликта интересов (связи персонала с контрагентами, с госорганами; лоббирование);

6) коммуникации в общественной среде (пресс-служба, соблюдение требований со стороны топ-менеджмента).

Для указанных направлений сегодня уже созданы и доступны для применения инструменты автоматизированного решения комплаенс-вопросов. Эти инструменты можно также разделить на группы [8,10]:

1) платформы для принятия на обслуживание клиентов;

2) платформы для ведения анкет клиентов и выполнения требования KYC (Know Your Client — «Знай своего клиента»);

3) скрининговые решения для проверки благонадежности контрагентов;

4) платежные программы для проверки платежей при их отправке;

5) решения для выявления сомнительных операций и отправки отчетности (AML software).

Однако, для решения внутренних проблем по соблюдению сотрудниками компании регламентов, кодексов подобных платформ создано недостаточно. Если открытость эмитентов можно проследить через "Единое окно раскрытия корпоративной информации" – совместный проект Национального расчетного депозитария (НРД) и Интерфакса, поддержанный Банком России, то закрытость корпорации остается «закрытым» вопросом [2]. Возможно, это потребует серьезных вложений и времени для апробации.

Итак, можно свидетельствовать, что комплаенс стал цифровым. Основная сложность заключается в том, что автоматизированные системы в большей части не интегрированы между собой, не достаточно гибки к регуляторным изменениям. Это является главным тормозом на пути развития цифрового комплаенса, т.к. связано с серьезными затратами на его модернизацию.

Цифровой комплаенс важен для всех компаний, и для крупных компаний и не только. Цифровой комплаенс важен для развития электронной коммерции, которая обеспечивает возможность онлайн-покупки товаров и услуг. Например, внедрение цифрового комплаенса позволяет отслеживать сомнительные транзакции, а также обеспечивать фактический объем транзакций в сфере электронной коммерции.

Очевидно, что для IT-бизнеса цифровизация комплаенс-процедур необходима. Риск, связанный с инцидентами в области цифровой безопасности, вошел в пятерку глобальных бизнес-рисков 2022 года: второе место после ненулевого COVID [8].

В условиях цифровой экономики киберпреступность, сбои в работе IT-инфраструктуры, утечки данных могут парализовать работу любой компании. Стоимость типичного инцидента цифровой безопасности составляет

около 200 000 дол. США (примерно столько же, сколько годовой бюджет фирмы на IT-безопасность), и это около 0,4% от предполагаемого годового дохода компании [1,3].

Важно заметить, что IT-компаниям, работающим в цифровом мире, нельзя думать, что комплаенс ограничивается вопросами цифровых рисков. Диапазон рисков в IT- инфраструктуре полностью включается в сферу комплаенс-рисков. Особенно остро стоит вопрос о соблюдении IT-бизнесом прав человека [6].

Организацией экономического сотрудничества и развития (ОЭСР) в 2018 г. было принято Руководство должной осмотрительности о том, какие практические шаги компания должна сделать для внедрения стандартов ответственного ведения бизнеса [4,6]. Для внедрения цифрового комплаенса с учетом данного руководства в переводе на отечественную специфику бизнеса (в любой сфере, не только IT) можно рекомендовать следующие шаги [4,9]:

1) Принять специальный документ – Политику ответственного поведения, направленную на определение и устранение ключевых рисков. Внедрение, например, системы устойчивости в российской компании 1С помогает определить шаги, предпринимаемые компанией по обеспечению конфиденциальности и безопасности данных.

2) Сформировать систему оценки потенциальных и фактических рисков проекта. Например, компания «Галактика» проводит комплексную оценку рисков компании за счет использования современных технологий и проведения опроса около 150 Топ-менеджеров компании.

3) Разработать меры по предотвращению и смягчению последствий после определения рисков. Так, компания «Контур» приняла программу в области прав человека и ответственного выбора поставщиков, которая включает меры по процедурам должной осмотрительности в отношении поставки конфликтных минералов.

4) Оценивать меры по снижению комплаенс-рисков, оценивать результаты этих мер. Например, ОАО «РЖД» применяет комплексный подход к управлению комплаенс-рисками (включая вопросы минимизации рисков нарушения неприкосновенности частной жизни и цифровой безопасности, обеспечения прозрачности транзакций) и использует механизм обратной связи для повышения качества работы [5].

5) Взаимодействовать с общественностью через специальные мероприятия: ежегодные доклады предприятия об устойчивости или корпоративной ответственности или другие формы раскрытия информации. Сбер ежегодно готовит отчет о корпоративной ответственности, в котором раскрывает результаты политики в области ответственного ведения бизнеса.

6) Принимать меры по восстановлению в случае наступления негативного воздействия (в случае необходимости). Для того чтобы минимизировать возможные риски. Рекомендуется использовать механизм

страхования кибер-рисков. Для того чтобы оценить внедрение компанией цифрового комплаенса, рекомендуются специальные опросники [9].

В Руководстве не используется термин «цифровой комплаенс», однако, суть рекомендаций сводится именно к нему, т.к. сформулированные правила внутренней политики, направленные на минимизацию рисков финансовых операций, цифровой безопасности, неприкосновенности частной жизни и других комплаенс-рисков, приобретают решающее значение в условиях цифровой экономики. Важно подчеркнуть, что перечисленные выше 6 шагов можно использовать для компаний – операторов железнодорожного транспорта.

Таким образом, проблема цифрового комплаенса должна решаться в двух аспектах: во-первых, внедрение и развитие цифрового комплаенса в компании возможно за счет использования современных IT-решений. Поэтому усиливается роль цифровых продуктов от IT бизнеса для сферы комплаенс. Использование технологий искусственного интеллекта позволяет выявлять финансовые и нефинансовые риски компаний. Во-вторых, российские IT-компании, которые предоставляют IT-продукты как на отечественном рынке или за рубежом, должны знать о требованиях ответственного ведения бизнеса. Решение это проблемы связано с активной позицией государства, которое берет на себя роль регулятора в сложных взаимоотношениях всех участников цифровой экономики.

Библиографический список

1. Головин С.В., Луценко М.С., Шендрикова О.О. Вопросы организации комплаенс-контроля в условиях цифровой экономики //Вестник Воронежского государственного университета. Серия: экономика и управление. 2021, № 2. С.15-26. Воронежский государственный университет. – URL: https://elibrary.ru/item.asp?id=46381046&ysclid=lg4qp0brwc9529853(дата обращения 02.04.2023).
2. Интерфакс. Interfax.ru//Сервер раскрытия корпоративной информации. – URL: https://www.e-disclosure.ru/# (дата обращения 21.03.2023).
3. Калмыкова С.В., Кобышева М.С., Сергеев Д.А. Цифровой комплаенс как фактор развития экономики региона. ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого //Российский экономический интернет-журнал. – URL: https://elibrary.ru/item.asp?id=42631321(дата обращения 11.03.2023).
4. Организация экономического сотрудничества и развития (ОЭСР)/ Руководство ОЭСР по должной осмотрительности в отношении ответственного ведения бизнеса, 2018 г. – URL: www.oecd.org/investment/ due-diligence-guidance-for-responsible-business-conduct.htm. (дата обращения 11.03.2023).
5. Орлова М.Г. Пространство расширения комплаенс/ / В сб. Проблемы антикризисного управления и экономического развития. Мат. V Междунар.

науч.-практ. конф. 12 ноября 2019 г., Новосибирск. Изд-во СГУПСа, 2020. – С. 104-109.
6. Отчет Центр Россия (РАНХиГС) - ОЭСР 2018: ОТЧЕТ Российского центра компетенций и анализа стандартов ОЭСР за 2018 г. – URL: https://www.ranepa.ru/images/News/2019-01/25-01-2019-oesr.pdf?ysclid=lg346et29g591032020. (дата обращения 05.04.2023).
7. Примаков Д. Санкционный комплаенс: обязательные элементы и возможные меры //Методический журнал. Международные банковские операции. 2020. №1. С. 26-31.
8. РБК: Тренды. Как технологии изменили сферу комплаенс. – URL: https://trends.rbc.ru/trends/innovation/5db0538a9a79474c280764e2 (дата обращения 28.03.2023).
9. Руководство по цифровому комплаенсу. Проект Центра Россия-ОЭСР РАНХиГС. – [Электронный ресурс]. – URL: https://www.ranepa.ru/images/News/2019-07/17-07-2019-rukovodstvo.pdf?ysclid=lfy1c2zojj923981819(дата обращения 30.03.2023).
10. Соленая В.М. Организация комплаенс-контроля в условиях цифровой экономики. Материалы XXIV международной научно-практической конференции // Наука и знание. Актуальные проблемы устойчивого экономического регионов России: правовые, аспекты развития и обеспечения безопасности. Социально-экономические и гуманитарные науки. / Под общей редакцией Л.А. Демидовой, Т.А. Куткович. Новороссийск. [Электронный ресурс]. – Издательство: Московский гуманитарно-экономический институт, Новороссийский филиал (Новороссийск). 2021. – URL: https://elibrary.ru/publisher_about.asp?pubsid=15610 (дата обращения 29.03.2023).
11. Цифровизация комплаенса. Национальная ассоциация комплаенса (НАК). – URL: https://compliance.su/info/articles/tsifrovizatsiya-komplaensa-usovershenstvovanie-tekhnologicheskikh-vozmozhnostey-sistemy/?sphrase_id=2935(дата обращения 28.03.2023).
12. Шорохов В.Е., Попов П.А. Противодействие коррупции в современной России: государственный и муниципальный уровень // Государственная власть и местное самоуправление. 2021. № 1. С. 53-57. DOI: 10.18572/1813-1247- 2021-1-53-5