

ОСНОВЫ ФОРМИРОВАНИЯ КОМПЛАЕНС-КОНТРОЛЯ В ОБЛАСТИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**Василий Александрович ДАДАЛКО^{a,*}, Евгений Александрович ТИМОФЕЕВ^b**

^a доктор экономических наук, профессор кафедры анализа рисков и экономической безопасности, Финансовый университет при Правительстве РФ, Москва, Российская Федерация
antikrizis1@bk.ru
<https://orcid.org/0000-0001-5436-3286>
SPIN-код: 4287-0228

^b студент факультета анализа рисков и экономической безопасности, Финансовый университет при Правительстве РФ, Москва, Российская Федерация
timofeev.e.a@inbox.ru
ORCID: отсутствует
SPIN-код: 8292-6952

* Ответственный автор

История статьи:

Per. № 247/2019
Получена 28.03.2019
Получена в доработанном виде 19.04.2019
Одобрена 12.05.2019
Доступна онлайн 14.02.2020

УДК 336.717
JEL: M12, M15

Ключевые слова:

комплаенс-контроль,
персональные данные,
комплаенс-риск,
комплаенс-функция

Аннотация

Предмет. Статья посвящена основам формирования комплаенс-контроля в области системы обеспечения безопасности персональных данных.

Цели. Определение роли комплаенс, уточнение термина «комплаенс обеспечения безопасности персональных данных», выяснение уровня актуальности комплаенс.

Методология. В работе использованы общенаучные методы анализа, сравнения, обобщения.

Результаты. В ходе исследования проанализирована роль защиты персональных данных. Отмечено, что для всех российских компаний работа с персональными данными является неотъемлемым элементом развития бизнеса. Таким образом, в связи с наметившейся тенденцией ужесточения законодательства в сфере защиты персональных данных организациям стоит обратить пристальное внимание на обеспечение превентивных мер в отношении противодействия утечке персональных данных. Отмечено, что на сегодняшний день до сих пор не принято четкого определения термина «комплаенс-контроль», как и не существует окончательного перечня того, чем должен заниматься комплаенс-менеджер, и что включает в себя комплаенс-функция.

Выводы. Успешная деятельность любой компании полностью зависит от отношения ее руководства к персональным данным, с которыми осуществляется работа. Нарушение системы защиты персональных данных может привести к непоправимым последствиям. Соблюдение законодательства о персональных данных – это комплекс мер, реализация которых должна поддерживаться в компании на постоянной основе. Важно не только фиксировать во внутренних актах комплекс таких мер и способы их реализации, но также в действительности их реализовывать.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2019

Для цитирования: Дадалко В.А., Тимофеев Е.А. Основы формирования комплаенс-контроля в области системы обеспечения безопасности персональных данных // *Национальные интересы: приоритеты и безопасность*. – 2020. – Т. 16, № 2. – С. 339 – 350.
<https://doi.org/10.24891/ni.16.2.339>

Комплаенс, как вид деятельности (в качестве функции, службы или профессии), состоит в том, чтобы находить способы выявления, управления и смягчения комплаенс-рисков. Данная деятельность подразумевает нечто большее, чем просто подчинение правилам, поскольку компании не зарабатывают, следуя одним лишь правилам: им необходимо каким-либо образом найти баланс между деятельностью по получению прибыли и

соблюдением правил и регламентов, которые ограничивают или направляют их методы достижения этой цели. Функция комплаенса¹ призвана играть важную роль в преодолении разрыва между этими двумя, казалось бы, несовместимыми понятиями путем обеспечения соответствия деятельности компании документам, определяющим порядок использования персональных данных [1].

Подразделение комплаенс-менеджмента является частью управленческого звена фирмы, однако оно не способно самостоятельно ликвидировать указанный 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 [2–4].

Комплаенс-контроль в области системы обеспечения безопасности персональных данных состоит из ряда нормативных понятий, представленных на *рис. 1*.

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

- защиту от претензий и штрафов со стороны регулирующих органов;
- преимущества перед конкурентами, поскольку декларирование соответствия требованиям законодательства о персональных данных приводит к повышению прозрачности и доверия к организации со стороны потенциальных и существующих контрагентов и клиентов;
- отсутствие 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;
- защиту информационных систем, соответствующих всем стандартам и требованиям законодательства в области персональных данных.

Первостепенное значение имеет безопасность персональных данных организации². Учитывая потенциал со стороны сотрудников организаций, предельно важно, чтобы работодатели прикладывали все возможные усилия для предотвращения кражи персональных данных сотрудниками (особенно это касается персональных данных клиентов)³ [5, 6].

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

- 1) корпоративное управление;
- 2) подбор и проверка персонала;
- 3) права доступа;
- 4) мониторинг доступа к данным клиентов и сотрудников;
- 5) ноутбуки и портативные устройства;
- 6) физическая безопасность;

¹ Буянский С.Г., Трунцевский Ю.В. Корпоративное управление, комплаенс и риск-менеджмент: учеб. пособие для магистрантов. М.: РУСАЙНС, 2016. 344 с.; Бабаева Ю.Г. «Комплаенс»: новое слово в юриспруденции: материалы международной научной конференции «Современная гуманитарная наука: проблемы и перспективы развития». Рязань, 2015. С. 41–43.

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

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

7) процесс архивирования данных;

8) внутренний аудит и комплаенс-мониторинг.

В рамках международного права комплаенс-контроль является особой культурой, в которой отображается **принцип независимости** по внедрению самой функции комплаенс-контроля. Данный принцип включает в себя четыре элемента, которые являются взаимозависимыми:

- 1) отдел комплаенс-контроля должен обладать официальным статусом;
- 2) важно определить специалиста комплаенс-контроля, отвечающего за осуществление контроля за комплаенс-системой и координацию управления комплаенс-рисками;
- 3) необходимо проконтролировать, чтобы среди участников отдела не было конфликтных ситуаций при осуществлении комплаенс-контроля и контроля за выполнением персональных функций в организации;
- 4) отдел комплаенс-контроля должен иметь доступ к определенным данным и отдельный бюджет в целях реализации своих функций.

В США работа комплаенс-подразделений регулируется Международной ассоциацией комплаенс, Комиссией по ценным бумагам и биржам Соединенных Штатов Америки, нормами антикоррупционного законодательства, стандартами Комитета спонсорских организаций Комиссии Тредвея (COSO) относительно системы внутреннего контроля и управления рисками, а также оценивается с помощью ключевых показателей эффективности (KPIs).

В США сотрудниками подразделений комплаенс обязательно проводится анализ информационной системы и разрабатываются технические задания для формирования или обновления системы комплаенса. Также 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:

- директивой Евросоюза «О рынках финансовых инструментов» (MIFID), устанавливающей обязанность инвестиционных компаний определять и обеспечивать работу функции комплаенс;
- отчетом Международной организации комиссий по ценным бумагам (IOSCO) относительно функции комплаенса в инвестиционных компаниях;
- документом «Комплаенс и комплаенс-функция в банках» Базельского комитета по надзору за банками, устанавливающая принципы работы функции комплаенс;
- инструкциями Органа финансового регулирования и надзора Великобритании (FSA), предусматривающими разделы функции комплаенса, а также систему внутреннего контроля;
- регулированием Банка Италии по функции комплаенса в банках, выпущенным в июле 2007 г.

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

Первая модель называется *централизованной*, в ней подразделение комплаенс-менеджмента выполняет практически все текущие задачи по комплаенсу – например, утверждение перечня внутренней информации, рассмотрение жалоб. **Вторая модель** – *децентрализованная*⁴. В ней подразделение комплаенс-менеджмента передает большую часть повседневной

⁴ Тимошкин А.В. Корпоративный комплаенс-контроль как инструмент экономической безопасности. М.: Институт экономики РАН, 2016.

ответственности за нормативные вопросы коммерческим отделам. Комплаенс-менеджеры ответственны следить за тем, что делают коммерческие отделы, проводя при этом оценку эффективности их работы и создавая мероприятия по устранению негативных последствий. В табл. 1 представлена сравнительная характеристика централизованной и децентрализованной моделей комплаенса.

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

- 1) обязательно получить указания и рекомендации от Совета директоров и высшего руководства компании относительно круга обязанностей и характера 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 служить нижним колонтитулом во всей документации, отчетах, процедурах и политиках по комплаенсу;
- 3) подготовить официальный Устав по комплаенсу, принятый и подтвержденный Советом директоров компании;
- 4) в руководство по комплаенсу поместить краткую сводку 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 с тем, чтобы

убедиться, что подразделение комплаенса находится на виду у других подразделений. Для этого можно разместить плакаты о том, что может предложить подразделение комплаенса, а также провести соревнование по комплаенсу.

Каждый из перечисленных шагов требует некоторого разъяснения. Что касается декларации миссии комплаенса, то в ней должно содержаться краткое определение самых фундаментальных целей подразделения комплаенса. Кроме того, декларируемые миссии для сотрудников комплаенс-менеджмента и сотрудников других подразделений компании достаточно сильно различаются [7].

Для сотрудников комплаенс-подразделения миссия комплаенс является некоторым напоминанием о том, что на самом деле означает быть членом данного подразделения, почему люди выбрали работу в комплаенс, и каких целей им нужно достичь. Также декларация миссии комплаенс может служить системой распределения приоритета поставленных задач для концентрации сотрудников на том, что действительно является важным⁵.

Для сотрудников других подразделений компании миссия комплаенс должна быть достаточно кратким напоминанием о том, для чего существует подразделение комплаенса (данное напоминание должно трактоваться весьма положительно для бизнеса).

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 четкое определение сферы и ограничений ответственности и полномочий данного подразделения.

Устав в некотором роде можно считать договором об оказании услуг между подразделением комплаенса и остальными

⁵ Обучающие курсы по комплаенсу «Комплаенсблог». URL: <http://complianceblog.ru>

отделами компании. Таким образом, подразделение комплаенса может в официальной форме перечислить, что оно будет делать для компании в целом, четко определяя при этом 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 обосновывать важность существенных мероприятий по исправлению какой-либо ситуации.

Важно отметить, что существует определенная процедура создания устава инсайд-комплаенса (рис. 2). После создания устав необходимо утвердить. Для этого следует убедиться, что устав был создан не только в комплаенс-подразделении и не представлен руководству компании просто как свершившийся факт. В противном случае данный устав будет считаться очередным документом комплаенс-подразделения, не имеющим никакого конкретного отношения к другим подразделениям.

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

После того, как в уставе комплаенса будет определена главная сфера обязанностей,

необходимо более подробно разобрать характеристику среды деятельности подразделения. Для этого важно собрать большое количество информации, которая станет 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.

Некоторые из перечисленных областей выходят за рамки подразделения комплаенса, но именно знание этих и других областей (отличных от прямых задач комплаенса) помещает его деятельность 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 для уверенности в том, что ведутся достаточно подробные, полные и актуальные списки всех сотрудников, имеющих доступ к персональным данным. Для того чтобы данный список был правильно создан, важно грамотно осуществить 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 – это внедрение механизмов, с помощью которых получаемая информация будет регистрироваться. Данные записи должны содержать: имя инсайдера; причины, по которым ему необходимо быть инсайдером; дата, когда человек стал инсайдером, и дата, когда он перестал им быть.

Третьим шагом является письменное подтверждение инсайдером того, что он осведомлен, что его имя внесено в список; согласен с датой регистрации начала обладания им персональными данными; знает о наказании за нарушение соответствующих требований⁶. Важно заметить, что сотрудникам необходимо в письменном виде подтвердить, что в случае их удаления из списка инсайдеров, они больше не будут иметь доступа к данному списку.

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

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

Далее, на *шестом шаге*, проводится информирование сотрудников о том, почему и когда списки инсайдеров становятся обязательными, и какие санкции будут применены, если не будут соблюдаться соответствующие требования.

Заключительный *седьмой шаг* заключается в периодическом мониторинге для создания и ведения списков инсайдеров должным образом.

Таким образом, посредством описанных шагов (этапов) в любом хозяйствующем субъекте возможно построение системы комплаенса⁷. Меры, направленные на соблюдение законодательства относительно защиты

персональных данных, делятся на три основные группы:

- 1) меры юридического контроля;
- 2) меры организационно-технического контроля;
- 3) меры внутреннего контроля.

К *юридическим мерам* относится использование банком внутренних документов и актов (политика в области обработки персональных данных, положения по обработке персональных данных, 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 персональных данных и контролировать доступ к ним (в частности, обеспечение нужного уровня технической защиты персональных данных и системы безопасности информационной системы) [5].

Мерами внутреннего контроля называют процесс внедрения системы мероприятий, которые представляются необходимыми для 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» компании находится под угрозой: генеральный директор, совет директоров, комитет по аудиту, неисполнительные директоры и т.д.;

⁶ Информационный ресурс СПАРК.
URL: <http://sparkinterfax.ru>

⁷ Мельников В.П., Куприянов А.И., Схиртладзе А.Г. Защита информации: учеб. пособие. М.: Академия, 2014. С. 45.

- 2) разрешение работать с персоналом для того, чтобы иметь возможность фиксировать нарушения, влекущие санкции (нарушения трудового договора, грубые проступки и т.д.), а также возможность применять различные типы внутренних санкций, которыми наказываются подобные нарушения. Подразделение комплаенс-менеджмента не станет эффективным, если не сможет накладывать жесткие санкции на тех, кто нарушает правила;
- 3) разрешение на доступ к любому документу или отчету, в том числе к личным документам, если существуют обоснованные причины считать, что это необходимо в нормативных целях;
- 4) достаточные ресурсы в виде персонала, компьютеров, офисных помещений, бюджета на командировки, обучение и т.д.;
- 5) право рассчитывать на сотрудничество со стороны других подразделений компании при выполнении деятельности по комплаенс.
- Подводя итоги исследования, можно сделать вывод, что комплаенс-контроль, связанный с системой обработки персональных данных, создает базовые правила и принципы обработки персональных данных, которыми руководствуется персонал компании в своей повседневной работе, а также во взаимодействии с клиентами, поставщиками, акционерами и сотрудниками.

Таблица 1**Сравнительная характеристика централизованной и децентрализованной моделей инсайд-комплаенса****Table 1****The comparative description of centralized and decentralized models of internal compliance**

Показатель	Вид модели	
	Централизованная	Децентрализованная
Характер взаимодействия коммерческих департаментов и подразделения инсайд-комплаенс	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
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 решении административных вопросов	Инсайд-комплаенс-менеджеры меньше вовлечены в работу с повседневными административными вопросами, поэтому больше времени уделяют стратегической работе по нормативному и корпоративному развитию
-------------------------------------	--	--

Источник: официальный сайт Национальной Ассоциации COMPLIANCE: URL: <http://compliance.su/>

Source: Official website of the National Compliance Association: URL: <http://compliance.su/> (In Russ.)

Рисунок 1

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

Figure 1

Constituents of compliance control of personal data protection



Источник: авторская разработка

Source: Authoring

Рисунок 2
Процедура формирования комплаенс-устава

Figure 2
The formation of the compliance charter



Источник: авторская разработка

Source: Authoring

Список литературы

1. Бородин А.Г. Комплаенс как важнейший принцип ведения бизнеса // Современные корпоративные стратегии и управленческие технологии России. 2017. № 5. С. 38–44.
2. Ермакова Н.А., Ахуньянова Ч.Ф. Комплаенс-контроль в системе внутреннего контроля корпораций // Международный бухгалтерский учет. 2014. Т. 17. Вып. 3. С. 2–10.
URL: <https://cyberleninka.ru/article/n/komplaens-kontrol-v-sisteme-vnutrennego-kontrolya-korporatsiy/viewer>
3. Королёв А.И. Общие понятия и порядок раскрытия информации // Право и политика. 2018. № 2. С. 265–267.
4. Ложкина Л.И. Комплаенс как психологический факт // Наука и практика. 2016. № 6. С. 49–57.

5. Позолотина В.И. Развитие комплаенс-контроля в России // *Фундаментальные и прикладные исследования в современном мире*. 2017. № 9-2. С. 34–39.
6. Росенко А.П. Внутренние угрозы безопасности конфиденциальной информации. Методология и теоретическое исследование: монография. М.: URSS, 2010. 160 с.
7. Черепанова В.В. Комплаенс-программа организации. М.: Аспект Пресс, 2016. 495 с.

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.

**FUNDAMENTALS OF SETTING THE COMPLIANCE CONTROL
OF PERSONAL DATA PROTECTION****Vasilii A. DADALKO**^{a,*}, **Evgenii A. TIMOFEEV**^b^a Financial University under Government of Russian Federation, Moscow, Russian Federation
antikrizis1@bk.ru
<https://orcid.org/0000-0001-5436-3286>^b Financial University under Government of Russian Federation, Moscow, Russian Federation
timofeev.e.a@inbox.ru
ORCID: not available

* Corresponding author

Article history:Article No. 247/2019
Received 28 March 2019
Received in revised form
19 April 2019
Accepted 12 May 2019
Available online
14 February 2020**JEL classification:** M12,
M15**Keywords:** compliance
control, personal data,
compliance risk,
compliance function**Abstract****Subject** The article discusses principles for setting the compliance control over personal data security.**Objectives** The study determines the role of compliance, specifies the term *compliance of personal data protection* and assesses the relevance of such compliance.**Methods** The study involves general scientific methods for analysis, comparison and generalization.**Results** We analyzed the significance of personal data protection. Every Russian company has to handle personal data as part of their business development. Therefore, as the personal data protection laws become more and more stringent, entities should take special efforts to prevent personal data leakage. Currently, compliance control has not yet been clearly defined, likewise there are still no firm list of compliance manager's duties and the content of a compliance function.**Conclusions and Relevance** The successful performance of any company totally depends on the way its management handles personal data used for operations. The personal data abuse may bring dramatic consequences. The compliance with personal data compliance implies a set of actions which any company should continuously perform. It is important not only document such measures and practical methods in internal papers, but also put them in practice.

© Publishing house FINANCE and CREDIT, 2019

Please cite this article as: Dadalko V.A., Timofeev E.A. Fundamentals of Setting the Compliance Control of Personal Data Protection. *National Interests: Priorities and Security*, 2020, vol. 16, iss. 2, pp. 339–350.
<https://doi.org/10.24891/ni.16.2.339>**References**

1. Borodin A.G. [Compliance as the most important business principle]. *Sovremennye korporativnye strategii i upravlencheskie tekhnologii Rossii = Russia's Modern Corporate Strategies and Management Technologies*, 2017, no. 5, pp. 38–44. (In Russ.)
2. Ermakova N.A., Akhun'yanova Ch.F. [Compliance control system of internal control of corporations]. *Mezhdunarodnyi bukhgalterskii uchet = International Accounting*, 2014, vol. 17, iss. 3, pp. 2–10. URL: <https://cyberleninka.ru/article/n/komplaens-kontrol-v-sisteme-vnutrennego-kontrolya-korporatsiy/viewer> (In Russ.)
3. Korolev A.I. [General concepts and disclosure procedures]. *Pravo i politika = Law and Policy*, 2018, no. 2, pp. 265–267. (In Russ.)

4. Lozhkina L.I. [Compliance as a psychological factor]. *Nauka i praktika = Science and Practice*, 2016, no. 6, pp. 49–57. (In Russ.)
5. Pozolotina V.I. [The history of development of compliance-control in Russia]. *Fundamental'nye i prikladnye issledovaniya v sovremennom mire = Fundamental and Applied Research in the Modern World*, 2017, no. 9-2, pp. 34–39. (In Russ.)
6. Rosenko A.P. *Vnutrennie ugrozy bezopasnosti konfidentsial'noi informatsii. Metodologiya i teoreticheskoe issledovanie: monografiya* [Internal threats to confidential data security: a monograph]. Moscow, URSS Publ., 2010, 160 p.
7. Cherepanova V.V. *Komplaens-programma organizatsii* [Corporate compliance program]. Moscow, Aspekt-Press Publ., 2016, 495 p.

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.