УДК 33-336.719
DOI 10.17150/2072-0904.2015.6(1).14

А. П. Стерхов
Иркутский государственный технический университет,
г. Иркутск, Российская Федерация

АУДИТ СИСТЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ИННОВАЦИОННОГО ПРЕДПРИЯТИЯ

Аннотация. В последнее время как на международном, так и на российском уровне большое внимание стало уделяться управленческому аудиту. Одной из форм такого аудита является аудит безопасности бизнеса, который помогает оценить соответствие системы комплексной безопасности предприятия способности противостоять различного вида угрозам и уязвимостям, а также определить способности системы минимизировать ущерб от возникающих внешних и внутренних угроз. В статье на основе комплексного системного подхода к обеспечению безопасности бизнеса рассматриваются вопросы проведения аудита безопасности инновационного предприятия. Приводится авторская трактовка аудита безопасности инновационного предприятия. Показывается, что успех внедрения аудита безопасности зависит от правильности поставленных перед аудитором задач и правильного выбора критериев оценки эффективности. Важным выводом является то, что аудит системы комплексной безопасности инновационного предприятия, рассматриваемый с позиций эффективности бизнес-процессов, позволяет не только получить информацию о соответствии процедур проведения бизнес-процессов целям деятельности организации, но и оценить степень влияния этих процедур на создание внутренней стоимости бизнеса в будущем развитии организации.

Ключевые слова. Комплексная безопасность бизнеса; аудит системы безопасности; инновационный бизнес; внутренний аудит; комплаенс.

Информация о статье. Дата поступления 31 октября 2014 г.; дата принятия к печати 10 ноября 2014 г.; дата онлайн-размещения 31 января 2015 г.

A. P. Sterkhov
Irkutsk State Technical University,
Irkutsk, Russian Federation

COMPLEX SECURITY SYSTEM AUDIT FOR INNOVATIVE COMPANIES

Abstract. Currently, much attention has been given to managerial audit both at the international and domestic levels. One of the forms of such audit is business security audit which help assess correspondence of company's complex security system to the ability of counteracting various types of threats and vulnerabilities, as well as determine the system's ability to minimize the losses resulting from arising internal and external threats. The article considers the issues of performing security audit for the innovative company on the basis of complex system approach to ensuring business security. It presents the author's interpretation of the innovative company security audit, reveals that the success in introducing security audit depends on correctness of the objectives faced by the auditor and correct choice of efficiency evaluation criteria. An important conclusion is made that audit of complex security system of the innovative company, considered in terms of business process efficiency, allows not only to get information about correspondence of business process procedure performance to the company' activity objectives but also to assess the incidence of these procedures on creating internal business value in the company' future development.

Keywords. Complex business security; security system audit; innovative business; internal audit; compliance.

Article info. Received October 31, 2014; accepted November 15, 2014; available online January 31, 2015.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

Обеспечение безопасности любого бизнеса, а инновационного бизнеса в особенности, можно достичь только при условии определения важнейших стратегических направлений обеспечения безопасности, когда построена четкая логическая схема своевременного обнаружения и ликвидации опасностей и угроз, уменьшения последствий предпринимательских и хозяйственных рисков. Для создания надежной системы комплексной безопасности бизнеса необходимо мобилизовать все имеющиеся средства организационного, правового, методического, информационного, технического, программного и прочего обеспечения для реализации всех основных и вспомогательных (обеспечивающих) процессов предприятия. До приятия решения о формировании органов безопасности конкретного бизнеса и выделении для этой цели материальных, финансовых и других ресурсов необходимо объективно оценить ситуацию, в которой находится конкретное предприятие [6].

В соответствии с формулировкой консалтинговой компании «Технологии безопасности бизнеса», более 10 лет осуществляющей деятельность по консультированию в области безопасности, аудит безопасности бизнеса представляет собой оценку соответствия системы комплексной безопасности предприятия целям, задачам и миссии бизнеса, а также определение ее способности минимизировать ущерб от возникающих внешних и внутренних угроз[1].

В последнее время как на международном, так и на российском уровне большое внимание стало уделяться аудиту, ориентированному на управление бизнесом. Формы такого аудиторского контроля могут быть различны. Так, в рамках управления организациями сформировался управленческий (операционный) аудит [3; 5]. На государственном уровне общим аналогом служит аудит эффективности [7]. В настоящее время понятие управленческого (операционного) аудита еще не закреплено системе нормативного регулирования аудиторской деятельности. Это можно объяснить тем, что в юридическом смысле аудит ориентирован на проверку бухгалтерского учета и финансовой отчетности. Критерием качества такого учета и отчетности служат нормативно-законодательные акты в области бухгалтерского учета.

Управленческий аудит (к каковому можно отнести и аудит безопасности), ориентирован на потребности менеджмента. Критерием качества такого аудита является необходимость (по характеру действий), достаточность (по объему процедур) и релевантность (значимость для принятия решений) информации, служащей для принятия и контроля выполнения управленческих решений.

Таким образом, в соответствии с Федеральным законом «Об аудиторской деятельности»[2] аудит безопасности бизнеса может рассматриваться как один из видов сопутствующих аудиту услуг. Аудиторские организации и индивидуальные аудиторы наряду с аудитом могут оказывать связанные с аудиторской деятельностью услуги, среди которых анализ финансово-хозяйственной деятельности организаций и индивидуальных предпринимателей; экономическое и финансовое консультирование, в том числе связанное с реорганизацией предприятий; разработка и анализ инвестиционных проектов; составление бизнес-планов и пр. Именно эти виды сопутствующих услуг являются наиболее важными для реализации в практической деятельности инновационных проектов.

Следовательно, задачей аудита хозяйственной деятельности является систематический и всесторонний анализ экономики предприятия, а также оценка инновационного вида его деятельности или исследование возможности реализации нового направления. В связи с этим отдельным видом аудиторских услуг можно выделить инновационный аудит, который представляет собой

[1] Кому и для чего нужен аудит? URL : http://bisec.ru/audit.htm.

[2] Об аудиторской деятельности : федер. закон от 30 дек. 2008 г. № 307-ФЗ (ред. от 4 марта 2014 г.).

системную оценку показателей развития организации в области разработки и коммерциализации новшеств, а также определение внутренних и внешних барьеров на их пути.

Существует несколько подходов к определению сущности инновационного аудита:

– аудит компетентностей (the competence innovation audit) — проводится на основе анализа компетентностей работников организации;

– аудит деятельности (the performance innovation audit) — основан на результатах деятельности организации с позиции появления инноваций;

– аудит инновационного процесса (the process innovation audit) — формируется с позиции оценки самого процесса создания инноваций[1].

Первый подход основан на оригинальности разработок и создании инноваций, осуществляемых конкретными работниками организации. При этом основным источником конкурентных преимуществ инновационной организации является ее способность к формированию из различных компонентов используемых фирменных технологий, процессов и навыков некоторых особых компетенций. Эти компетенции создают основное конкурентное преимущество бизнеса организации и лежат в основе ее успешной деятельности.

Особенностью второго подхода является использование количественных методов оценки результатов инновационного процесса. В рамках данного подхода вопросы идентифицируются инновационными метриками (параметрами оценки), посредством чего результаты работы, а также причастность тех или иных работников или подразделений организации сопоставляются с заданными параметрами, главными из которых являются финансовые и временные затраты. Недостатком данного подхода является то, что метрики являются запаздывающими индикаторами, поскольку измеряют лишь результаты прошлой деятельности.

Третий подход к определению сущности инновационного аудита заключается в использовании лучших (эталонных) практик для осуществления инновационного процесса. Особенностью этого подхода является то, что здесь используются различные аналитические приемы, позволяющие оценить деятельность организации в различных контекстах. Используя в качестве эталона специально разработанную модель инновационного процесса для конкретной отрасли или организации, оценивается практика управления конкретным инновационным процессом. При этом, сопоставляя разрывы между текущим и эталонным уровнем организации инновационного процесса, определяются действия, которые необходимо предпринять для закрытия этих разрывов[2].

Рассмотренные подходы позволяют определить цель инновационного аудита, которая заключается в систематическом процессе сбора и оценки свидетельств об экономических действиях и событиях, позволяющих создавать новые потребности, снижать себестоимость продукции удовлетворять рыночному спросу и приносить прибыль производителю.

По отношению к организации, которой оказываются аудиторские услуги, аудит безопасности бизнеса может быть внешним и внутренним. Внешний аудит носит, как правило, периодический характер, а внутренний аудит может быть непрерывным. Текущий контроль однотипных операций и выявление отклонений индикативных показателей от заданных плановых или общепринятых нормативных уровней осуществляется, как правило, при помощи внутреннего аудита, для чего в организации должно существовать соответствующее структурное подразделение (отдел или сектор).

[1] Technological innovation audit methodology. URL : http://upetd.up.ac.za/thesis/submitted/etd-12212006-132438/unrestricted/01chapter1.pdf.

[2] I bid.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

Вообще говоря, решение о проведении внешнего аудита принимается, как правило, исходя из двух основных факторов, а именно, из необходимости более тщательного анализа угроз, существующих в компании, и анализа положения с точки зрения выполнения законодательства в компании. Речь идет об основных составляющих безопасности, таких как информационная, пожарная, промышленная, экологическая и целый ряд других видов безопасности. Конкретные их виды зависят от специфики бизнеса.

Поскольку система безопасности любого предприятия всегда является уникальным, индивидуальным продуктом [12], аудит нужно начинать с диагностики компании, в ходе которой исследуется бизнес-модель компании и фиксируются возможные уязвимые места. На начальном этапе осуществляется аудит основных объектов и субъектов безопасности бизнеса, а также анализ угроз и уязвимостей безопасности бизнеса и возможных сценариев развития событий. В частности, может проводиться:

– анализ организационной структуры;

– описание основных бизнес-процессов и информационных потоков;

– анализ применяемого законодательства и нормативов;

– анализ системы учета поступления и выбытия товарно-материальных ценностей;

– анализ степени зависимости компании от ключевых сотрудников;

– исследование лояльности сотрудников;

– анализ степени зависимости компании от поставщиков, потребителей и кредиторов;

– аудит системы управленческого учета.

Рассмотренные вопросы относятся к так называемому первичному аудиту безопасности, который обычно проводится при создании системы комплексной безопасности любого предприятия. При использовании аудита для обеспечения безопасности в разрезе различных конкретных угроз служба безопасности и руководство предприятия могут иметь прямой контакт с аудиторской компанией для того, чтобы иметь возможность ставить ей определенные задачи.

Специфика проведения аудита безопасности инновационного предприятия на основе комплексного системного подхода к обеспечению безопасности бизнеса состоит в том, что сам аудит встроен как в систему управления бизнесом, так и в систему (схему) повышения уровня безопасности бизнеса. Схема повышения уровня безопасности бизнеса имеет спиралевидный циклический характер и отражает логическую последовательность внедрения и корректировки системы управления безопасностью бизнеса. Поскольку в центре спирали находится анализ оптимальности проводимых мероприятий, который напрямую зависит от творческого потенциала персонала инновационной компании, являющегося ее уникальным и неповторимым внутренним ресурсом, в данном случае фактически реализуется аудит компетентностей, встроенный в систему повышения уровня безопасности инновационного бизнеса. Именно системный подход позволяет эффективно использовать внутренние ресурсы компании, обеспечивая устойчивое развитие инновационного бизнеса с одновременным обеспечением его комплексной безопасности.

Особенностью аудита инновационного предприятия является то, что при анализе инноваций, а также хозяйственных операций, связанных с их созданием, используются не только данные самого предприятия, но и сведения об аналогичных и альтернативных проектах, реализуемых другими предприятиями и организациями [1; 2].

Для оценки рыночных возможностей и угроз для фирмы, а также для использования опыта эффективного функционирования успешных компаний с целью улучшения собственной работы возможно использование бенчмаркинга

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

[13]. В качестве примера эффективного использования бенчмаркинга, позволяющего идеально копировать чужие достижения, можно привести Японию и Китай. Бенчмаркинг помогает относительно быстро и с наименьшими затратами совершенствовать бизнес-процессы, а в более широком смысле, просто совершенствовать свою деятельность.

Применительно к инновациям бенчмаркинг означает изучение бизнеса других предприятий или предпринимателей с целью выявления основополагающих характеристик для разработки своей инновационной политики и конкретных видов инноваций. Использование бенчмаркинга может улучшить производственные и маркетинговые функции компании, так как при этом внедряются лучшие методы и технологии других предпринимательских организаций. Однако необходимо учитывать, что использование бенчмаркинга может оказаться и опасным, поскольку стандарт (эталон) обеспечения безопасности должен разрабатываться на основе анализа потенциала фирмы и всего рынка в целом, а не только в сравнении фирмы с одним конкурентом, пусть и передовым.

Необходимо отметить, что обеспечение контроля, прозрачности и соблюдения законности в деятельности компании является залогом ее собственной безопасности. При этом создаваемые на предприятиях службы обеспечения безопасности (экономической, информационной или комплексной) являются лишь надстройкой. Фундаментом же обеспечения безопасности бизнеса должно служить правильно выстроенное корпоративное управление, содержащее интегрированную систему внутреннего контроля и управления рисками. Несмотря на имеющийся в настоящее время прогресс в осуществлении контрольной деятельности на корпоративном уровне, в этой сфере еще сохраняется ряд проблем, к которым можно отнести:

– недостаточную эффективность деятельности службы внутреннего аудита (контроля);

– отставание в развитии компетенций и мотивации сотрудников службы внутреннего контроля;

– несовершенство внутренних регламентов в области корпоративного контроля;

– проблемы конструктивного взаимодействия внутреннего аудита с ключевыми заказчиками и менеджментом компаний;

– несовершенство технологий компьютерного контроля;

– отсутствие постоянного мониторинга внутренних и внешних корпоративных рисков;

– недостатки системы контроля бизнес-процессов;

– непроизводительное управление рисками информационной безопасности;

– неэффективное использование потенциала внутреннего контроля в противодействии корпоративному мошенничеству и др.

При внедрении внутреннего контроля в организации важно понимать, что он может быть полезен только в том случае, если будет направлен на достижение каких-то конкретных целей. Прежде чем оценивать результаты контроля, необходимо определить эти цели. Так, основными целями внутреннего контроля (аудита) являются:

– надежность и полнота информации;

– экономичное и эффективное использование ресурсов;

– соответствие политике, планам, процедурам и законодательству;

– достижение подразделениями компании поставленных целей и задач;

– обеспечение сохранности активов.

В качестве основных задач корпоративного внутреннего контроля выступают оценка достижения предприятием или организацией задач, определенных корпоративной стратегией; анализ достоверности и сопоставимости информа-

ции, формируемой в финансовом и управленческом учете; оценка сохранности активов; анализ результативности ключевых бизнес-процессов и эффективности использования ресурсов; мониторинг рисков и т. д.

Для реализации поставленных задач выделим основные объекты и направления контроля в схеме организации внутреннего контроля с точки зрения функционального подхода (рис. 1). Исходя из приведенной схемы, можно сделать вывод о том, что в настоящее время внутренний аудит представляет собой функцию, охватывающую практически все аспекты деятельности компании.

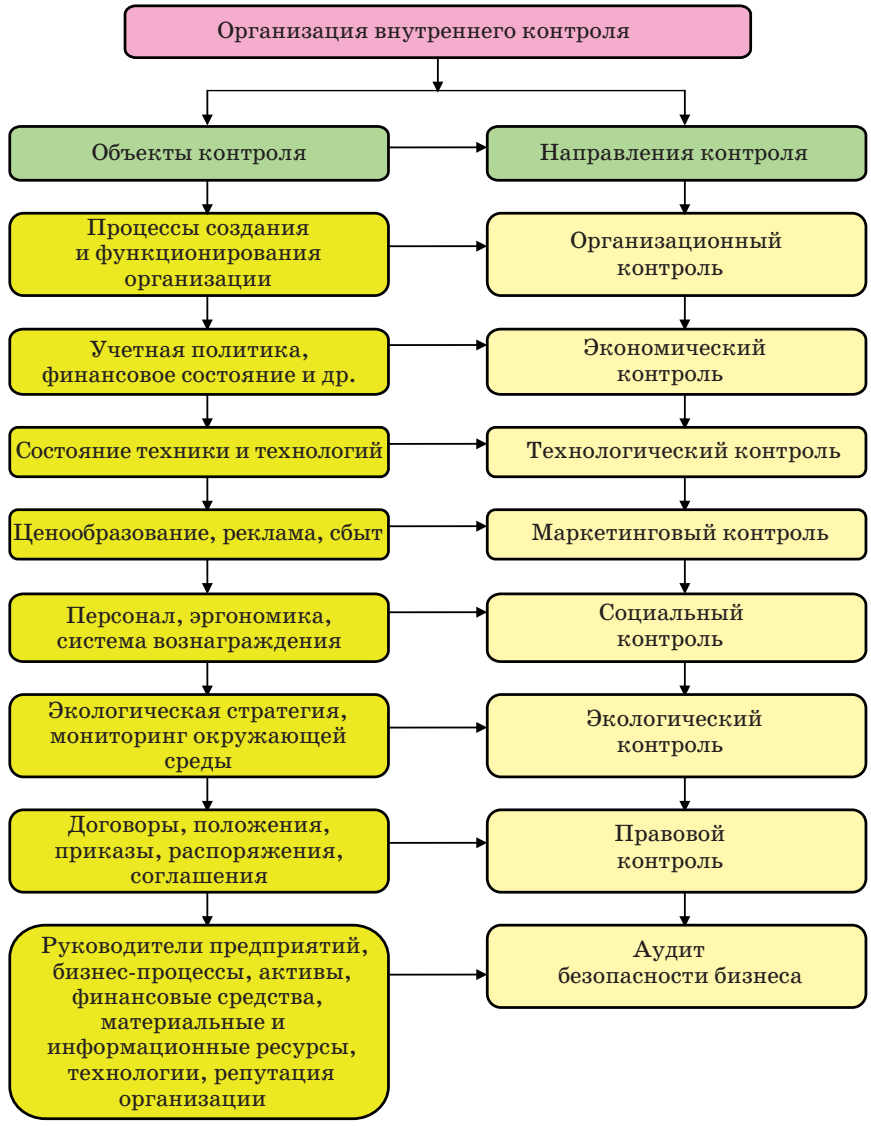

Рис. 1. Схема организации внутреннего контроля с точки зрения функционального подхода

В работе автора [10] было дано определение функции «комплаенс», входящей в систему внутреннего контроля организации. Комплаенс (англ. *compliance* — согласие, соответствие) представляет собой соответствие каким-либо внутренним или внешним требованиям, или нормам. При этом данная функция, строго говоря, не относится ни к аудиту, ни к обеспечению

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

безопасности, ни к управленческому контролю. Однако одновременно она влияет на все сразу. Под комплаенсом подразумевается часть системы управления/контроля в организации, связанная с комплаенс-рисками — рисками несоответствия, несоблюдение требований законодательства, нормативных документов, правил и стандартов надзорных органов, отраслевых ассоциаций и саморегулируемых организаций, кодексов поведения и т. д.

Если еще совсем недавно комплаенс в России был известен лишь в банковской и финансовой сфере, то сейчас он становится все более многовекторным. В качестве примера можно привести некоторые признанные международные стандарты по внутреннему контролю, где использование данной функции стало нормой:

– интегрированная схема внутреннего контроля COSO/Internal Control — Integrated Framework (США, 1992 г.);

– схема внутреннего контроля Coco (Канада);

– схема внутреннего контроля Turnbull (Великобритания);

– закон Сарбейнса-Оксли SOX (США).

В интегрированной схеме COSO/Internal Control — Integrated Framework дано следующее определение внутреннего контроля: процесс, осуществляемый советом директоров, руководством и другими сотрудниками, цель которого дать разумную уверенность в отношении достижения целей по следующим категориям: действенность и эффективность деятельности; надежность финансовой отчетности; соблюдение применимых законов и нормативных требований. Согласно данной схеме внутренний контроль состоит из пяти взаимосвязанных компонентов (рис. 2). Эти компоненты применимы к организациям разного масштаба, хотя к малому бизнесу предъявляются менее жесткие и менее формальные требования (подробное описание компонентов см.: [8]). При этом внутренний контроль является наиболее действенным, когда средства контроля встроены в инфраструктуру организации и являются частью самой организации.

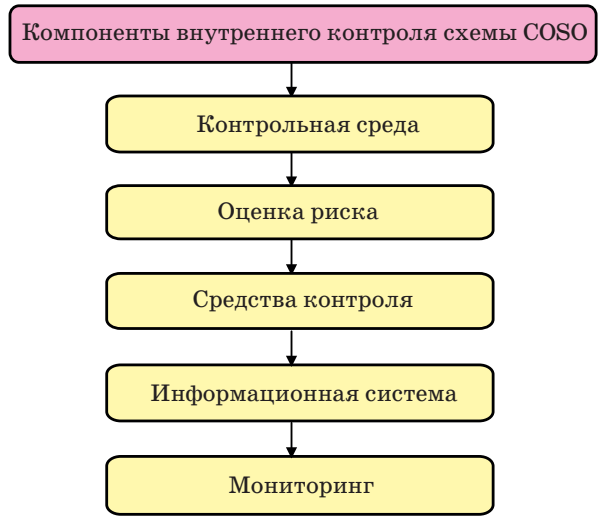

Рис. 2. Компоненты внутреннего контроля схемы COSO

Следует отметить, что в 2006 г. COSO выпустил руководство «Указания для небольших публичных компаний», которое направлено на то, чтобы помочь руководству компаний создать действенную систему внутреннего контроля и проводить ее оценку. В этом документе содержатся примеры того, каким образом принципы схемы COSO могут быть реализованы в небольших компаниях.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

Эмпирические исследования использования модели COSO Internal Control-Integrated Framework в странах мира доказывают определенную сложность ее понимания и применения на практике. В связи с этим модель Coco, предложенная Советом по критериям контроля Канадского института дипломированных бухгалтеров и построенная на основных принципах модели COSO, считается более конкретизированной и приближенной к практике. Внутренний контроль в модели Coco рассматривается в контексте того, как выполняются поставленные задачи, и включает те элементы организации (в том числе ресурсы, системы, процессы, культуру, структуру и задачи), которые в совокупности поддерживают людей в достижении ими целей. К сожалению, использование данной системы не может полностью гарантировать защиту информации на предприятии, поэтому каждому руководителю стоит задуматься об информационной защите персональных данных.

Схема внутреннего контроля Turnbull дает рекомендации директорам компаний, акции которых котируются на бирже, по внедрению требований, касающихся внутреннего контроля (более подробно см. напр.: [4]).

Закон Сарбейнса-Оксли SOC, который направлен на реформирование учета, корпоративного управления и финансовой отчетности в публичных компаниях, также используется рядом российских компаний, которые желали выйти на международный рынок капитала, и перестраивали всю систему корпоративного управления акционерной компании, приведя ее в соответствие с международными стандартами [9].

Особенность аудита безопасности инновационного предприятия напрямую связана со спецификой внутренних и внешних угроз и опасностей для инновационного бизнеса. Характерными чертами инновационного бизнеса являются:

– гибкость, мобильность и приспособляемость к быстро меняющимся условиям;

– ориентация на достижение максимально возможного результата (зачастую при ограниченных ресурсах);

– высокая производительность труда и низкие издержки;

– творческая специализация бизнеса;

– склонность к разумному риску;

– немногочисленный, но чаще всего высококвалифицированный персонал;

– чаще всего руководитель — инноватор;

– повышенная мотивация к инновационной деятельности.

Поскольку перечисленные черты наиболее характерны для малого инновационного бизнеса, у которого фактически нет средств для создания собственной высокоэффективной службы обеспечения безопасности, значительно возрастают риски недружественного захвата высокотехнологичных региональных инновационных предприятий малого и среднего бизнеса. В связи с этим аудит таких предприятий должен разрабатываться с учетом внедрения системы комплексной защиты предприятия от недружественного поглощения, способной блокировать возможный захват компании и обеспечить собственникам контроль над устойчивым развитием предприятия (см. напр.: [11]).

В заключение следует отметить, что аудит системы комплексной безопасности инновационного предприятия, рассматриваемый с позиций эффективности бизнес-процессов, хотя и не регламентируется федеральным законодательством в отличие от обязательного аудита, позволяет не только получить информацию о соответствии процедур проведения бизнес-процессов целям деятельности организации, но и оценить степень влияния этих процедур на создание внутренней стоимости бизнеса в будущем развитии организации.

Поскольку основной целью аудита системы комплексной безопасности предприятия является оценка существующей или вновь создаваемой системы

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

безопасности выбранной или утвержденной ранее концепции безопасности, последняя должна отвечать своему главному предназначению:

– обеспечение собственника, управляющего, начальника службы безопасности достоверной информацией о реальной ситуации на объекте;

– оптимизация расходов при построении комплексной системы безопасности бизнеса;

– принятие решений, направленных на предотвращение или минимизацию возможного ущерба от внешних и внутренних угроз для инновационного предприятия;

– оптимизация системы комплексной безопасности инновационного предприятия.

Следует отметить, что аудит обеспечения безопасности инновационного бизнеса является достаточно новой разновидностью аудита для России. Этот аудит ставит перед собой решение более сложных задач в отличие от традиционного аудита, поскольку охватывает практически всю деятельность предприятия. Успех его внедрения зависит от правильности поставленных перед аудитором задач и правильного выбора критериев оценки эффективности.

Список использованной литературы

1. Булыга Р. П. Инновации современного аудита: аудит эффективности бизнес-процессов / Р. П. Булыга // Аудитор. — 2012. — № 3. — С. 16–22.

2. Вертакова Ю. В. Управление инновациями: Теория и практика / Ю. В. Вертакова, Е. С. Симоненко. — М. : Эксмо, 2008. — 432 с.

3. Галкина Е. В. Бухгалтерский учет и аудит : учеб. пособие / Е. В. Галкина. — М. : Кнорус, 2009. — 592 с.

4. Зайцева О. П. Корпоративный внутренний контроль: принципы, организация, интеграция подходов / О. П. Зайцева, Б. А. Аманжолова // Экономика и менеджмент. — 2011. — № 6. — С. 125–130.

5. Мельник М. В. Анализ и контроль в коммерческой организации / М. В. Мельник. — М. : Эксмо, 2011. — 560 с.

6. Основы предпринимательской деятельности / В. И. Самаруха, Д. И. Сачков, Л. В. Гуляева [и др.]. — Иркутск : Изд-во БГУЭП, 2011. — 140 с.

7. Парушина Н. В. Аудит : учеб. / Н. В. Парушина, С. П. Суворова. — 2-е изд., перераб. и доп. — М. : Форум, 2009. — 288 с.

8. Постникова О. Г. Система внутреннего контроля в корпоративном управлении : дис. ... канд. экон. наук : 08.00.12 / О. Г. Постникова. — М., 2008. — 211 с.

9. Соколов Б. Н. Практика организации внутреннего контроля в корпорациях / Б. Н. Соколов, А. С. Русакова // Акционерное общество: вопросы корпоративного управления. — 2010. — № 10. — С. 22–29.

10. Стерхов А. П. Использование маркетинговых технологий для обеспечения безопасности инновационного бизнеса / А. П. Стерхов // Вестник Иркутского государственного технического университета. — 2013. — № 7 (78). — С. 206–214.

11. Стерхов А. П. Противодействие рейдерским захватам с позиций системного подхода к обеспечению безопасности инновационного бизнеса / А. П. Стерхов // Вестник Иркутского государственного технического университета. — 2014. — № 12 (95). — С. 352–362.

12. Стерхов А. П. Создание и управление комплексной системой безопасности бизнеса / А. П. Стерхов // Вестник Иркутского государственного технического университета. — 2014. — № 8 (91). — С. 199–208.

13. Хайниш С. В. Бенчмаркинг на предприятии как инструмент управления изменениями / С. В. Хайниш, Э. Т. Климова. — М. : Едиториал УРСС, 2012. — 144 с.

References

1. Bulyga R. P. Innovations of modern audit: audit of business process efficiency. *Auditor = Auditor*, 2012, no. 3, pp. 16–22. (In Russian).

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru

2. Vertakova Yu. V., Simonenko E. S. *Upravlenie innovatsiyami: Teoriya i praktika* [Innovation management: Theory and Practice]. Moscow, Eksmo Publ., 2008. 432 p.

3. Galkina E. V. *Bukhgalterskiy uchet i audit* [Accounting and Audit]. Moscow, Knorus Publ., 2009. 592 p.

4. Zaytseva O. P., Amanzholova B. A. Corporative internal control: principles, organization, integration of approaches. *Ekonomika i menedzhment = Economics and Management*, 2011, no. 6, pp. 125–130. (In Russian).

5. Mel'nik M. V. *Analiz i kontrol' v kommercheskoy organizatsii* [Analysis and control in commercial organizations]. Moscow, Eksmo Publ., 2011. 560 p.

6. Samarukha V. I., Sachkov D. I., Gulyaeva L. V. et al. *Osnovy predprinimatel'skoy deyatel'nosti* [Basics of Entrepreneurship]. Irkutsk, Baikal State University of Economics and Law Publ., 2011. 140 p.

7. Parushina N. V., Suvorova S. P. *Audit* [Audit]. 2nd ed. Moscow, Forum Publ., 2009. 288 p.

8. Postnikova O. G. *Sistema vnutrennego kontrolya v korporativnom upravlenii. Kand. Diss.* [Internal control system in corporative management. Cand. Diss.]. Moscow, 2008. 211 p.

9. Sokolov B. N., Rusakova A. S. Practice of organizing internal control in corporations. *Aktsionernoe obshhestvo: voprosy korporativnogo upravleniya = Joint-stock company: issues of corporate management*, 2010, no. 10, pp. 22–29. (In Russian).

10. Sterkhov A. P. Using marketing technologies to ensure innovative business security. *Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta = Bulletin of Irkutsk State Technical University*, 2013, no. 7 (78), pp. 206–214. (In Russian).

11. Sterkhov A. P. Counteracting illegal seizures from a perspective of system approach to ensuring innovative business security. *Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta = Bulletin of Irkutsk State Technical University*, 2014, no. 12 (95), pp. 352–362. (In Russian).

12. Sterkhov A. P. Creation and management of integrated business security system. *Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta = Bulletin of Irkutsk State Technical University*, 2014, no. 8 (91), pp. 199–208. (In Russian).

13. Khaynish S. V., Klimova E. T. *Benchmarking na predpriyatii kak instrument upravleniya izmeneniyami* [Benchmarking in the company as a change management tool]. Moscow, Editorial URSS Publ., 2012. 144 p.

Информация об авторе

Стерхов Анатолий Петрович — кандидат технических наук, доцент, профессор, кафедра экономической теории и финансов, Иркутский государственный технический университет, 664074, г. Иркутск, ул. Лермонтова, 83, e-mail: rabota@istu.edu.

Author

Anatoly P. Sterkhov — PhD in Engineering, Associate Professor, Chair of Economic Theory and Finance, Irkutsk State Technical University, 83 Lermontov St., 664074, Irkutsk, Russian Federation; e-mail: rabota@istu.edu.

Библиографическое описание статьи

Стерхов А. П. Аудит системы комплексной безопасности инновационного предприятия / А. П. Стерхов // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2015. — Т. 6, № 1. — URL : http://eizvestia.isea.ru/reader/article.aspx?id=19964. — DOI: 10.17150/2072-0904.2015.6(1).14.

Reference to article

Sterkhov A. P. Complex security system audit for innovative companies. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii* (*Baykalskiy gosudarstvennyy universitet ekonomiki i prava*) = *Izvestiya of Irkutsk State Economics Academy* (*Baikal State University of Economics and Law*), 2015, vol. 6, no. 1. Available at: http://eizvestia.isea.ru/reader/article.aspx?id=19964. DOI: 10.17150/2072-0904.2015.6(1).14. (In Russian).

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2015. Т. 6, № 1
http://eizvestia.isea.ru