

УДК 336.717

DOI: 10.34670/AR.2019.89.3.015

Организация системы комплаенса в области защиты персональных данных

Дадалко Василий Александрович

Доктор экономических наук,
профессор кафедры «Анализ рисков и экономическая безопасность»,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, Москва, просп. Ленинградский, 49;
e-mail: antikrizis1@bk.ru

Тимофеев Евгений Александрович

Студент,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, Москва, просп. Ленинградский, 49;
e-mail: timofeev.e.a@inbox.ru

Аннотация

Задачи: Определение значения комплаенс, определение термина «комплаенс обеспечения безопасности персональных данных», определение уровня актуальности комплаенс. **Методология:** Введение определения комплаенс, выделение элементов комплаенс, анализ моделей комплаенс-системы, рассмотрение общемирового опыта использования комплаенс, а также процедуры формирования системы комплаенс в компании. **Результаты:** Вопрос защиты персональных данных имеет особую важность. Для всех российских компаний работа с персональными данными является неотъемлемым элементом развития бизнеса. Таким образом, в связи с наметившейся тенденцией по ужесточению законодательства в сфере защиты персональных данных, организациям стоит обратить пристальное внимание на обеспечение превентивных мер в отношении противодействия утечке персональных данных. На сегодняшний день не существует четкого понятия термина «комплаенс-контроль», как и окончательного перечня того, чем должен заниматься комплаенс-менеджер, а чем – нет, что включает в себя комплаенс-функция. **Выводы:** Эффективная деятельность компании полностью зависит от отношения к персональным данным, с которыми функционирует работа. Нарушение системы защиты персональных данных может привести к непоправимым последствиям. Соблюдение законодательства о персональных данных – это комплекс мероприятий, реализация которых должна поддерживаться в компании на постоянной основе. Важно не только фиксировать во внутренних актах комплекс таких мер и способы их реализации, но в действительности их реализовывать. Также необходимо поддерживать внедрение и реализацию мер на постоянной основе и иметь доказательства того, что меры не являются декларативными и существующими только на бумаге.

Для цитирования в научных исследованиях

Дадалко В.А., Тимофеев Е.А. Организация системы комплаенса в области защиты персональных данных // Экономика: вчера, сегодня, завтра. 2019. Том 9. № 3А. С. 145-155. DOI: 10.34670/AR.2019.89.3.015

Ключевые слова

Комплаенс-контроль, защита персональных данных, система защиты, экономические риски, комплаенс-миссия, управление персональными данными.

Введение

Такой вид деятельности, как комплаенс, в качестве функции, службы или профессии, состоит в том, чтобы находить способы выявления, управления и смягчения комплаенс-рисков. Данная деятельность является нечто большим, чем просто подчинение правилам, поскольку компании не зарабатывают себе на жизнь, следуя лишь правилам: им необходимо каким-либо образом найти баланс между деятельностью по зарабатыванию денег и соблюдением правил и регламентов, которые ограничивают или направляют их методы достижения этой цели. Функция комплаенса должна играть важную роль в преодолении разрыва между этими двумя, казалось бы, несовместимыми понятиями путем обеспечения соответствия деятельности компании документам, определяющим порядок использования персональных данных.

Подразделение комплаенс-менеджмента является частью менеджмента, однако оно не способно самостоятельно ликвидировать вышеуказанный разрыв. Комплаенс-менеджмент образует комплаенс-функцию и комплаенс-культуру, описывающие общую систему нормативного регулирования инсайдерской информации и методы, посредством которых данная система внедрена в философию и стиль работы компании, в отличие от существования только одном подразделении (комплаенс-менеджмента).

Основная часть

Комплаенс-контроль в области системы обеспечения безопасности персональных данных состоит из следующих нормативных понятий, которые представлены на рисунке 1.



Источник: составлено авторами

Рисунок 1 – Элементы, составляющие комплаенс-контроль в области обеспечения безопасности персональных данных

Наличие в организации департамента комплаенс-контроля в сфере системы обеспечения защиты персональных данных означает получение организацией:

- Защиты от претензий и штрафов со стороны регулирующих органов;
- Преимуществ перед конкурентами, т.к. декларирование соответствия требованиям законодательства о персональных данных приведет к повышению прозрачности и доверия к организации со стороны потенциальных и существующих контрагентов и клиентов;
- Отсутствия негативных отзывов в прессе и СМИ, связанных с неудовлетворительными результатами прохождения проверок регулирующих органов;
- Возможности продолжения собственной деятельности без претензий от клиентов и сотрудников компании;
- Возможности реализации использования персональных данных внутри компании, а также в рамках передачи их сторонним компаниям;
- Защиту от возможной остановки работы компании;
- Защиту от деятельности недобросовестных конкурентов;
- Информационных систем, соответствующих всем стандартам и требованиям законодательства в области персональных данных.¹

Безопасность персональных данных организации имеет первостепенное значение.² Учитывая потенциал со стороны сотрудников организаций, предельно важно, чтобы работодатели совершали всевозможные усилия в целях предотвращения кражи персональных данных сотрудниками (особенно это касается персональных данных клиентов).³

Компаниям необходимо оценивать риски, которые связаны с обеспечением безопасности в следующих областях:

- Корпоративное управление;
- Подбор и проверка персонала;
- Права доступа;
- Мониторинг доступа к данным клиентов и сотрудников;
- Ноутбуки и портативные устройства;
- Физическая безопасность;
- Процесс архивирования данных;
- Внутренний аудит и комплаенс-мониторинг.

В рамках международного права комплаенс-контроль является особой культурой, где отражаются определенные принципы по внедрению функции комплаенс-контроля:

1. Независимость. Данный принцип по внедрению комплаенс-контроля включает в себя четыре элемента по комплаенс, которые являются взаимозависимыми:

- Отдел комплаенс-контроля должен обладать официальным статусом;
- Важно определить специалиста комплаенс-контроля, отвечающего за осуществление контроля за комплаенс-системой и координацию управления комплаенс-рисками;
- Необходимо проконтролировать, чтобы среди участников отдела комплаенс-контроля не было конфликтных ситуаций при осуществлении комплаенс-контроля и контроля по

¹ Официальный сайт компьютерной справочной правовой системы Российской Федерации

² Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 31.12.2014)

³ Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (ред. от 05.04.2013)

выполнению персональных функций в организации;

- Отдел комплаенс-контроля должен иметь доступ к определенным данным и отдельный бюджет в целях реализации функций комплаенс-контроля.

В Соединенных Штатах Америки работа комплаенс-функции регулируется Международной Комплаенс Ассоциацией, Комиссией по ценным бумагам и биржам Соединенных Штатов Америки, нормами антикоррупционного законодательства, Стандартами Комитете Спонсорских организаций Комиссии Тредвея (COSO) относительно системы внутреннего контроля и управления рисками и оценивается с помощью ключевых показателей эффективности (KPIs).

Сотрудниками подразделения комплаенс в США обязательно проводится анализ информационной системы и разрабатываются технические задания для формирования или обновления системы комплаенса. Так же, данное подразделение принимает обязательное участие в разработке системы корпоративного управления и тестирует контроль, установленный для уменьшения комплаенс-рисков в области утечки персональных данных.

В Европейских странах комплаенс-функция прежде всего регулируется следующими документами:

- Директива Евросоюза «О рынках финансовых инструментов» (MIFID), устанавливающая обязанность инвестиционных компаний устанавливать и обеспечивать работу функции комплаенс;
- Отчет Международной организации комиссий по ценным бумагам (IOSCO) относительно функции комплаенса в инвестиционных компаниях;
- Документ «Комплаенс и комплаенс-функция в банках» Базельского комитета по надзору за банками, устанавливающая принципы работы функции комплаенс;
- Инструкции Органа финансового регулирования и надзора Великобритании (FSA), предусматривающие разделы функции комплаенса, а также систему внутреннего контроля;
- Регулирование Банка Италии по функции комплаенса в банках, выпущенное в июле 2007 года.

Несмотря на то, что распределение обязанностей между комплаенс-менеджером и руководством компании может носить совершенно разный характер, существует две различные модели комплаенса в бизнесе.

Первая модель называется централизованной, где подразделение комплаенс менеджмента выполняет практически все текущие задачи по комплаенсу – например, утверждение перечня внутренней информации, рассмотрение жалоб. Вторая модель называется децентрализованной [Тимошкин, 2016]. Так, подразделение комплаенс менеджмента передает большую часть повседневной ответственности за нормативные вопросы коммерческим отделам.

Далее в таблице 1 представлена сравнительная характеристика централизованной и децентрализованной моделей комплаенса.

Таблица 1 – Сравнительная характеристика централизованной и децентрализованной моделей инсайд-комплаенса

Централизованная модель	Децентрализованная модель
Характер взаимодействия коммерческих департаментов и инсайд-комплаенс подразделения	
Велика вероятность частых конфликтов с коммерческими департаментами в случае, если они регулярно обращаются в подразделение инсайд-комплаенс менеджмента за утверждением в сферах, где данные менеджеры не склонны его давать	С одной стороны, инсайд-комплаенс менеджеры имеют менее изнурительную работу, так как дают указания коммерческим департаментам, но решение по поводу того, будут ли выполнять данные департаменты рекомендации остается за ними

Централизованная модель	Децентрализованная модель
Безопасность инсайд-комплаенс менеджмента	
Данная модель может считаться наиболее безопасной для инсайд-комплаенс менеджмента, так как менеджер инсайд-комплаенса сохраняет большую часть контроля над текущей деятельностью	Данная модель является наиболее рискованной для инсайд-комплаенс менеджмента, поскольку нормативные решения коммерческих департаментов могут не быть такими же обоснованными как решения инсайд-комплаенс менеджмента
Ответственность за инсайд-комплаенс	
Ответственность будет считаться обязанностью только инсайд-комплаенс менеджмента	Каждый сотрудник коммерческих департаментов возьмет на себя ответственность только за вопросы, входящие в сферу его собственных обязанностей и деятельности
Обновление информации	
Инсайд-комплаенс менеджментом отслеживаются источники административной информации «в режиме реального времени», например, нетипичное для какого-либо подразделения использование базы персональных данных сотрудников или клиентов	Руководство коммерческих подразделений намного лучше осведомлено о нормативных аспектах, касающихся их ведомств. Таким образом, они с большей вероятностью узнают о недопустимой работе сотрудников с персональными данными и т.д.
Участие в административных вопросах	
Представители инсайд-комплаенс менеджмента активно участвуют в административных вопросах	Инсайд-комплаенс менеджеры меньше вовлечены в работу с повседневными административными вопросами, поэтому, больше времени уделяют занятиям по стратегической работе по нормативному и корпоративному развитию

Источник: Официальный сайт Национальной Ассоциации Комплаенс

Стоит также отметить, что для создания для подразделения комплаенс в сфере обеспечения безопасности персональных данных необходимо сделать следующее:

1. Обязательно получить советы и указания от Совета директоров и высшего руководства относительно сферы обязанностей и характере деятельности подразделения комплаенса;
2. Подготовить декларацию миссии комплаенса. Данная декларация должна быть включена в руководство по комплаенсу, а также размещена на интернет-сайте организации. Важно добавить, что декларация (или ее сокращенный вариант) может быть вставлена в виде подписи во всех сообщениях электронной почты, а также сделать нижним колонтитулом во всей документации, отчетах, процедурах и политиках по комплаенсу;
3. Подготовить официальный Устав по комплаенсу, официально подтвержденный советом директоров компании;
4. В руководство по комплаенсу необходимо поместить резюме обязанностей, деятельности и преимуществ комплаенса;
5. Провести тренинг в целях ознакомления всего персонала компании о том, чем занимается подразделение комплаенс менеджмента, зачем он существует и как может им помочь;
6. Провести «рекламную кампанию» для всего персонала организации для того, чтобы убедиться, что подразделение комплаенса на виду у других подразделений. Для этого можно разместить плакаты о том, что может предложить подразделение комплаенса, а также провести соревнование по комплаенсу.

Необходимо отметить, что каждый из вышеуказанных этапов требует некоторого разъяснения. Что касается декларации миссии комплаенса, то в ней должно содержаться краткое определение самых фундаментальных целей подразделения комплаенса. Так же, назначение цели миссии для сотрудников комплаенс-менеджмента и сотрудников других подразделений компании достаточно сильно отличается.

Для сотрудников комплаенс-подразделения миссия комплаенс является некоторым напоминанием о том, что на самом деле значит быть членом данного подразделения, почему люди выбрали работу в комплаенс и каких целей им нужно достичь. Так же, декларация миссии комплаенс может служить системой распределения приоритета поставленных задач в целях создания концентрации на том, что действительно важно.⁴

Что касается устава комплаенса, то он должен подробно освещать все ключевые концепции, содержащиеся в миссии комплаенса. Он может иметь двойную цель – продвижение услуг, предлагаемых компании подразделением по комплаенсу, а также четко определять сферу и ограничения ответственности и полномочий подразделения.

В некотором роде устав можно считать договором об оказании услуг между подразделением комплаенса и остальными подразделениями компании. Таким образом, подразделение комплаенса может в официальной форме перечислить, что оно будет делать для компании в целом, при этом четко определяя основные положения, из которых инсайд-комплаенс будет исходить при работе.

Далее, данный документ должен быть обязательно утвержден высшим руководством, чтобы каждый сотрудник знал какова позиция данного подразделения. В дальнейшем, опираясь на данный устав, можно будет регулировать различные споры, разногласия об использовании инсайдерской информации или обосновать важность существенных мероприятий по исправлению какой-либо ситуации.

Важно заметить, что существует некоторая процедура создания устава инсайд-комплаенса, которая представлена далее на рисунке 2.

К вышеуказанной схеме стоит добавить, что данный устав необходимо утвердить. Для этого необходимо убедиться, что устав был создан не только в комплаенс-подразделении и представлен руководству компании как свершившийся факт. В случае принятия данного подхода, никакой вклад со стороны бизнеса не будет получен, так как данный устав будет считаться очередным документом комплаенс-подразделения, не имеющим никакого конкретного отношения к другим подразделениям.

Для того чтобы извлечь пользу из устава комплаенс, необходимо убедить бизнес внести свой вклад в концепцию. Высшее руководство должно рассмотреть и обсудить устав и, если необходимо, адаптировать его наиболее удобный образом для бизнеса. Если устав будет отредактирован более двух раз до того, как обе стороны будут им довольны, то это является очень хорошим признаком. Чем большую активность проявляет руководство в подготовке данного документа, тем больше оно будет иметь привязанность к нему, а вследствие этого, и иметь тесное сотрудничество с подразделением комплаенса.

После того, как будет определена высокоуровневая сфера обязанностей в уставе комплаенса, будет необходимо более подробно разобрать характеристику среды деятельности подразделения. Для этого важно собрать большое количество информации, которая станет

⁴ Официальный сайт обучающих курсов по комплаенсу «Комплаенсблог».

базой внедряющегося в компании режима комплаенса, охватывающего следующие сферы:

- Операционные субъекты подразделения;
- Бизнес-подразделения внутри каждого субъекта;
- Внешние поставщики услуг;
- Нормативно-правовая среда (регулирующие органы и другие органы по установлению стандартов, нормативы правил передовых практик);
- Продукты, услуги и коммерческая деятельность.



Источник: составлено авторами

Рисунок 2 – Процедура формирования комплаенс-устава

Некоторые из перечисленных выше областей выходят за рамки подразделения комплаенса, но именно знание других областей, отличных от комплаенса помещает деятельность комплаенса в нужный контекст.

После завершения стадии по анализу среды функционирования, необходимо проанализировать соответствие процедур того или иного департамента компании соответствующим законам.

Завершающим этапом формирования комплаенса в хозяйствующем субъекте является формирование и последующее ведение списка инсайдеров. Данный список формируется в целях убеждения, что ведутся достаточно подробные, полные и актуальные списки всех сотрудников, имеющих доступ к персональным данным. Для того чтобы данный список был грамотно создан, важно соблюсти некоторые действия.

Первый шаг заключается в определении списка департаментов и лиц внутри компании, которые, скорее всего, имеют доступ к внутренней информации в настоящий момент.

Второй шаг – внедрение механизмов, с помощью которых информация будет регистрироваться. Данные записи должны содержать: имя инсайдера; причины, почему ему необходимо быть инсайдером; дата, в которую каждый такой человек стал инсайдером и дата, в которую он перестал им быть.

Третий шаг состоит из письменного подтверждения инсайдером, что он: осведомлен, что его имя внесено в список; согласен с датой регистрации начала обладания им персональными данными; знает о наказаниях за нарушение соответствующих требований.⁵ Важно заметить, что сотрудникам необходимо в письменном виде подтвердить, что при удалении их из списка инсайдеров, они больше не имеют доступа к данному списку.

Четвертым шагом является определение, кто будет хранить списки инсайдеров – это может быть либо подразделение комплаенса, либо соответствующие руководители других подразделений компании.

В рамках пятого шага важно разработать письменные процедуры по использованию списков инсайдеров в организации.

Далее, на шестом шаге проводится обучение сотрудников относительно того, почему и когда списки инсайдеров становятся обязательными, и какие санкции будут применены, если не будут соблюдаться соответствующие требования.

Седьмой, заключительный шаг, заключается в периодическом мониторинге для создания и ведения списков инсайдеров должным образом.

Таким образом, с помощью с помощью вышеуказанных этапов в любом ХС возможно построение системы комплаенса [Мельников, Куприянов, Схиртладзе, 2014].

Меры, которые направлены на соблюдение системы законодательства относительно защиты персональных данных, делятся на три крупные группы:

- Меры юридического контроля;
- Меры организационно-технического контроля;
- Меры внутреннего контроля.

К юридическим мерам относится использование банком внутренних документов и актов (политика в области обработки ПД, положения по обработке ПД, другие приказы и акты), внутри которых должны отражаться индивидуальный подход банка к процессу обработки данных (способы, цели, ответственные лица и т.д.).

Организационно-технические меры должны включать в себя систему выполнения комплекса мероприятий по обеспечению информационной безопасности, которая позволит банку поддерживать режим конфиденциальности ПД и контролировать доступ к ним (в частности, обеспечение нужного уровня технической защиты ПД и системы безопасности информационной системы) [Королев, 2018].

⁵ Информационный ресурс СПАРК

Мерами внутреннего контроля называют процесс внедрения системы мероприятий, которые представляются необходимыми в целях оказания поддержки режима по защите персональных данных в банковской системе на регулярной основе (использование тренингов, периодических внутренних проверок с фиксированием проведенных мероприятий в определенных журналах и т.д.).

Подразделение комплаенс-менеджмента также должно иметь:

1. Возможность прямого доступа к независимым лицам с достаточными полномочиями, которые будут в состоянии предпринять меры вмешательства, если нормативное здоровье банка находится под угрозой: генеральный директор, совет директоров, комитет по аудиту, неисполнительные директора и т.д.;

2. Разрешение работать с HR, чтобы иметь влияние на такие типы нормативных нарушений, которые представляют собой преступления, влекущие санкции; нарушения трудового договора; грубые проступки и т.д., и возможность применять такие типы внутренних санкций, которыми должны наказываться подобные нарушения. Подразделение комплаенс-менеджмента не будет эффективным, если не будет существовать очень четких санкций для тех, кто нарушает правила;

3. Разрешение на доступ к любому документу или отчету о банке, в том числе к личным документам, если существуют обоснованные причины считать, что это необходимо для нормативных целей;

4. Достаточные ресурсы в виде персонала, компьютеров, офисных помещений, обучения, бюджета по поездки и т.д.;

5. Право рассчитывать на сотрудничество со стороны других подразделений банка при выполнении деятельности по комплаенс.

Заключение

Резюмируя, можно сделать вывод, что комплаенс-контроль, связанный с системой обработки персональных данных, создает базовые правила и принципы обработки персональных данных, которыми руководствуется банка в рамках его работы, а также во взаимодействии с клиентами, поставщиками, акционерами и сотрудниками.

Библиография

1. Бабаева Ю.Г. «Комплаенс»: новое слово в юриспруденции // Современная гуманитарная наука: проблемы и перспективы развития. 2017. № 4. С. 41-43.
2. Бородин А.Г. Комплаенс как важнейший принцип ведения бизнеса // Современные корпоративные стратегии и управленческие технологии России. 2017. № 5. С. 38-44.
3. Буянский С.Г., Трунцевский Ю.В. Корпоративное управление, комплаенс и риск-менеджмент. М.: РУСАЙНС, 2016. 344 с.
4. Ермакова Н.А. Комплаенс-контроль в системе внутреннего контроля корпораций // Международный бухгалтерский учет. 2017. №3. С. 5-12.
5. Королев А.И. Общие понятия и порядок раскрытия информации // Право и политика. 2018. № 2. С. 265-267.
6. Ложкина Л.И. Комплаенс как психологический факт // Наука и практика. 2016. № 6. С. 49-57.
7. Официальный сайт Института Внутренних Аудиторов. URL: <https://www.iaa-ru.ru>
8. Позолотина В.И. Развитие комплаенс-контроля в России // Фундаментальные и прикладные исследования в современном мире. 2017. № 9. С. 34-39.
9. Росенко А.П. Внутренние угрозы безопасности конфиденциальной информации. Методология и теоретическое исследование. М.: Красанд, 2014. С. 476.
10. Черепанова В.В. Комплаенс-программа организации. М.: Аспект Пресс, 2016. 495 с.

Basics of compliance control in the field of personal data security

Vasilii A. Dadalko

Doctor of Economics,
Professor,
Financial University under the Government of the Russian Federation,
125993, 49, Leningradskii av., Moscow, Russian Federation;
e-mail: antikrizis1@bk.ru

Evgenii A. Timofeev

Graduate Student,
Financial University under the Government of the Russian Federation,
125993, 49, Leningradskii av., Moscow, Russian Federation;
e-mail: timofeev.e.a@inbox.ru

Abstract

The issue of the protection of personal data is of particular importance. For all Russian companies, working with personal data is an integral element of business development. Thus, in connection with the emerging trend of tightening legislation in the field of personal data protection, organizations should pay close attention to ensuring preventive measures in relation to countering the leakage of personal data. To date, there is no clear concept of the term “compliance control,” just as there is no definitive list of what the compliance manager should do and what not, which includes the compliance function. The level of expectations regarding the role of compliance management in connection with regulatory scandals has steadily increased, and in today's global economic uncertainty climate, considerable emphasis is placed on the large contribution that a compliance manager can make to the company. The success of any company depends entirely on its attitude to the personal data. Violation of the personal data protection system may lead to irreparable consequences. Compliance with the law on personal data is a set of measures, the implementation of which should be supported in the company on an ongoing basis. It is important not only to fix in the internal acts a complex of such measures and methods for their implementation, but also to actually implement them. It is also necessary to support the implementation and implementation of measures on an ongoing basis and to have evidence that the measures are not declarative and exist only on paper.

For citation

Dadalko V.A., Timofeev E.A. (2019) Organizatsiya sistemy komplensa v oblasti zashchity personal'nykh dannykh [Basics of compliance control in the field of personal data security]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 9 (3A), pp. 145-155. DOI: 10.34670/AR.2019.89.3.015

Keywords

Compliance control, personal data, security, compliance risk, compliance function, management.

References

1. Babaeva Yu.G. (2017) «Komplaens»: novoe slovo v yurisprudentsii [Compliance: a new word in jurisprudence]. *Sovremennaya gumanitarnaya nauka: problemy i perspektivy razvitiya* [Modern Humanitarian Science: Problems and Prospects for Development], 4, pp. 41-43.
2. Borodin A.G. (2017) Komplaens kak vazhneishii printsip vedeniya biznesa [Compliance as the most important business principle]. *Sovremennye korporativnye strategii i upravlencheskie tekhnologii Rossii* [Modern corporate strategies and management technologies of Russia], 5, pp. 38-44.
3. Buyanskii S.G., Truntsevskii Yu.V. (2016) *Korporativnoe upravlenie, komplaens i risk-menedzhment* [Corporate governance, compliance and risk management]. Moscow: RUSAINS Publ.
4. Cherepanova V.V. (2016) *Komplaens-programma organizatsii* [Compliance organizational program]. Moscow: Aspekt Press Publ.
5. Ermakova N.A. (2017) Komplaens-kontrol' v sisteme vnutrennego kontrolya korporatsii [Compliance control in the system of internal control of corporations]. *Mezhdunarodnyi bukhgalterskii uchet* [International Accounting], 3, pp. 5-12.
6. Korolev A.I. (2018) Obshchie ponyatiya i poryadok raskrytiya informatsii [General concepts and procedure for disclosure of information]. *Pravo i politika* [Law and Politics], 2, pp. 265-267.
7. Lozhkina L.I. (2016) Komplaens kak psikhologicheskii fakt [Compliance as a psychological fact]. *Nauka i praktika* [Science and Practice], 6, pp. 49-57.
8. *Ofitsial'nyi sait Instituta Vnutrennikh Auditorov* [The official website of the Institute of Internal Auditors]. URL: <https://www.iiia-ru.ru>
9. Pozolotina V.I. (2017) Razvitie komplaens-kontrolya v Rossii [Development of compliance control in Russia]. *Fundamental'nye i prikladnye issledovaniya v sovremennom mire* [Fundamental and applied research in the modern world], 9, pp. 34-39.
10. Rosenko A.P. (2014) *Vnutrennie ugrozy bezopasnosti konfidentsial'noi informatsii. Metodologiya i teoreticheskoe issledovanie* [Internal threats to the security of confidential information. Methodology and theoretical research]. Moscow: Krasand Publ.