

Применение положений концепций COSO и COBIT при организации внутреннего контроля

Application of COSO and COBIT Frameworks for the Purpose of Organization of Internal Control

УДК 657.6

DOI: 10.12737/1998-0701-2021-7-5-15-23

Нгуен Тхи Ха Ми, аспирантка Факультета налогов, аудита и бизнес-консалтинга, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»

e-mail: camilla.nguyen.thi@gmail.com

Nguyen Thi Ha My, Postgraduate Student, Faculty of Taxes, Audit and Business-Analysis, Financial University under the Government of the Russian Federation

e-mail: camilla.nguyen.thi@gmail.com

Научный руководитель:

М.В. Мельник, д-р экон. наук, профессор, профессор Факультета налогов, аудита и бизнес-консалтинга, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»

Scientific Advisor:

M.V. Melnik, Doctor of Economic Sciences, Professor, Faculty of Taxes, Audit and Business-Analysis, Financial University under the Government of the Russian Federation

Аннотация. В данной статье проанализирована релевантность концепции COBIT для целей организации внутреннего контроля и предложена схема интеграции концепций COBIT и COSO: взаимосвязаны положения двух концепций через понятия «процесс» и «информационные потоки». Также в статье рассмотрено применение интегрированной концепции в условиях внедрения принципов устойчивого развития в деятельность организации.

Ключевые слова: система внутреннего контроля, внутренний контроль, информационные системы, концепции COSO, COBIT.

Abstract. This article analyzes the relevance of this framework for the purposes of organizing internal control and proposes a scheme for integrating COBIT and COSO frameworks: the theses of these two frameworks are interconnected through the concepts of «process» and «information flows». The article also considers the application of the integrated concept in the context of the implementation of the principles of sustainable development in the activities of the organization.

Keywords: internal control system, internal control, information systems, COSO framework, COBIT.

Одним из ключевых понятий рыночной экономики является конкуренция. Уникальные характеристики, выгодно отличающие конкретный экономический субъект от других игроков рынка, варьируются в зависимости от отрасли, региона и других факторов, однако неотъемлемым условием конкурентоспособности является наличие эффективного контроля за деятельностью экономического субъекта. Вопрос организации системы внутреннего контроля (СВК) становится все более актуальным ввиду тесной взаимосвязи эффективности внутреннего контроля и результатов деятельности экономического субъекта, а также относительной контролируемости данного аспекта в отличие от макроэкономических факторов его деятельности.

Проблема постановки и поддержания эффективной системы внутреннего контроля является предметом исследований многих специалистов, тем не менее существующие концепции не дают четких указаний по ее организации.

Модель внутреннего контроля COSO

Наиболее распространенной среди организаций коммерческого сектора является модель внутреннего контроля Комитета организаций-спонсоров Комиссии Тредвея (COSO). Основные положения данной модели нашли отражение в нормативно-правовой базе ряда стран, в том числе и в России, а именно — в Информации Минфина РФ ПЗ-11/2013 [1]. Обычно модель COSO

представляется в виде куба, основными элементами которого являются пять компонентов: контрольная среда, оценка рисков, процедуры внутреннего контроля, информация и коммуникация, мониторинг (см. рис. 1).

Причины широкого распространения данной концепции заключаются в следующих ее особенностях.

1. Универсальность концепции. Представленные в модели COSO компоненты внутреннего контроля в той или иной мере характерны для всех экономических субъектов. Так, например, даже в компаниях без формализованных политик может существовать контрольная среда, заключающаяся в неформальном инструктировании сотрудников. Вариативность способов организации компонентов внутреннего контроля позволяет компаниям адаптировать модель COSO под собственные нужды и возможности. Дополнительным преимуществом является возможность сравнения систем внутреннего контроля организаций на основании элементов внутреннего контроля, выделенных в модели COSO.

2. Взаимосвязь между рисками организации и процедурами внутреннего контроля. В концепции COSO акцент делается на взаимосвязи рисков и контрольных процедур. Одним из ключевых элементов модели является матрица рисков и контрольных действий, представляющая собой свод рисков и перечень контрольных действий, направленных на их митигирование. Данный подход позволяет связывать факторы, влияющие на бизнес, и действия организации: в процессе сопоставления рисков и контрольных процедур обозначается цель каждого действия и исключаются процедуры, не приносящие пользы компании.

3. Применимость контрольных действий для разнообразных бизнес-процессов. Несмотря на то, что компании могут кардинально отличаться друг от друга ввиду отраслевой, региональной специфики, контрольные действия, проводимые для митигирования различных рисков, схожи по своей сути. Вне зависимости от того, кто, с какой частотой и в отношении каких объектов выполняет контрольные действия, их перечень ограничивается следующим: разграничение полномочий и ротация обязанностей, сверка, документальное оформление, подтверждение

соответствия между объектами, санкционирование, контроль фактического наличия и состояния, надзор за достижением целей, процедуры, связанные с компьютерной обработкой информации.

В то же время, применение концепции COSO на практике связано с определенными проблемами, основными из которых являются следующие.

1. Абстрактность понятий. В концепции COSO отсутствуют четкие указания по организации внутреннего контроля, в том числе и в отношении такого важного аспекта, как объект контроля. Исходя из определения внутреннего контроля, можно сделать вывод, что целью контроля является обеспечение результативности и эффективности деятельности организации, достоверности отчетности и соблюдения законов и правил, следовательно, объектом внутреннего контроля является деятельность экономического субъекта. В то же время на практике нередко требуется необходимо дальнейшее дезагрегирование понятия «деятельность организации».

2. Слабое акцентирование на взаимосвязи всех компонентов внутреннего контроля между собой. Наибольшее внимание в модели COSO уделяется вопросу взаимодействия двух элементов контроля — «Оценка рисков» и «Контрольные процедуры», при этом зачастую компаниями упускаются вопросы взаимосвязи остальных компонентов системы внутреннего контроля. В самой модели не приводятся детальные рекомендации по организации внутреннего контроля, в связи с чем вопрос эффективности СВК во многом зависит от интерпретации экономическими субъектами положений стандартов и нормативно-правовых актов.

3. Отсутствие взаимосвязи с новыми тенденциями на рынке. Одним из последствий универсальности концепции является то, что в ней не отражены новшества, возникающие в экономической среде, а следовательно, не учитываются потенциальные возможности и проблемы внутреннего контроля, связанные с новыми тенденциями. Таким образом, отражение изменений на рынке полностью зависит от уровня компетенции сотрудников, отвечающих в компании за оценку рисков.



Таким образом, концепция COSO применима как основа для постановки внутреннего контроля, однако для адаптации СВК к изменяющимся условиям окружающей среды необходимо своевременное отслеживание тенденций на рынке и инкорпорирование соответствующих изменений в систему внутреннего контроля.

Концепция COBIT

В связи с возрастающим влиянием информационных технологий были разработаны новые концепции, посвященные руководству и управлению за информацией и технологиями. Одной из самых распространенных в этой области концепций является COBIT (Control Objectives for Information and Related Technologies — «Задачи управления для информационных и смежных технологий»).

Будучи впервые опубликованной Ассоциацией по аудиту и контролю информационных систем (ISACA) в 1996 году, концепция COBIT нацелена на эффективное использование информации и технологий для максимизации их ценности для стейкхолдеров организации, оптимизации ресурсов для проведения трансформации бизнеса, оценки и митигирования рисков деятельности. Согласно определению, данному Ассоциацией по аудиту и контролю информационных систем, *внутренний контроль — это совокупность политик, процедур, практик и организационных структур, разработанных для обеспечения достаточной уверенности в том, что бизнес-цели экономического субъекта будут достигнуты, а непредвиденные события будут предотвращены или выявлены и скорректированы*. Данное определение внутреннего контроля не противоречит термину, приведенному в концепции COSO, и также ставит во главу угла достижение экономическим субъектом поставленных целей. Авторы концепции акцентируют внимание на возможности интеграции COBIT с другими доктринами. Последняя версия COBIT (COBIT 2019) учитывает положения других стандартов, концепций и правил, в частности, таких как: Концепция управления рисками COSO (COSO ERM), Европейская рамка ИКТ-компетенций (European e-Competence Framework), Масштабированный гибкий фреймворк (Scaled Agile Framework). Таким образом, COBIT — это

единая интегрированная методология, вобравшая в себя элементы различных стандартов и авторских методик.

В основе концепции COBIT лежат руководство и управление информацией и технологиями, используемыми экономическими субъектами для достижения своих целей. При этом в ней четко разграничиваются понятия «руководство» и «управление»:

- *руководство* (governance) осуществляется Советом директоров и иными высшими органами, направлено на оценку и анализ потребностей стейкхолдеров и условий окружающей среды и преобразование их в стратегию и цели организации;

- *управление* (management) производится менеджментом более низкого уровня и заключается в планировании, выполнении и мониторинге операций в соответствии с направлениями, выделенными руководством (governance).

Таким образом, проводится разделение целей руководства и менеджмента организации: с точки зрения организации внутреннего контроля данная конкретизация помогает разграничить их обязанности и полномочия.

COBIT выделяет следующие компоненты, необходимые для внедрения и поддержания системы руководства (governance):

- процессы — структурированный набор практик и мероприятий, направленных на достижение определенных целей;

- организационные структуры — ключевые субъекты принятия решений в организации;

- политики и процедуры — инструкции и стандарты, закрепляющие ожидаемое поведение субъектов;

- информационные потоки — в контексте COBIT означает информацию, требуемую для осуществления эффективного руководства;

- культура и поведение — действия и мышление субъектов;

- навыки — компетенции, необходимые для принятия надлежащих решений и успешного выполнения задач;

- инфраструктура — технологии и приложения, используемые для руководства ИТ.

Компоненты, выделенные в концепции COBIT, можно сопоставить с компонентами модели COSO, что и сделано на рис. 1.

В основе системы руководства концепции COBIT лежат шесть принципов:

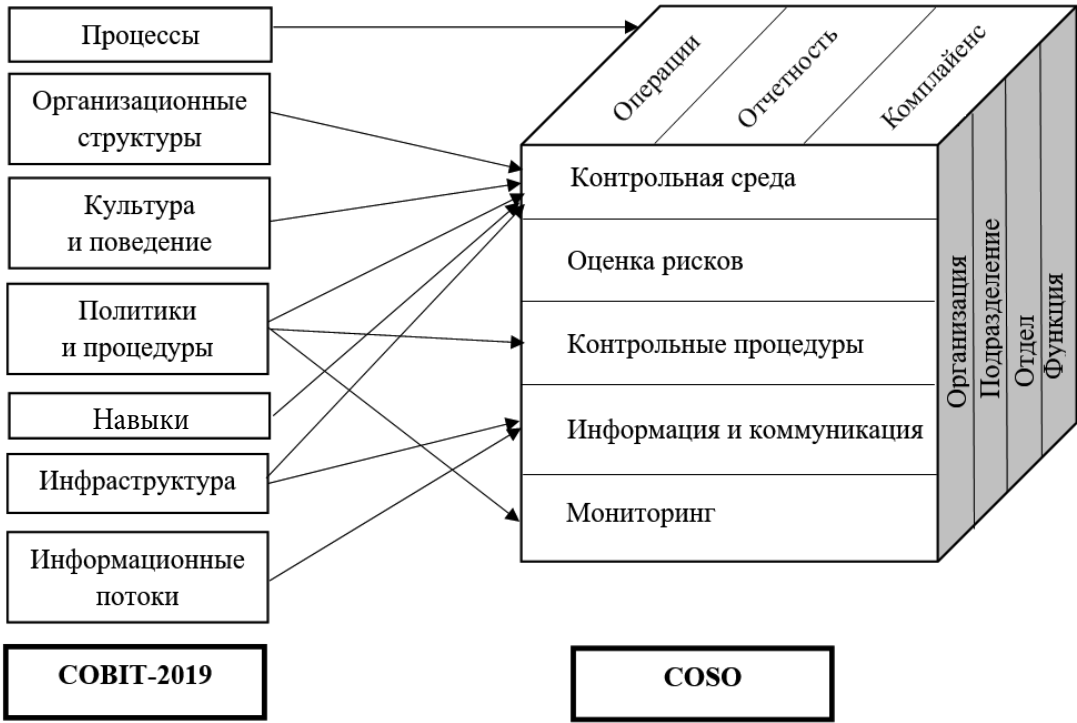


Рис. 1. Сопоставление компонентов COBIT-2019 и COSO

- направленность на удовлетворение нужд стейкхолдеров и повышение эффективности использования информационных технологий (ИТ);
- целостный подход: все компоненты системы руководства должны взаимодействовать между собой и дополнять друг друга;
- динамичность: система руководства должна меняться при выявлении факторов, влияющих на функционирование информационных технологий;
- разделение функций руководства и управления;
- специфичность: система руководства должна быть адаптирована под нужды конкретной организации;
- комплексный взгляд на предприятие: руководство ИТ следует рассматривать как неотъемлемую часть руководства предприятием в целом. Таким образом, необходимо уделять внимание не только ИТ-функции предприятия, но и всей информации и технологиям, используемым экономическим субъектом для достижения стоящих перед ним целей.

Как было отмечено, одним из основных принципов COBIT является специфичность системы руководства. Таким образом, данная

концепция не формирует какого-либо универсального метода организации системы внутреннего контроля, а предлагает пользователям адаптировать систему руководства ИТ под конкретные условия. Основными факторами (дизайн-факторами), которые следует учитывать при организации системы руководства, являются следующие.

1. Стратегия организации. Примеры основных стратегий приведены в табл. 1.

Таблица 1

Виды стратегий согласно COBIT-19

Вид стратегии	Основа стратегии
Рост/Приобретение	Увеличение выручки, доли на рынке
Инновация/Дифференциация	Производство особенной, специальной продукции или услуг
Лидерство в издержках	Оптимизация затрат
Качество сервиса/Стабильность	Ориентированность на потребителя

2. Цели организации. COBIT основана на идее интеграции всех компонентов, особое



внимание уделяется взаимосвязи между различными уровнями целей. Концепция предлагает использовать так называемый «каскад целей», связывающий нужды стейкхолдеров с целями руководства и управления информацией и технологиями. Данная мысль соответствует общей идее направленности системы руководства ИТ на увеличение ценности для стейкхолдеров.

3. *Риски организации* — потенциальные риски, связанные с информационными технологиями, которым подвержена организация: несанкционированные операции, сбои в системах, управление данными, несоответствие установленным требованиям, затраты на ИТ и др.

4. *Проблемы, связанные с ИТ* — текущие вопросы или, иными словами, материализовавшиеся риски. В COBIT приводятся 20 потенциальных ИТ-проблем, среди которых: недостаточность финансирования и руководства, существенные сбои в ИТ-системе, отсутствие интеграции между компонентами ИТ-системы и др.

5. *Угрозы* — окружающая среда, в которой осуществляет свою деятельность предприятие: геополитическая ситуация, отрасль.

6. *Требования комплайенса* — уровень регулирования деятельности организации (низкий/средний/высокий).

7. *Роль ИТ* — функции, выполняемые информационными и технологиями в организации.

8. *Модели работы ИТ* — аутсорсинг, облачные технологии, собственный ИТ-отдел или гибридная модель, сочетающая в себе различные свойства остальных моделей.

9. *Методы внедрения ИТ* — Гибкая методология разработки (Agile), методология DevOps, традиционный метод, гибридные методы.

10. *Стратегия внедрения технологий* — лидер в инновациях, последователь, поздний последователь.

11. *Масштабы предприятия* — для целей COBIT компании подразделяются по категориям: крупные (более 250 работников), средние и маленькие компании (от 50 до 250 работников).

В целом преимуществами концепции COBIT являются следующие:

- *гибкость концепции COBIT и возможность интегрирования с другими моделями.* Концепция может быть адаптирована под

нужды предприятия в зависимости от разнообразных факторов. COBIT также позволяет компаниям успешно адаптировать систему руководства и управления ИТ в соответствии с отраслевыми стандартами, требованиями и практиками, что обеспечивается за счет высокого уровня интеграции концепции с другими идеями.

- *взаимоувязка потребностей стейкхолдеров, целей и компонентов системы.* Одним из ключевых принципов COBIT является учет нужд заинтересованных сторон, также идея «каскада целей» позволяет взаимодействовать цели организации с компонентами системы руководства. Таким образом, потребности стейкхолдеров выступают в роли ориентира, основы для создания системы руководства и внутреннего контроля.

- *учет влияния информационных технологий на организацию системы руководства.* Концепция COBIT сосредоточена на корпоративном управлении в целом, гораздо меньшее внимание в ней уделяется постановке внутреннего контроля. В то же время, положения COBIT могут быть использованы и в вопросах организации СВК, в частности, совместно с положениями модели COSO.

Интеграция концепций COSO и COBIT

Точкой интеграции двух концепций может быть понятие «процесса»: являясь одним из основных компонентов в COBIT, он может рассматриваться как объект контроля и в рамках концепции COSO. Применение процессного подхода широко распространено на практике, и многие компании строят систему внутреннего контроля вокруг бизнес-процессов организации. Интеграция положений COBIT и COSO позволяет воспользоваться преимуществами каждой из концепций, в частности, появляется возможность адаптировать информационную систему под специфику организации и структурировать информационные потоки в соответствии с целями бизнес-процессов.

Наибольшую ценность в интеграции данных концепций представляет собой возможность взаимодействовать потребности стейкхолдеров экономического субъекта с целями конкретного бизнес-процесса и информацией. Согласно концепции COBIT, с помощью «каскада целей»

требования заинтересованных сторон транслируются в цели организации, затем в «согласовывающие цели», потом в цели руководства и менеджмента, на достижение которых, в свою очередь, направлены процессы, включающие в себя определенный набор действий. На обеспечение работы бизнес-процессов направлена система внутреннего контроля, которая подразделяется в соответствии с моделью COSO на пять компонентов. Среди элементов внутреннего контроля числится информационная система, формирование которой регулируется концепцией COBIT и зависит от ряда факторов, включая стратегию, масштаб предприятия, степень внедрения ИТ-технологий и т.д. Интеграция двух концепций представлена на рис. 2.

Одним из аспектов применения данной интегрированной системы является постановка внутреннего контроля при внедрении принципов устойчивого развития в деятельность

организации. Преимущества использования интегрированной концепции в данном случае обусловлены следующим:

- основой концепции устойчивого развития является учет потребностей стейкхолдеров — использование интегрированной концепции обеспечивает соблюдение данного принципа при построении внутреннего контроля;

- цели, указанные в системе COBIT, сформированы в соответствии с системой сбалансированных показателей, которая, помимо финансовых аспектов, включает в себя внутреннюю эффективность, инновации и обучение, а также рассматривает организацию с точки зрения покупателей. Несмотря на то что концепция устойчивого развития включает в себя более широкий спектр вопросов, многие аспекты, связанные с устойчивым развитием, находят отражение в целях COBIT;

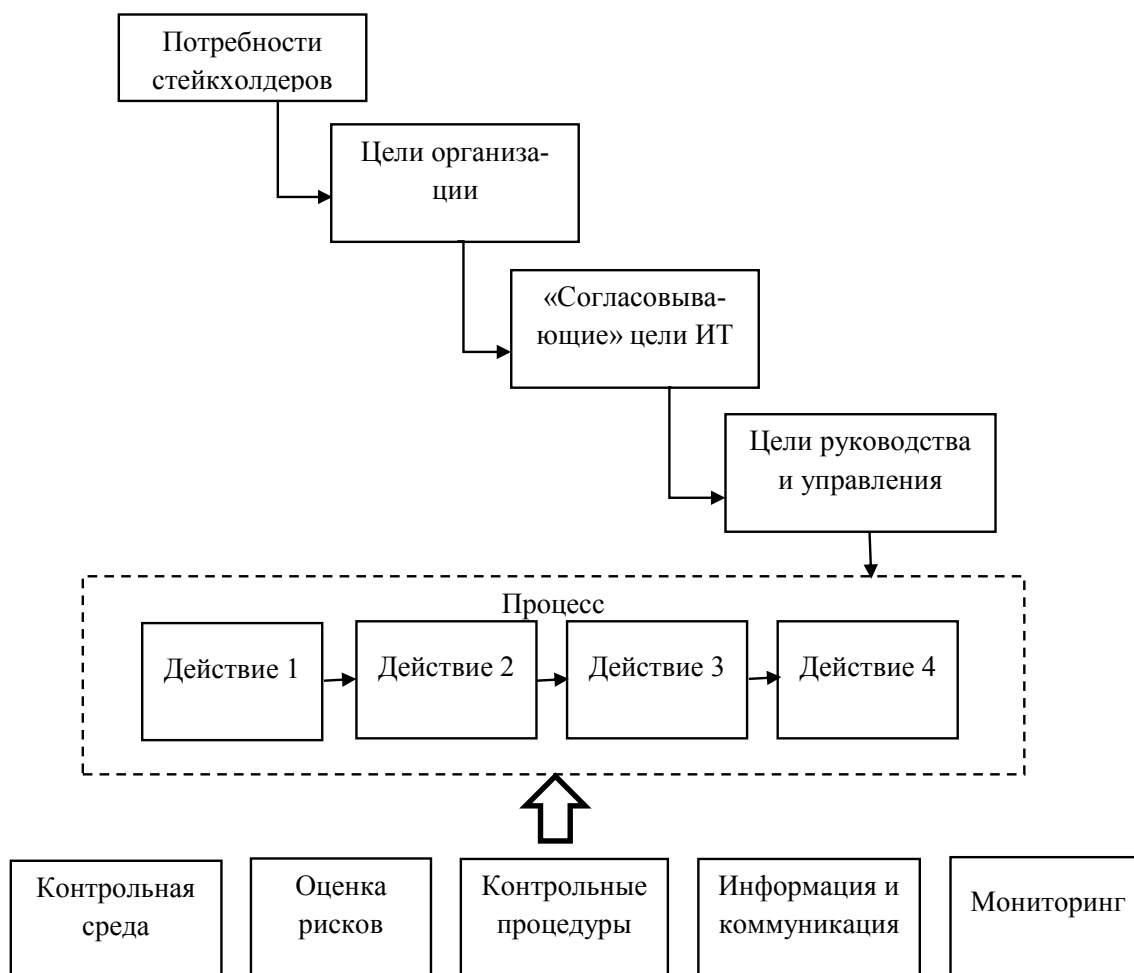


Рис. 2. Интеграция концепций COBIT и COSO

■ зачастую при внедрении концепции устойчивого развития организации сталкиваются с необходимостью сбора дополнительной информации для осуществления контроля за соблюдением принципов устойчивого развития. Применение интегрированной концепции связано с формированием специфичных показателей для каждой цели, а также позволяет определить требуемые «входящие» информационные данные для осуществления процессов, связанных с устойчивым развитием, а также «исходящие» данные, являющиеся результатом процессов. На основании данной информации экономический субъект может наладить информационную систему для формирования требуемых показателей.

Постановка внутреннего контроля в области устойчивого развития на основе интегрированной концепции рассмотрена нами на примере цели устойчивого развития Организации Объединенных Наций (ООН) № 8 «Достойная работа и экономический рост». В данном случае выделена следующая потребность стейкхолдеров — работников организации: заинтересованность в высокооплачиваемой и интересной работе, а также в профессиональном росте. Данная потребность соответствует цели EG10 концепции COBIT «Навыки сотрудников, мотивация и продуктивность», которой, в свою очередь, соответствует «согласовывающая цель» AG12 «Компетентный и мотивированный персонал с по-



Рис. 3. Соответствие процесса потребностям стейкхолдеров

ниманием технологий и бизнеса». Полный путь от потребностей стейкхолдеров к бизнес-процессу (поддержание навыков и компетенций персонала) представлен на рис. 3.

Для эффективного осуществления процесса поддержания навыков и компетенций персонала необходима соответствующая система внутреннего контроля, основными элементами которой являются:

- *контрольная среда*: отражение в организационной структуре соответствующей обязанности по проведению оценки навыков и компетенций персонала, планированию и проведению обучающих программ, закрепление в корпоративной культуре стремления к росту и обучению, отражение в системе вознаграждений поощрений за повышение уровня квалификации, формирование политик по обучению и отражение соответствующих требований в должностных инструкциях;

- *оценка рисков*: рассмотрение таких рисков, как некорректная оценка уровня квалификации персонала, несоответствие программ обучения требованиям к должностям, незаинтересованность персонала в обучении, некачественное проведение обучения, невыполнение сотрудниками программ по повышению навыков и компетенций;

- *процедуры внутреннего контроля*: контроль присутствия персонала на тренингах, документальное оформление оценки персонала, периодическое подтверждение соответствия информации из программ обучения требованиям нормативно-правовых актов и др.;

- *мониторинг*: проверка доказательств осуществления контроля за процессом оценки персонала, рассмотрение случаев нарушений и т.д.

Отдельное внимание следует уделить компоненту «информация и коммуникация» (см. рис. 2), который представляет собой «точку соприкосновения» концепций COBIT и COSO. В концепции COBIT одним из компонентов системы руководства являются «информационные потоки», которые рассматриваются с двух позиций — как входные и выходные данные. Для целей рассматриваемого нами бизнес-процесса могут быть выделены следующие потоки информации:

- *входные данные*:
 - целевые навыки и компетенции персонала;

- действующая политика в области управления персоналом;

- требования стейкхолдеров к уровню квалификации персонала: сложность работы, ожидания рынка и работников, т.д.;

- отчеты об оценке персонала;

- *выходные данные*:

- матрица навыков и компетенций;

- план обучения персонала;

- отчеты о повторной оценке персонала;

- отчеты, отслеживающие динамику уровня квалификации персонала;

- отчеты о нарушениях в процессе обучения персонала.

Таким образом, для обеспечения эффективности процесса поддержания навыков и компетенций персонала необходима информационная система, обеспечивающая сбор, обработку и хранение вышеуказанной информации, а также система коммуникации:

- для информирования сотрудников о требованиях к навыкам и компетенциям;

- информирования сотрудников о программах обучения;

- сообщения результатов оценки сотрудникам, руководству и лицам, ответственным за процесс обучения персонала.

Заключение

На практике при организации российскими компаниями системы внутреннего контроля целесообразно применение положений концепций COSO и COBIT, что позволит привести в соответствие систему внутреннего контроля с внешними факторами деятельности компании и требованиями заинтересованных сторон, структурировать требования к информационной системе, а также взаимоувязать между собой элементы внутреннего контроля. Использование положений COBIT при организации внутреннего контроля особенно актуально в связи с возрастающей важностью ИТ-процессов в бизнесе, в то время как в рамках концепции COSO основное внимание уделяется сопоставлению рисков и процедур внутреннего контроля. В пользу интегрированного применения положений COSO и COBIT говорит также универсальность модели COSO и наличие детальных рекомендаций по организации процессов, политик и информационных потоков в концепции COBIT, что служит



основой для дальнейшей организации компонентов внутреннего контроля.

Применение интегрированной концепции обеспечивает также более эффективную организацию внутреннего контроля в условиях внедрения принципов устойчивого развития в деятельность организации, подразумевающего развитие, при котором удовлетворение потребностей нынешних поколений осуществляется без ущерба для возможностей будущих поколений удовлетворять свои потребности.

В статье рассмотрен пример организации внутреннего контроля во взаимосвязке в целях устойчивого развития ООН № 8 «Достойная работа и экономический рост». Учитывая релевантность данной цели для программы устойчивого развития каждого экономического субъекта, показана актуальность положений интегрированной концепции, основанной на концепциях COSO и COBIT, для целей организации внутреннего контроля в российских компаниях.

Литература

1. Информация Минфина России № ПЗ-11/2013 «Организация и осуществление экономическим субъектом внутреннего контроля совершаемых фактов хозяйственной жизни, ведения бухгалтерского учета и составления бухгалтерской (финансовой) отчетности».
2. COBIT 2019 FRAMEWORK: INTRODUCTION AND METHODOLOGY. — 2019. URL: <https://www.isaca.org/resources/cobit>
3. COBIT 2019 FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES. — 2019. URL: <https://www.isaca.org/resources/cobit>
4. 70-я сессия ООН: Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года.
5. Лисовский А.Л. Оптимизация бизнес-процессов для перехода к устойчивому развитию в условиях четвертой промышленной революции // Стратегические решения и риск-менеджмент. — 2018. — № 4 (109). — С. 10–18.
6. Ситнов А.А. Методология COBIT как современный инструментальный аудита и управления // Экономика и управление: проблемы и решения. — 2014. — № 3. — С. 54–62.
7. Суленова Ю.С., Корзовых Ж.М. Методические основы системы внутреннего контроля предприятий в современных рыночных условиях // Вестник университета ФГБОУ ВО «Государственный университет управления». — 2020 — № 1. — С. 28–35.

ДЕНЬГИ С ЧУЖИХ КАРТ ПО QR-КОДУ

«Известия» рассказали о намерении некоторых российских банков внедрить в обслуживание новую технологию, которая позволит снимать деньги с чужих карт по сгенерированному в специальном приложении QR-коду. Его владелец карточки сможет пересылать лицу, которое получит таким способом разрешение на снятие.

Метод на практике может получить широкое распространение, потому что довольно часто приходится отдавать знакомым не очень крупные суммы (например, долги), специально для этого встречаясь и занимаясь поисками банкомата для снятия, тогда как с QR-кодом все станет намного проще. С другой стороны, есть опасность, что коды начнут перехватывать мошенники.

Внедрить новую технологию уже в следующем году готовятся банк «Открытие», Уральский банк реконструкции и развития и СКБ-банк, а опробовать в тестовом режиме — банк ВТБ. Для внедрения новой функции потребуются модернизировать банкоматы с учетом функции считывания

кода. Впрочем, затраты вполне способны себя окупить благодаря существенному расширению функционала: мало того что для снятия денег необязательно даже будет каждый раз таскать карточки с собой, так еще и снимать деньги по QR-коду сможет клиент какого угодно банка.

Однако, несмотря на все открывающиеся преимущества, некоторые эксперты — например, директор департамента технологического развития СКБ-банка Александр Ельцев — считают, что с новыми возможностями придут и новые риски в виде еще большего распространения мошенничества, в том числе и с использованием методов социнженерии. Если уже сегодня, до этого расширения возможностей, жертвам мошенников ежегодно в России становятся тысячи людей, какая тогда будет статистика пару лет спустя?

Источник: GAAP.RU

Дата публикации: 17 мая 2021 г..