# АНАЛИЗ ТРЕБОВАНИЙ НОРМАТИВНОЙ ДОКУМЕНТАЦИИ К УРЕГУЛИРОВАНИЮ КОНФЛИКТА ИНТЕРЕСОВ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Алексеев А.Д.[1], Воробьёва А.А.[2], Лившиц И.И. [3], Юрин И.В.[4]*

***Аннотация***

***Цель исследования:*** *анализ действующих национальных стандартов России по информационной безопасности и системам менеджмента и оценка уровня готовности содержащихся в них требований к регулированию конфликта интересов на соответствие законодательству Российской Федерации, а также их сравнение с требованиями стандартов ISO.*

***Метод исследования:*** *исследуется проблема регулирования конфликта интересов в соответствии с требованиями федерального закона Российской Федерации № 273-ФЗ, указания Банка России № 5511-У и стандартов по системам менеджмента и информационной безопасности. Анализируются пересечения в требованиях данных документов. Проводится сравнительный анализ требований в национальных стандартах России и стандартов ISO. Исследуются существующие патенты и системы автоматизированного поиска и анализа конфликта интересов.*

***Результат исследования:*** *выполнено исследование и сопоставление требований федерального закона Российской Федерации ФЗ-273 и стандартов по системам менеджмента и информационной безопасности. Приведена сравнительная таблица требований по урегулированию конфликта интересов. Приведены предложения по регулированию конфликта интересов в организациях за счет использования автоматизированных средств.*

***Ключевые слова:*** *конфликт интересов, федеральный закон, информационная безопасность, стандарт, ГОСТ, ISO, коррупция, Банк России, программные средства, анализ конфликта интересов.*

**DOI:** 10.21681/2311-3456-2021-4-48-60

## Введение

В современном мире все больше уделяют внимания борьбе с коррупцией, на фоне которой стали прорабатываться многие темы, ранее не имевшие широкого распространения. Одной из них является тема конфликта интересов [1, 2]. Вопрос конфликта интересов является очень серьёзным и до настоящего времени слабо раскрытым с точки зрения нормативной документации Российской Федерации [3, 4], в частности стандартов по информационной безопасности.

К конфликту интересов предъявляются все более строгие требования по контролю. Это коррелирует с общей тенденцией в вопросах мониторинга информационной безопасности, о которой пишет Полтавцева М.А. в статье «Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем» [5] в журнале «Вопросы кибербезопасности».

Также в данном журнале опубликована статья Кубарева А.В., Лапсарь А.П. и Асютикова А.А. «Синтез модели объекта критической информационной инфраструктуры для безопасного функционирования технической системы в условиях деструктивного информационного воздействия» [6]. В ней с первых абзацев говориться об участившихся атаках деструктивного характера, оперирующих информационным воздействием на персонал организаций. Данное воздействие, в свою очередь, является почвой для возникновения деструктивного конфликта интересов, в частности в критических информационных структурах.

Еще одним доказательством актуальности темы регулирования конфликта является статья [7] Аносова Р.С., Аносова С.С. и Шахалова И.Ю. о риск-ориентированной модели системы информационных технологий. Авторы описывают структуру информационного конфликта сторон, после чего осуществляют формализацию процессов управления информационной безопасностью с применением методов теории динамических (многошаговых) игр.

Цель данной статьи показать, на какой стадии проработанности находится тема конфликта интересов в национальных стандартах РФ по информационной безопасности и системам менеджмента, а также провести сравнительный анализ национальных стандартов России и стандартов ISO.

1 Алексеев Андрей Дмитриевич, магистрант университета ИТМО, Санкт-Петербург, Россия. Email: andalexs@yandex.ru

2 Воробьёва Алиса Андреевна, кандидат технических наук, доцент университета ИТМО, Санкт-Петербург, Россия. Email: alice_w@mail.ru

3 Лившиц Илья Иосифович, доктор технических наук, доцент университета ИТМО, Санкт-Петербург, Россия. Email: Livshitz.il@yandex.ru

4 Юрин Игорь Валентинович, кандидат военных наук, доцент университета ИТМО, доцент ГУМРФ имени адмирала С.О. Макарова, Санкт-Петербург, Россия. Email: 9402015@mail.ru

**Обзор основной действующей нормативно-правовой базы по вопросам конфликта интересов в Российской Федерации**

Во главе законодательства по вопросам конфликта интересов стоит федеральный закон № 273 «О противодействии коррупции»[5] (далее – 273-ФЗ). В статье 10 273-ФЗ определение конфликта интересов звучит примерно следующим образом:

«Конфликт интересов – это ситуация, при которой личная заинтересованность лица, выполняющего обязанности по принятию мер по предотвращению и урегулированию конфликта интересов, влияет или может повлиять на надлежащее, объективное и беспристрастное исполнение им должностных обязанностей».

В данном законе также описываются лица, на которых возлагается обязанность принимать меры по противодействию конфликтам интересов. В основном это главы и руководители государственных, муниципальных и военных структур (организаций), а также, отдельно выделенные в законе, должностные лица Центрального Банка России.

Частными определениями конфликта интересов в банковской сфере являются определения, указанные во втором абзаце пункта 1.1 статьи 39 (для управляющей компании инвестиционных фондов) и во втором абзаце пункта 10.1 статьи 44 (для специализированного депозитария) федерального закона № 156-ФЗ «Об инвестиционных фондах»[6]. Этот закон обязывает все банки России разработать собственные политики по урегулированию конфликта интересов. В соответствии с данными политиками они должны осуществлять деятельность по выявлению, противодействию и ликвидации конфликта интересов.

Положения, описывающие требования, порядок действий и сроки, в случае выявления конфликта интересов в банковской сфере (а именно в управляющей компании инвестиционных фондов, паевых инвестиционных фондов, негосударственных пенсионных фондов и специализированного депозитария), изложены в указании Центрального Банка России от № 5511-У[7] (далее – Указание), вступившее в силу 1 апреля 2021 года. Данное указание можно рассматривать как базовые требования к процедурам урегулирования конфликта интересов в банковской сфере, потому что подавляющее большинство банков так или иначе связаны с деятельностью, описываемой в Указании.

В соответствии с Указанием управление конфликтом интересов в банках осуществляется на основе частных «политик по управлению конфликтом интересов», в которых каждый банк описывает применяемые у себя методы и способы по выявлению, предупреждению, сдерживанию и регулированию конфликта интересов.

В 273-ФЗ описаны следующие требования, на момент написания статьи:

1. В статье 11 изложены положения, описывающие обязанности и ответственность должностных лиц и работодателя в вопросе урегулирования конфликта интересов, а именно:
   a. обязанность принимать меры по недопущению любой возможности возникновения конфликта интересов;
   b. обязанность работника уведомлять работодателя о возникшем конфликте интересов или о возможности его возникновения, сразу как о нем станет известно работнику;
   c. обязанность работодателя принять меры по предотвращению или урегулированию конфликта интересов, если ему стало известно о возникновении у работника личной заинтересованности, которая приводит или может привести к конфликту интересов;
   d. работник должен быть отстранен от исполнения должностных обязанностей и (или) отказаться от выгоды, явившейся причиной возникновения конфликта интересов;
   e. обязанность производить работниками самоотвод, в случае возникновения конфликта интересов;
   f. обязанность передавать ценные бумаги в доверительное управление в соответствии с гражданским законодательством.
2. В соответствии со статьей 13, в случае несоблюдения работником положений нормативных документов по противодействию коррупции и урегулированию и (или) предотвращению конфликта интересов, он считается утратившим доверие и подлежит увольнению.
3. В статье 13.3 описаны меры по противодействию коррупции, которые может использовать организация:
   a. определение ответственных за профилактику правонарушений;
   b. сотрудничество организации с правоохранительными органами;
   c. разработка и внедрение в практику стандартов и процедур, направленных на обеспечение добросовестной работы организации;
   d. принятие кодекса этики и служебного поведения работников организации;
   e. предотвращение и урегулирование конфликта интересов;
   f. недопущение составления неофициальной отчетности и использования поддельных документов.
4. В статье 15 описывается факт публикации перечня лиц, утративших доверие, в открытой базе (реестре), сроком на пять лет.

Также в кодексе Российской Федерации об административных правонарушениях имеются положения об ответственности за коррупционные деяния, например:

1. Статья 2.6. Административная ответственность иностранных граждан, лиц без гражданства и иностранных юридических лиц.
2. Статья 19.28. Незаконное вознаграждение от имени юридического лица.

5 Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции» (дата обращения: 10.04.2021)

6 Федеральный закон от 29.11.2001 № 156-ФЗ «Об инвестиционных фондах» (дата обращения: 15.04.2021)

7 Указание Банка России от 22.07.2020 № 5511-У «О требованиях к выявлению конфликта интересов и управлению конфликтом интересов управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов и специализированного депозитария» (дата обращения: 15.04.2021)

DOI: 10.21681/2311-3456-2021-4-48-60

**Обзор требований стандартов ISO, в контексте конфликта интересов**

Начнем обзор со стандарта ISO 37500 «Руководство по аутсорсингу»[8]. Данный стандарт не имеет аналогов среди стандартов Российской Федерации. Этот международный стандарт является руководством в вопросах выбора качественных услуг аутсорсинга, анализа рисков, характерных для аутсорсинга, обеспечения взаимовыгодных отношений сотрудничества. На первых страницах стандарта описывается факт того, что организации вынуждены адаптироваться в быстро развивающемся мире. В последние годы такой адаптацией становиться передача на аутсорсинг управления затратами, проведения стратегических изменений в организациях, передача рисков и получение доступа к различным ресурсам.

Одним из основных видов рисков, описанных в п. 4.3 стандарта, является риск «недооценённого влияния на бизнес» (d). Он подразумевает столкновение различных культур и интересов организаций при заключении соглашения о предоставлении услуг и в процессе их предоставления. Это можно расценивать как риск потенциальных конфликтов интересов. О нем же говорит и вид рисков (e) «плохая культурная совместимость» и (g) «плохое управление взаимоотношениями».

По данному стандарту аутсорсинговое управление делится на четыре этапа (п. 4.4):

1. «Анализ стратегии аутсорсинга» – данный этап клиентоориентированный. Он направлен на поиск и оценку возможностей аутсорсинга, а также создание стратегии аутсорсинга, максимально соответствующей бизнес целям и требованиям организации-клиента.
2. «Инициация и отбор» – этап состоит в том, чтобы определить требования к предлагаемым услугам для аутсорсинга, выбрать адекватных поставщиков услуги и успешно заключить соглашения об аутсорсинге, учитывая положения стратегии, разработанной на этапе 1. Если на этом этапе возникли проблемы или недопонимание клиента с поставщиком, то необходимо возвращение на 1 этап. По результатам данного этапа пописывается соглашение о предоставлении услуг.
3. «Переход» – этот этап может включать передачу персонала, активов и связанных с ними процедур управления изменениями. При формальном заключении сделки ответственность переходит к поставщику, а остаточные риски оцениваются и принимаются клиентом. По результатам выполнения этапа должно прийти понимание жизнеспособности идеи использования услуг аутсорсинга для организации.
4. «Доставка ценностей» – цель этого этапа заключается в обеспечении осознания клиентом и поставщиком ценности аутсорсинга, и поддержка его в соответствии с бизнес-целями и амбициями.

ISO 37500 определяет важность деловых отношений, в рамках аутсорсингового управления, для создания постоянного согласования амбиций и интересов всех заинтересованных сторон (п. 4.5). В соответствии со стандартом все этапы жизненного цикла аутсорсинга повторяются, что обеспечивает адаптивность организаций к изменяющимся реалиям и постоянную переоценку рисков.

В главе 5, как и во всем стандарте, сделан упор на взаимоотношения клиента и поставщика аутсорсинговых услуг. Описывается большое количество процедур, необходимых для взаимовыгодного принятия решений. Как пример, можно привести следующие положения:

- Создание клиентом и поставщиком совместных комитетов по управлению аутсорсингом.
- Акцентирование внимания на культурные различия в организациях при составлении аутсорсинговой стратегии.
- Создание коллективов по выполнению надзорных функций за выполнением требований стандарта и стратегии.

Наибольший интерес с точки зрения управления конфликтом интересов представляет глава 9 стандарта ISO 37500, а именно п. 9.4 «Управление разногласиями и решение проблем (на ходу)». Основными направлениями деятельности в этом процессе являются:

1. Четкое определение и совместное принятие целей, которые должны лежать в основе аутсорсинговых отношений, а также должен быть организован способ разрешения вопросов и споров, с учетом установленных совместных целей взаимоотношений.
2. Документирование процессов регистрации, классификации, эскалации и передачи информации о проблемах и конфликтах, исходя из их уровня важности.
3. Согласование процесса эскалации вопросов и/или проблем, которые не могут быть решены с момента их возникновения до истечения установленного периода времени реагирования.
4. Ведение регистра/журнала проблем, включая действия по их регулированию, который будет рассмотрен в рамках соответствующего объединенного комитета по управлению. Клиент и поставщик должны работать вместе, чтобы разрешить проблемы.
5. Журнал проблем и журнал решений по проблемам должны быть возвращены обратно в системы управления знаниями, обеспечивающие будущие сделки.

Также большой интерес вызывает п. 9.9 «Управление отношениями». Основными направлениями деятельности в этом процессе являются:

1. Укрепление доверия между всеми заинтересованными сторонами.
2. Проверка, что клиент и поставщик четко представляют себе ожидаемое друг от друга поведение, в части обеспечения открытости, прозрачности и честной коммуникации в любое время.
3. Оценка отношений, которую следует использовать на регулярной основе для мониторинга силы и качества отношений. Как результаты, так и соответствующая зрелость проведения совместной работы должны быть оценены.
4. Обеспечение соответствия ожиданий эффективности согласованным требованиям с помощью регулярных проверок заинтересованных сторон.

8 ISO 37500:2014 Guidance on outsourcing

5. Рассмотрение и внедрение улучшений, согласованных совместной управленческой командой.

Далее в ISO 37500 следуют приложения к стандарту, которые являются частными руководствами по стандарту в целом и, по каждому этапу жизненного цикла аутсорсинга, в частности.

Рассмотрим теперь стандарты ISO 31000:2018 и IEC № 31010:2019. У данных стандартов есть Российские аналоги ГОСТ Р ИСО 31000 – 2019 и ГОСТ Р ИСО/МЭК 31010 – 2011 (копия старой версии ISO/IEC 31010 от 2008 года) замененный на ГОСТ Р 58771-2019.

Новая редакция стандарта ISO/IEC 31010 существенно отличается от предыдущей версии:

1. Количество методик оценки риска стало 41, вместо 31 в предыдущей редакции.
2. Используется другая классификация методик оценки риска. Вместо двух больших групп «Анализ сценариев» и «Анализ функциональности», а также ряда небольших и вспомогательных, методики сгруппированы в 10 групп, связанных с элементами процесса менеджмента риска. Такая классификация лучше гармонирует с ISO 31000:2018.
3. Также в ISO 31010:2019 предпринята новая попытка сравнения методик оценки риска с использованием метрики из 8 характеристик.

Данный стандарт, как никакой другой, позволяет выполнить оценку риска в социальной сфере, в том числе в сфере конфликта интересов, и интегрировать данную оценку в уже существующую систему оценки рисков.

На стандарт ISO 31000 ссылается относительно свежая версия стандарта ISO/IEC 27001:2013, который описывает требования к системам менеджмента информационной безопасности и может быть интегрирован в уже существующие системы менеджмента, основанные на стандартах ISO 9001, 14001, 20000 и других.

Опять же в России есть ГОСТ Р ИСО/МЭК 27001:2006, основанный на стандарте ISO 27001:2005 и являющийся его полной переведённой копией. Это в очередной раз показывает, что Российские стандарты в сфере оценки рисков и информационной безопасности основаны на международных стандартах и не успевают актуализироваться под быстро изменяющиеся мировые движения.

Далее приведена таблица 1, в которой была произведена попытка сопоставления требований из 273-ФЗ, Указания, ГОСТ Р ИСО/МЭК 27001 – 2006, ГОСТ Р ИСО/МЭК 22301 – 2019 и ГОСТ Р 57580.1 – 2017.

Стоит отметить, что стандарты ГОСТ ИСО/МЭК были взяты, как полные копии оригинальных стандартов ISO и полностью им идентичны.

### Преимущества и недостатки в отечественных и международных стандартах

*Преимущества:*

Стандарты ISO, ориентированные на системы менеджмента, совместимы и не имеют между собой конфликтов. В большинстве случаев подходы к решению похожих задач будут одинаковы, что упрощает их совместное использование. Также ИСО используют актуальные (и инновационные) подходы к решению задач (а именно, использование модели PDCA в жизненных циклах систем, новые походы к оценке рисков и др.). Имеют высокую ценность при сотрудничестве с зарубежными рынками товаров и услуг.

ГОСТ имеют подробное описание процессов и действий, а также низкую неопределенность в требованиях. Используются практики, проверенные временем и заработавшие положительную репутацию. Адаптированы под российские реалии и законодательные требования. Полностью локализованы под Россию.

*Недостатки:*

В Стандартах ISO большая часть требований описана в широком смысле, что с одной стороны дает свободу действия и вариативность, а с другой стороны оставляет большую неопределенность в самих требованиях. Использование новейших методик требует более тщательной подготовки к решению задач и более высокой подготовки кадров. Низкий уровень корреляции с Российским законодательством, не создает стимула к повсеместному использованию стандартов. Новые стандарты изданы только на иностранных языках.

ГОСТы зачастую сразу устаревают на пару десятков лет, что является причиной замедления в развитии организации. В них почти не обращается внимания на документирование деятельности организации, включая ее подразделений.

В обоих случаях слабо затрагивается вопрос ответственности кадрового состава за те или иные деяния. Низкий акцент на цифровизацию и использование технологий искусственного интеллекта.

### Предложения по решению вопроса конфликта интересов

Поскольку вопрос регулирования конфликта интересов набирает популярность [8-17], то внесение дополнительных правок в стандарты и законопроекты не заставит себя долго жать. Тем временем, выдвигается предложение к формированию базы по регулированию конфликта интересов на основе уже имеющихся требований и ресурсов.

В настоящее время в большинстве организаций вопросами конфликта интересов занимаются только комплаенс подразделения [18, 19]. Но вся их работа выполняется преимущественно со слов клиентов или работников организации, что в значительной степени уменьшает объективность принимаемых решений в силу невозможности наверняка убедиться в достоверности предоставляемой информации.

В крупных организациях принимаются автоматизированные системы по выявлению конфликта интересов при взаимодействии с клиентами, такие как:

- Платформа «IQPLATFORM»[9].
- Платформа «автоматизации внутреннего аудита, контроля и оценки рисков (АВАКОР)»[10].

9 Официальный сайт «Платформа IQPLATFORM» – URL: https://www.iqmen.ru/iqplatform (дата обращения: 10.04.2021)

10 Официальный сайт «Платформа «Авакор» – URL: https://digdes.ru/products/avtomatizatsiya-vnutrennego-audita-kontrolya-i-otsenki-riskov-avakor (дата обращения: 10.04.2021)

*Таблица 1*

*Соответствия в требованиях ФЗ, указания БР и стандартов*

| № п/п | Требование | ФЗ от 25.12.2008 № 273-ФЗ | Указания БР от 22.07.2020 № 5511-У | ГОСТ Р ИСО/МЭК 27001 – 2006, ГОСТ Р ИСО/МЭК 22301 – 2014 | ГОСТ Р 57580.1 – 2017 |
|---|---|---|---|---|---|
| **1** | Требования по комплексному анализу деятельности организации. | – | – | 27001, Глава 4, п. 4.1 – Организация должна разработать, внедрить ... документированную СМИБ применительно ко всей деловой деятельности организации и рискам. 22301, Глава 4, п. 4.1 – Высшее руководство должно установить политику непрерывности бизнеса. | Глава 6, п. 6.7 – Уровень защиты информации устанавливается на основе: вида деятельности, состава предоставляемых услуг, реализуемых бизнес-процессов и (или) технологических процессов... |
| **2** | Требования к политикам организации и внедряемым стандартам. | Статья 13.1, п. 2, п.п. 3 – рекомендует разработку и внедрение в практику стандартов и процедур, направленных на обеспечение добросовестной работы организации. | Приложение 1, п. 2 – Проведение мероприятий по обеспечению выявления конфликта интересов, осуществляется в порядке, определенном Политикой управления конфликтом интересов. | 27001, Глава 4, п. 4.2.1, п.п. b – определить политику СМИБ, которая: ... 2) принимает во внимание требования бизнеса, нормативно-правовые требования по обеспечению безопасности. 22301, Глава 4, п. 4.3.2 -При определении области применения организация должна документировать и обосновать все исключения... | Глава 6, п. 6.9, – Содержание политики обеспечения защиты информации должно определять: -цели и задачи; -основные типы защищаемой информации; -основные принципы и приоритеты... |
| **3** | Требования по идентификации риска. | – | – | 27001, Глава 4, п. 4.2.1, п.п. d – идентифицировать риски. 22301, Глава 6, п. 6.1 – При планировании СМНБ организация должна рассмотреть вопросы, упомянутые в 4.1 и 4.2 и определить риски и благоприятные возможности... 22301, Глава 8, п. 8.2.3. | Глава 6, п. 6.1, – Для управления операционным риском, связанным с безопасностью информации, необходимо обеспечить: ... оценку остаточного операционного риска... |

| № п/п | Требование | ФЗ от 25.12.2008 № 273-ФЗ | Указания БР от 22.07.2020 № 5511-У | ГОСТ Р ИСО/МЭК 27001 – 2006, ГОСТ Р ИСО/МЭК 22301 – 2014 | ГОСТ Р 57580.1 – 2017 |
|---|---|---|---|---|---|
| 4 | Требования по недопущению возникновения конфликта. | Статья 11 п. 1 –Должностное лицо обязано принимать меры по недопущению возникновения конфликта интересов. | Глава 2, п. 2.1 – Управляющая компания обязана выявлять конфликты интересов, возникающие при осуществлении деятельности, в том числе конфликты интересов. | 27001, Глава 4, п. 4.2.2, п.п. h – внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты… 27001, Глава 4, п. 4.2.3, п.п. a – … своевременно обнаруживать ошибки в результатах обработки; своевременно выявлять попытки нарушения и инциденты; способствовать обнаружению событий ИБ;… | Глава 7, п. 7.1, п.п. д – … процесс 5 «Предотвращение утечек информации»;… |
| 5 | Требования об уведомлении, о возникшем конфликте интересов. | Статья 11 п. 2 – Должностное лицо обязано уведомить работодателя о возникшем конфликте интересов или о возможности его возникновения, как только ему станет об этом известно. | Приложение 1, 5.1 – Фиксация не позднее одного рабочего дня после дня выявления конфликта интересов контролером финансовой организации следующей информации о конфликте интересов… | 27001, Глава 6 – Руководитель, ответственный за проверяемый участок деятельности организации, должен своевременно и без задержки обеспечить проведение проверки в целях устранения обнаруженных несоответствий и их причин. Последующие действия должны включать в себя проверку предпринятых действий и сообщение о результатах проверки. | Глава 7, п. 7.1, п.п. д – … процесс 5 «Предотвращение утечек информации»;… Глава 7, п.п. 7.7.2.3, мера РИ.9 – Своевременное (оперативное) оповещение членов ГРИЗИ о выявленных инцидентах защиты информации. |
| 6 | Требования по предотвращению конфликта интересов. | Статья 11 п. 3 – Работодатель обязан принять меры по предотвращению или урегулированию конфликта интересов, о котором ему известно. | Глава 1, п. 1.2 – Финансовая организация обязана осуществлять мероприятия по выявлению конфликта интересов. | 27001, Глава 6 – Руководитель… должен своевременно и без задержки обеспечить проведение проверки в целях устранения обнаруженных несоответствий и их причин. 22301, Глава 5, п. 5.2 – Организация должна: -сообщать результаты анализа со стороны руководства важным заинтересованным сторонам; -выполнять необходимые действия в соответствии с результатами. 22301, Глава 9, п. 9.3 – проведение регулярных проверок руководством. | Глава 7, п.п. 7.7.2.3, мера РИ.9 – определение роли: … руководитель ГРИЗИ, в обязанности которого входит обеспечение оперативного руководства реагированием на инциденты; … |

DOI: 10.21681/2311-3456-2021-4-48-60

| № п/п | Требование | ФЗ от 25.12.2008 № 273-ФЗ | Указания БР от 22.07.2020 № 5511-У | ГОСТ Р ИСО/МЭК 27001 – 2006, ГОСТ Р ИСО/МЭК 22301 – 2014 | ГОСТ Р 57580.1 – 2017 |
|---|---|---|---|---|---|
| **7** | Требования по урегулированию конфликта интересов. | Статья 11 п. 5 – Должностное лицо, обязано произвести отвод или самоотвода указанного лица в случаях конфликта интересов или личной заинтересованности. | В соответствии с законодательством РФ. | 27001, Глава 4, п. 4.2.1, п.п. d – идентифицировать риски, для чего необходимо: 1) ... определить владельцев активов... 22301, Глава 5, п. 5.4 – Высшее руководство должно обеспечить распределение ответственности и полномочий. | Глава 8, п.п. 8.3.1 – ...назначение ответственных лиц... Приложение Б, мера Б.18 – В финансовой организации должно быть назначено лицо, ответственное за организацию обработки ПДн. |
| **8** | Ответственность за неверное действие или бездействие в ситуации с конфликтом интересов. | Статья 11 п. 6 – Непринятие Должностным лицом, являющимся стороной конфликта интересов, мер по предотвращению или урегулированию конфликта интересов является правонарушением. | В соответствии с законодательством РФ. | | |
| **9** | Требования об уведомлении о призывах к правонарушениям или личной заинтересованности. | Статья 11.1 – ... обязаны уведомлять об обращении к ним каких-либо лиц в целях склонения к совершению коррупционных правонарушений, о возникновении личной заинтересованности, которая приводит к конфликту интересов. | В соответствии с законодательством РФ. | | |
| **10** | Административная ответственность. | Статья 13 – В случае не соблюдения Должностным лицом положений по урегулированию конфликта интересов, лицо считается утратившим доверие и подлежит увольнению. | В соответствии с законодательством РФ. | В соответствии с законодательством РФ. | В соответствии с законодательством РФ. |

| № п/п | Требование | ФЗ от 25.12.2008 № 273-ФЗ | Указания БР от 22.07.2020 № 5511-У | ГОСТ Р ИСО/МЭК 27001 – 2006, ГОСТ Р ИСО/МЭК 22301 – 2014 | ГОСТ Р 57580.1 – 2017 |
|---|---|---|---|---|---|
| **11** | Меры по предотвращению конфликта интересов. | Статья 13.3 – ...: предотвращение и урегулирование конфликта интересов;... | Приложение 1, п. 2.1 – Определение лицом, ответственным за выявление конфликта интересов, контролера финансовой организации. Приложение 1, п. 6. Приложение 1, п. 12. | 22301, Глава 8, п. 8.4.3 – Процедуры обмена информацией и предупреждения необходимо регулярно проверять. | Глава 7, п.п. 7.2. |
| **12** | Требования по повышению осведомленности и квалификации персонала. | Статья 6 – ...: формирование в обществе нетерпимости к коррупционному поведению; антикоррупционная экспертиза правовых актов и их проектов... Статья 6 –– Сведения о применении к лицу взыскания в виде увольнения в связи с утратой доверия ..., подлежат включению в специальный реестр, сроком на пять лет. | – | 27001, Глава 5, п. 5.4.2. – Организация должна обеспечить необходимую квалификацию персонала, на который возложены обязанности выполнения задач в рамках СМИБ... 22301, Глава 7, п. 7.2 – Организация должна: определить необходимую компетентность работников, ...; обеспечить компетентность людей посредством обучения, проведения учений и обмена опытом... 22301, Глава 7, п. 7.3 – Персонал, осуществляющий работу под контролем организации, должен знать: ... c) последствия, которые могут возникнуть в случае несоответствия требованиям СМНБ; d) свои функции в случае разрушительных инцидентов. | Глава 7, п.п. 7.7.2.3, мера РИ.9 – Своевременное оповещение членов ГРИЗИ о выявленных инцидентах. Глава 8, п.п. 8.3.1 – В рамках направления «Реализация» финансовая организация обеспечивает: обучение, практическую подготовку работников, ответственных за применение мер защиты информации; повышение осведомленности работников в области защиты информации. |

DOI: 10.21681/2311-3456-2021-4-48-60

| № п/п | Требование | ФЗ от 25.12.2008 № 273-ФЗ | Указания БР от 22.07.2020 № 5511-У | ГОСТ Р ИСО/МЭК 27001 – 2006, ГОСТ Р ИСО/МЭК 22301 – 2014 | ГОСТ Р 57580.1 – 2017 |
|---|---|---|---|---|---|
| **13** | Требования по регулярному проведению проверок. | Статья 13.4. – Осуществление проверок уполномоченным подразделением Администрации Президента Российской Федерации. | Приложение 1, п. 14 – Контроль и значительное влияние определяются в соответствии с Международными стандартами финансовой отчетности, введенными в действие на территории Российской Федерации... | 27001, Глава 6 – Организация должна в соответствии проводить внутренние аудиты СМИБ, позволяющие установить, что цели ... СМИБ: соответствуют требованиям стандарта и соответствующим законам или нормативным документам;... | Глава 7, п.п. 8.4.2, мера КЗИ.7 – Проведение проверок знаний работников. |
| **14** | Требования к документированию. | Статья 13.1, п. 2, п.п. 5 – возможная мера противодействия коррупции: недопущение составления неофициальной отчетности и использования поддельных документов. | Приложение 1, п. 10 – Мероприятия по хранению информации и документов, подтверждающих соответствие деятельности финансовой организации по выявлению конфликта интересов и управлению конфликтом интересов ... и обеспечивающие хранение указанных информации и документов не менее трех лет со дня прекращения конфликта интересов. | 27001, Глава 6 – ... Правила и требования, относящиеся к планированию, проведению аудита... должны быть документированы. 27001, Глава 4, п. 4.3.3. 22301, Глава 4, п. 4.1 – Организация должна идентифицировать и документировать следующее: ... взаимодействия с заинтересованными сторонами, потенциально уязвимые по отношению к разрушительному инциденту;... 22301, Глава 5, п. 5.2 – Организация должна сохранять документацию ... 22301, Глава 7, п. 7.5. | Глава 7, п.п. 7.7.2.3, мера РИ.9 – определение роли: ... секретарь ГРИЗИ, в обязанности которого входит документирование результатов реагирования на инциденты... |

- Платформа «Контур.Фокус»[11].
- Платформа «НЕКСТБИ Аналитика» – система противодействия мошенничеству»[12].

Во всех описанных программных продуктах есть функционал построения графов связности, функционал по их анализу и составлению отчетности. Недостатком и ограничением данного вида продуктов является обработка только различных клиентских или пользовательских данных, предоставляемых ими самостоятельно или опубликованных в открытых источниках.

Также, в некоторых продуктах реализованы средства по сбору данных о физических и юридических лицах с целью проверки их упоминания в различных открытых базах данных (например, база террористов), и выявлению наличия связей между ними.

Указанные продукты требуют доработки под инфраструктуру каждого предприятия, а также являются дорогостоящими. Обработку же результатов выполняет ответственное лицо за управление конфликтом интересов. Это лицо тоже, в свою очередь, может иметь личную заинтересованность в решении конфликта.

Главным недостатком всех этих программных средств является невозможность анализировать конфликт интересов в пределах работников организации [20, 21]. В силу специфики самих конфликтов (конфликты могут не включать близких или родственных связей, а основываться на межличностных отношениях или психологическом состоянии работников), эти процедуры сводятся к ручному труду, либо вовсе не выполняются из-за отсутствия информации о социальном климате внутри отделов. Это, в свою очередь, является серьёзной угрозой информационной безопасности, о чем написано далее.

## Конфликт интересов в информационной безопасности

С точки зрения информационной безопасности, конфликт интересов может быть причиной нанесения ущерба целостности, конфиденциальности и доступности информации организации. Именно на базе конфликта интересов рождаются многочисленные инсайдерские диверсии по отношению к информационным системам (нарушение работоспособности, несанкционированный удаленный доступ и др.), утечки данных организации после увольнения работника и так далее.

В результате ненадлежащего управления конфликтом интересов у организаций могут реализоваться следующие виды рисков:

- Правовой риск (например, несоответствие законодательным и регуляторным требованиям).
- Репутационный риск (например, риск потери деловой репутации).
- Риск материальных и финансовых потерь (например, риск утраты клиентской базы и выгодных договоров).

Любое подразделение по обеспечению информационной безопасности решает вопросы по урегулированию конфликта интересов, в той или иной мере, на всех стадиях жизни организации, при использовании системы менеджмента информационной безопасности.

В ГОСТ Р ИСО/МЭК 27001:2006 года описан ряд позиций, косвенно связанных с регулированием конфликта интересов. Такими положениями являются п.п. 4.2.3 и 4.3.2, описывающие необходимость отслеживать операционные ошибки и документооборот в организации.

Именно на основе этих процедур можно начать формировать базу по автоматизированному анализу конфликта интересов и враждебности окружающей среды для работника. Имеется в виду анализ действий работника на наличие психологической нестабильности, которая может привести к конфликту среди работников, а также оценка враждебности среды в организации.

Также управление конфликтом интересов можно рассматривать как средство снижения реализации, по меньшей мере, половины рисков информационной безопасности, связанных с пользователями, а сам конфликт интересов как одна из возможных причин реализации риска ИБ.

В ГОСТ Р 57580.1 – 2017 тоже есть косвенная связь с управлением конфликтом интересов. Одним из примеров может являться п. 6.10, описывающий принципы, используемые при предоставлении доступа к защищаемой информации:

- «Знать своего клиента»: принцип, реализация которого в основном направлена на обладание информацией в отношении благонадежности клиента, его основных потребностей, отсутствия его незаконной или нелегальной деятельности.
- «Знать своего работника»: принцип, реализация которого в основном направлена на обладание информацией об отношении работников финансовой организации к их служебным обязанностям, наличии у них возможных проблем, в том числе финансовых, имущественных или личных, которые могут потенциально привести к действиям, направленным на нарушение требований к защите информации.
- «Необходимо знать»: принцип, реализация которого в основном направлена на ограничение прав логического и (или) физического доступа работников финансовой организации на уровне, минимально необходимом для выполнения служебных обязанностей.
- «Двойное управление»: принцип, реализация которого в основном направлена на сохранение целостности и неизменности информации путем дублирования действий субъектов доступа в рамках реализации финансовых операций и транзакций, выполняемого до их окончательного завершения.

Но методической базы, позволяющей эффективно следовать данным принципам (то есть получать точный результат за короткое время), нет. В большинстве случаев эти операции просто описываются на бумаге.

Основная проблема оперативности предупреждения потенциального конфликта интересов сводится к автоматизированной обработке разрозненных массивов данных конфиденциального характера (служебная переписка, логи сетевого трафика, информация о доку-

11 Официальный сайт «Контур.Фокус» – URL: https://focus.kontur.ru/ (дата обращения: 10.04.2021)

12 Официальный сайт «Платформа «НЕКСТБИ Аналитика» – Система противодействия мошенничеству» – URL: https://nextbi.ru/ (дата обращения: 10.04.2021)

ментообороте, персональные данные и др.). Это, в свою очередь, накладывает ряд ограничений с точки зрения безопасности информации, например, необходимость обезличивания персональных данных.

Также, в предупреждении конфликта интересов помогают средства сбора и анализа информации из открытых источников, и средства построения деревьев связей между работниками и клиентами банка. Примеры таких средств были описаны выше.

**Выводы**

Существующие подходы к предотвращению конфликта интересов обладают рядом ограничений. Учитывая повышение требований к качеству предоставляемых услуг и требования регуляторов, необходимо существенное снижение информационных, операционных и кадровых рисков, возникающих вследствие конфликта интересов внутри структуры организации. Современное состояние науки и техники позволяет автоматизировать процессы выявления и предсказания конфликтов интересов за счет использования аппарата математической статистики, применения технологий машинного обучения и распознавания текста (звука).

Исследование темы конфликта интересов направлено на минимизацию возможных финансовых, имиджевых и кадровых потерь из-за конфликтов интересов, а также разработку методического аппарата по отслеживанию и противодействию конфликтам. В ближайшем будущем данная тема будет набирать популярность в силу клиент ориентированности всех сфер деятельности и повсеместной автоматизации бизнес-процессов.

По результатам исследования и сопоставления требований ФЗ-273 и стандартов по системам менеджмента и информационной безопасности можно сделать вывод о том, что необходима модернизация действующих стандартов по информационной безопасности и системам менеджмента. Положениями, требующими внимания при модернизации, являются: более четкое распределение ответственности, методы и способы внедрения информационных систем с искусственным интеллектом и алгоритмами машинного обучения, также описание подразделений по урегулированию конфликтных ситуаций.

**Литература**


1. Лихолетов В.В., Пестунов М.А. Псевдоинновации и конфликты интересов в инновационной сфере современной России как угроза национальной безопасности // Управление в современных системах. 2020. N 4(28). С. 89–99. DOI: 10.24411/2311-1313-2020-10016.
2. Шумкин Е.М. Управленческая деятельность актора, как потенциал конфликта интересов: конвергентный подход // Вестник пермского университета. Философия. Психология. Социология. 2020. № 1. С. 152–161. DOI: 10.17072/2078-7898/2020-1-152-161.
3. Капинус О.С. Правовые проблемы предупреждения конфликта интересов в системе государственного управления // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 3. С. 15–19. DOI: 10.12737/art.2018.3.3.
4. Охотский Е.В. Понятие «конфликт интересов» в административном праве Российской Федерации // Право и управление. XXI Век. 2019. № 4(53). Т 19. С. 118–129. DOI: 10.24833/2073-8420-2019-4-53-118-129.
5. Полтавцева М.А. Модель активного мониторинга как основа управления безопасностью промышленных киберфизических систем // Вопросы кибербезопасности. 2021. № 2. С. 51–60. DOI: 10.21681/2311-3456-2021-2-51-60.
6. Кубарев А.В., Лапсарь А.П., Асютиков А.А. Синтез модели объекта критической информационной инфраструктуры для безопасного функционирования технической системы в условиях деструктивного информационного воздействия // Вопросы кибербезопасности. 2020. № 6. С. 48–56. DOI: 10.681/2311-3456-2020-06-48-56.
7. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Формализованная риск-ориентированная модель системы информационных технологий // Вопросы кибербезопасности. 2020. № 5. С. 69–76. DOI: 10.21681/2311-3456-2020-05-69-76.
8. Головкин Б.Н., Белецкий А.В. Конфликт интересов как фактор коррупции // Norwegian Journal of development of the International Science. 2018. № 2. С. 68–71.
9. Деев И.А. Конфликт интересов: читатель решит сам // Вопросы современной педиатрии. 2016. № 15(6). С. 547. DOI: 1010.15690/vsp.v15i6.1647.
10. Луцкая Н.В. Аутсорсинг и инсорсинг как взаимодополняющие инструменты менеджмента для формирования оптимальной организационной структуры предприятий // Стратегическое планирование и развитие предприятий. 2016. № 2. С. 41–57.
11. Карцева К.Г., Каткова В.А., Тупикова В.А. Конфликт интересов на государственной службе как социальный конфликт // Актуальные исследования. 2019. № 3. С. 94–97.
12. Husham A., Manickam S., Alqattan Z. Threats Against Information Privacy and Security in Social Networks: A Review. // Advances in Cyber Security (Part of the CCIS). 2020. С. 358–372. DOI: 10.1007/978-981-15-2693-0_26.
13. Oloomi, Farideh & Masoumi, Razieh & Karimipour, K. & Hosseiny, Ali & Jafari, G. Competitive balance theory: Modeling conflict of interest in a heterogeneous network. Physical Review E. 2021. С. 103. DOI: 10.1103/PhysRevE.103.022307.
14. Baygildin, S. & Musina, L. & Khismatullina, Z. Conflict of interest: the authors declare no conflict of interest // Journal Biomed. 2021. С. 70–81. DOI: 10.33647/2074-5982-17-1-70-81.
15. Curi, F., Nikolopoulos, D. and Araújo, E. A Social Network Model for Integration of Refugees. // Proceedings of the 9th International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2019). 2019. С. 165–175. DOI: 10.5220/0007930601650175.
16. Михайлов В.И. Конфликт интересов: вопросы этики и совершенствования законодательного оформления // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 3. С. 26–31. DOI: 10.12737/ art.2018.3.5.

17. Паулов П.А., Утепкалиева К.Х. Меры по борьбе с проявлением коррупции сквозь призму конфликта интересов // Юридическая наука. 2020. № 5. С. 51–53.
18. Хабриева Т.Я. Конфликт интересов: природа, предупреждение, социальное регулирование // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 3. С. 5–12. DOI: 10.12737/art.2018.3.1.
19. Чертов В.А., Сигарев С.И. Анализ организационно-управленческой структуры трудового коллектива в интересах выявления причин возникновения внутрифирменных конфликтов // Вестник российского нового университета. Серия: сложные системы: модели, анализ и управление. 2020. № 2. С. 114–121. DOI: 10.25586/ RNoU.V9187.20.02.P.114.
20. Ниязова И.М. Конфликты интересов как составляющая часть конфликтогенности в организации // Human progress. 2020. № 1. С. 6. DOI: 10.34709/IM.161.6.
21. Красильникова Е.О. Риски в системе корпоративного управления // Бизнес-образование в экономике знаний. 2018. № 3. С. 66–70.
22. Triki, Salah & Ben-Abdallah , Hanene & Feki, J. & Harbi, Nouria. (2010). Modeling Conflict of Interest in the Design of Secure Data Warehouses. С. 445–448. URL: https://www.researchgate.net/publication/220802211_Modeling_Conflict_of_Interest_in_the_Design_of_Secure_Data_Warehouses (дата обращения: 10.03.2021).
23. Пат. 8225218 Соединенные Штаты Америки, МПК G 06 F 3/00. Methods and systems for identifying, assessing and clearing conflicts of interest / Yuri Danilov; Serge Hug; Alp. заявитель и патента обладатель The Frayman Group, Inc. № 43880079; заявл. 19.02.10; опубл. 17.07.12. URL: https://patents.google.com/patent/US8225218B2/ en?oq=8225218 (дата обращения: 10.03.2021).
24. Пат. 2697963 Российская Федерация, МПК G 06 Q 50/18. Способ оценки сделки клиента с контрагентом на предмет конфликта интересов / Подласов М.С.; заявитель и патента обладатель АО «Лаборатория Касперского». № 2018111483; заявл. 30.03.18; опубл. 21.08.19. URL: https://yandex.ru/patents/doc/RU2697963C1_20190821 (дата обращения: 15.03.2021).
25. Herbert, S. Conflict analysis: Topic guide. Birmingham, UK: GSDRC, University of Birmingham. 2017. // Официальный сайт GSDRC, University of Birmingham – URL: https://gsdrc.org/wp-content/uploads/2017/05/ConflictAnalysis.pdf (дата обращения: 16.03.2021).

# CONFLICT OF INTEREST RESOLUTION REGULATORY DOCUMENTATION REQUIREMENTS ANALYSIS IN THE CONTEXT OF INFORMATION SECURITY

***Alekseev A.D.[13], Vorobeva A.A.[14], Livshitz I.I. [15], Yurin I.V.[16]***

***Research aim:*** *analysis and assessment of the level of readiness of the requirements for the regulation of conflicts of interest contained in the current standards of the Russian Federation on information security and management systems, for compliance with national legislation, as well as their comparison with the requirements of ISO standards.*

***Research method:*** *a comprehensive analysis of regulating conflicts of interest problem was carried out the regulatory framework of the Russian Federation (273-FZ, Bank of Russia Ordinances No. 5511-U and standards for management systems and information security). The requirements contained in the national standards of the Russian Federation and international ISO standards are analyzed for their mutual correspondence.*

***Results obtained:*** *The research presents the comparison of the requirements of the federal law of the Russian Federation FZ-273 and standards for management systems and information security. Comparative table of requirements for resolving conflicts of interest is presented. The existing software of automated search and analysis of conflicts of interest are analyzed. It is proposed to use of modern automated tools for regulation of conflicts of interest in organizations.*

***Keywords:*** *conflict of interest, federal law, information security, standard, GOST, ISO, corruption, Bank of Russia, software, conflict of interest analysis.*

## References

1. Leeholetov V.V., Pestunov M.A. Psevdoinnovatcii i konflikty` interesov v innovatcionnoi` sfere sovremennoi` Rossii kak ugroza natcional`noi` bezopasnosti // Upravlenie v sovremenny`kh sistemakh. 2020. N 4(28). S. 89–99. DOI: 10.24411/2311-1313-2020-10016.
2. Shumkin E.M. Upravlencheskaia deiatel`nost` aktora, kak potentcial konflikta interesov: konvergentny`i` podhod // Vestneyk permskogo universiteta. Filosofiia. Psihologiia. Sotciologiia. 2020. № 1. S. 152–161. DOI: 10.17072/2078-7898/2020-1-152-161.

13 Andrei Alekseev, student at ITMO University, St. Petersburg, Russia. E-mail: andalexs@yandex.ru
14 Alice Vorobeva, Ph.D., Associate Professor, ITMO University, Saint Petersburg, Russian Federation. E-mail: Alice_w@mail.ru
15 Ilya Livshitz, Dr.Sc., Associate Professor, Professor of Information Technology Security at ITMO University, St. Petersburg, Russia. E-mail: Livshitz.il@yandex.ru
16 Igor Yurin, Ph.D., Associate Professor, ITMO University, Admiral Makarov SUMIS, Saint Petersburg, Russian Federation. Email: 9402015@mail.ru

3. Kapinus O.S. Pravovy`e problemy` preduprezhdeniia konflikta interesov v sisteme gosudarstvennogo upravleniia // Zhurnal zarubezhnogo zakonodatel`stva i sravnitel`nogo pravovedeniia. 2018. № 3. C. 15–19. DOI: 10.12737/art.2018.3.3.
4. Ohotskii` E.V. Poniatie «konflikt interesov» v administrativnom prave Rossii`skoi` Federatcii // Pravo i upravlenie. XXI Vek. 2019. № 4(53). T 19. C. 118–129. DOI: 10.24833/2073-8420-2019-4-53-118-129.
5. Poltavtceva M.A. Model` aktivnogo monitoringa kak osnova upravleniia bezopasnost`iu promy`shlenny`kh kiberfizicheskikh sistem // Voprosy` kiberbezopasnosti. 2021. № 2. C. 51–60. DOI: 10.21681/2311-3456-2021-2-51-60.
6. Kubarev A.V., Lapsar` A.P., Asiutikov A.A. Sintez modeli ob``ekta kriticheskoi` informatcionnoi` infrastruktury` dlia bezopasnogo funktcionirovaniia tekhnicheskoi` sistemy` v usloviiakh destruktivnogo informatcionnogo vozdei`stviia // Voprosy` kiberbezopasnosti. 2020. № 6. C. 48–56. DOI: 10.681/2311-3456-2020-06-48-56.
7. Anosov R.S., Anosov S.S., Shahalov I.Iu. Formalizovannaia risk-orientirovannaia model` sistemy` informatcionny`kh tekhnologii` // Voprosy` kiberbezopasnosti. 2020. № 5. C. 69–76. DOI: 10.21681/2311-3456-2020-05-69-76.
8. Golovkin B.N., Beletckii` A.V. Konflikt interesov kak faktor korruptcii // Norwegian Journal of development of the International Science. 2018. № 2. C. 68–71.
9. Deev I.A. Konflikt interesov: chitatel` reshit sam // Voprosy` sovremennoi` pediatrii. 2016. № 15(6). C. 547. DOI: 1010.15690/vsp.v15i6.1647.
10. Lutckaia N.V. Autsorsing i insorsing kak vzaimodopolniaiushchie instrumenty` menedzhmenta dlia formirovaniia optimal`noi` organizatcionnoi` struktury` predpriiatii` // Ctrategicheskoe planirovanie i razvitie predpriiatii`. 2016. № 2. C. 41–57.
11. Kartceva K.G., Katkova V.A., Tupikova V.A. Konflikt interesov na gosudarstvennoi` sluzhbe kak sotcial`ny`i` konflikt // Aktual`ny`e issledovaniia. 2019. № 3. C. 94–97.
12. Husham A., Manickam S., Alqattan Z. Threats Against Information Privacy and Security in Social Networks: A Review. // Advances in Cyber Security (Part of the CCIS). 2020. S. 358–372. DOI: 10.1007/978-981-15-2693-0_26.
13. Oloomi, Farideh & Masoumi, Razieh & Karimipour, K. & Hosseiny, Ali & Jafari, G. Competitive balance theory: Modeling conflict of interest in a heterogeneous network. Physical Review E. 2021. S. 103. DOI: 10.1103/PhysRevE.103.022307.
14. Baygildin, S. & Musina, L. & Khismatullina, Z. Conflict of interest: the authors declare no conflict of interest // Journal Biomed. 2021. S. 70–81. DOI: 10.33647/2074-5982-17-1-70-81.
15. Curi, F., Nikolopoulos, D. and Araújo, E. A Social Network Model for Integration of Refugees. // Proceedings of the 9th International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2019). 2019. S. 165–175. DOI: 10.5220/0007930601650175.
16. Mihai`lov V.I. Konflikt interesov: voprosy` e`tiki i sovershenstvovaniia zakonodatel`nogo oformleniia // Zhurnal zarubezhnogo zakonodatel`stva i sravnitel`nogo pravovedeniia. 2018. № 3. C. 26–31. DOI: 10.12737/ art.2018.3.5.
17. Paulov P.A., Utepkalieva K.KH. Mery` po bor`be s proiavleniem korruptcii skvoz` prizmu konflikta interesov // Iuridicheskaia nauka. 2020. № 5. C. 51–53.
18. Habrieva T.Ia. Konflikt interesov: priroda, preduprezhdenie, sotcial`noe regulirovanie // Zhurnal zarubezhnogo zakonodatel`stva i sravnitel`nogo pravovedeniia. 2018. № 3. C. 5–12. DOI: 10.12737/art.2018.3.1.
19. Chertov V.A., Sigarev S.I. Analiz organizatcionno-upravlencheskoi` struktury` trudovogo kollektiva v interesakh vy`iavleniia prichin vozniknoveniia vnutrifirmenny`kh konfliktov // Vestneyk rossii`skogo novogo universiteta. Seriia: slozhny`e sistemy`: modeli, analiz i upravlenie. 2020. № 2. C. 114–121. DOI: 10.25586/ RNoU.V9187.20.02.P.114.
20. Niiazova I.M. Konflikty` interesov kak sostavliaiushchaia chast` konfliktogennosti v organizatcii // Human progress. 2020. № 1. C. 6. DOI: 10.34709/IM.161.6.
21. Krasil`nikova E.O. Riski v sisteme korporativnogo upravleniia // Biznes-obrazovanie v e`konomike znanii`. 2018. № 3. C. 66–70.
22. Triki, Salah & Ben-Abdallah , Hanene & Feki, J. & Harbi, Nouria. (2010). Modeling Conflict of Interest in the Design of Secure Data Warehouses. C. 445–448. URL: https://www.researchgate.net/publication/220802211_Modeling_Conflict_of_Interest_in_the_Design_of_Secure_Data_Warehouses (data obrashcheniia: 10.03.2021).
23. Pat. 8225218 Soedinenny`e Shtaty` Ameriki, MPK G 06 F 3/00. Methods and systems for identifying, assessing and clearing conflicts of interest / Yuri Danilov; Serge Hug; Alp. zaiavitel` i patenta obladatel` The Frayman Group, Inc. № 43880079; zaiavl. 19.02.10; opubl. 17.07.12. URL: https://patents.google.com/patent/US8225218B2/ en?oq=8225218 (data obrashcheniia: 10.03.2021).
24. Pat. 2697963 Rossii`skaia Federatciia, MPK G 06 Q 50/18. Sposob ocenki sdelki clienta s kontragentom na predmet konflikta interesov / Podlasov M.S.; zaiavitel` i patenta obladatel` AO “Laboratoriia Kasperskogo”. № 2018111483; zaiavl. 30.03.18; opubl. 21.08.19. URL: https://yandex.ru/patents/doc/RU2697963C1_20190821 (data obrashcheniia: 15.03.2021).
25. Herbert, S. Conflict analysis: Topic guide. Birmingham, UK: GSDRC, University of Birmingham. 2017. // Ofitcial`ny`i` sai`t GSDRC, University of Birmingham – URL: https://gsdrc.org/wp-content/uploads/2017/05/ConflictAnalysis.pdf (data obrashcheniia: 16.03.2021).