УДК 334

Эффективное управление контрольной средой как основа безопасного информационного обеспечения организации

Д-р экон.наук, профессор **Макарченко М.А.** makarchenko68@mail.ru,
Неркарарян С.А. Sofiya.nerkararyan@rambler.ru
Университет ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49

Непрерывное развитие информационной среды организации, ее расширение и разнообразие факторов влияющих на ее эффективность увеличивается с каждым днем. Безопасность информационного обеспечения является ключевым факторов с точки зрения исправного и эффективного функционирования. В крупных организациях безопасность информационной среды одна из наиболее капиталоемких статей затрат, чем и обусловлен повышенный интерес в этом направлении. В работе рассматривается эффективное управление контрольной средой организации, так как именно она является основополагающей для безопасности информационного обеспечения организации.

Работа посвящена оценке влияния непрерывного мониторинга, как современного контрольного механизма, на контрольную среду организации. Исследование поднимает актуальные для бизнеса проблемы повышения эффективности контрольной среды в организации; а также рассматривает вопрос оптимизации контрольных процедур с точки зрения операционной эффективности и распределения ресурсов в информационных системах.

Исследование дает практические знания о функционировании контрольной среды и ее механизмах, в частности систем непрерывного мониторинга. Предложенный в работе подход к оценке эффективности непрерывного мониторинга, имеет прикладное значение для оценки целесообразности внедрения систем непрерывного мониторинга в организации, а также может быть рекомендован для оценки операционной и экономической эффективности контрольной среды организации.

Ключевые слова: информационное обеспечение, контроль, эффективность, непрерывный мониторинг, контрольная среда, надежность финансовой отчетности, риски, базы данных.

Effective management of the internal control as the basis for secure information support of the organization

D.Sc, prof., **Makarchenko M.A.** makarchenko68@mail.ru
Nerkararyan S.A. sofiya.nerkararyan@rambler.ru
ITMO University
197101, St. Petersburg, Kronverksky ave., 49

Continuous development of the information environment of the organization, its extension and the variety of factors affecting its efficiency is increasing every day. Secure information support is a key factor in terms of serviceable and effective functioning. In large organizations, security of the information environment is one of the most capital-cost items, and this leads to the increased interest in this area. This article outlines the effective management of the internal control of the organization, as far as it is a fundamental of the security of information support of the organization.

The article is devoted to evaluation of the effect of continuous monitoring, as a modern internal controlling mechanism, on the internal control of the organizational environment. The study raises the actual problems for the business such as - efficiency increase of the internal control of the organization; as well as considering the optimization of controlling procedures in terms of operational efficiency and distribution of resources in information systems.

The study provides practical knowledge about the functioning of the internal control and its mechanisms, in particular uninterrupted monitoring systems. In this article the proposed approach to the evaluation of the effectiveness of continuous monitoring, is applicable to the assessment of the feasibility of implementing continuous monitoring systems in the organization, and can also be recommended to assess the operational and economic efficiency of the internal control of the organization.

Keywords: information support, control, efficiency, continuous monitoring, internal control, the reliability of financial reporting, risks, databases.

Ключом к успеху организации является эффективное управление ее деятельностью. Основатель классической школы управления Анри Файоль считал, что контроль, как функция управления, завершает управленческий цикл и, таким образом, гарантирует выполнение остальных функций управления. В современных организациях внутренний контроль представляет собой особый процесс, предназначенный для обеспечения достаточной уверенности руководства касательно выполнения организацией следующих задач:

- эффективность и продуктивность операций и информационных потоков
- надежность финансовой отчетности
- соблюдение законодательства и внутренних процедур.

В условиях рыночной экономики, любая коммерческая организация подвержена рискам, влияющим на достижение ее целей. Перед руководством организации стоит задача снижения этих рисков, которая решается повышением эффективности контрольной среды в рамках общей системы информационного обеспечения организации[1].

На текущий момент в большинстве организаций контрольные процедуры выполняются вручную, что приводит к появлению ошибок и требует привлечения большого числа финансовых и человеческих ресурсов. Кроме того, в крупных организациях в виду масштаба деятельности руководству становится все труднее осуществлять функцию контроля. В то же время проблема снижения рисков становится все более острой и требует от руководства компании своевременных мер, направленных на повышение безопасности внешних и внутренних информационных потоков и одним из условий является повышении эффективности контрольной среды.

Таким образом, современные организации сталкиваются со следующей проблемой: как повысить эффективность контрольной среды; и какой набор контрольных процедур и механизмов является оптимальным с точки зрения операционной эффективности и распределения ресурсов.

Одним из современных механизмов внутреннего контроля является непрерывный мониторинг, который позволяет увеличить точность контрольных процедур и сократить время реакции на возможные инциденты. Под непрерывным мониторингом понимается автоматический механизм, предоставляющий менеджменту информацию об операционной эффективности процедур внутреннего контроля в режиме реального времени. [2]

Таким образом, для решения поставленной проблемы необходимо провести исследование влияния непрерывного мониторинга на эффективность контрольной среды организации и решить следующие задачи:

- определить влияние контрольной среды на управление организацией;
- проанализировать принципы работы непрерывного мониторинга, как современного механизма внутреннего контроля;
- изучить факторы, влияющие на эффективность контрольной среды организации, на основе методологии Д. Брюэра и У. Листа;

Эффективность управления рисками влияет на достижение организацией поставленных целей, и зависит от эффективности контрольной среды организации.[3]

Контрольная среда включает в себя набор контрольных процедур, направленных на снижение рисков. Эффективная контрольная среда дает возможность руководству компании своевременно получать точную информацию, необходимую для принятия управленческих решений.

Таким образом, очевидно, что влияние контрольной среды на управление организацией значительно.

Если в маленькой организации руководитель может осуществлять контроль самостоятельно, то для крупных организаций это невозможно из-за больших масштабов деятельности, требующих избирательного подхода к контролю. Таким образом, руководству организации необходимо установить оптимальный набор контрольных процедур, который позволит эффективно осуществлять функцию контроля.[4]

Решение данной задачи осложняется тем, что в крупных организациях существует множество бизнес-процессов, тысячи сотрудников имеют права доступа на проведение операций в системе, количество совершающихся транзакций постоянно растет, и компании оперируют в среде со множеством рисков.

[1] Файоль А., Эмерсон Г., Тейлор Ф., Форд Г., Управление — это наука и искусство М.: Республика 1992. С 349
[2] Кастель М. Информационная эпоха: экономика, общество и культура М.: Высшая школа экономики, 2010 С. 608
[3] Сонин А. М. Внутренний аудит в новой реальности // Аудитор. — 2012. — № 7. — с. 39–45

На текущий момент одним из наиболее эффективных механизмов, который направлен на решение поставленной задачи является непрерывный мониторинг.

Современный уровень развития информационных технологий и их повсеместное распространение положительно влияют как на эффективность бизнес-процессов, так и на контрольную среду организации. На сегодняшний день наблюдается тенденция к автоматизации процедур внутреннего контроля и их переходу на качественно новый уровень – к непрерывному мониторингу. Данный механизм позволяет получать максимально точную информацию о работе контрольных процедур в любой момент времени. [5]

Как и любая автоматизация, переход на непрерывный мониторинг предполагает внедрение аналитической системы, взаимодействующей с корпоративной информационной системой. Рассмотрим общую схему взаимодействия системы непрерывного мониторинга с ERP (Enterprise Resource Planning - Управление ресурсами предприятия) - системой организации (рис 1.1).

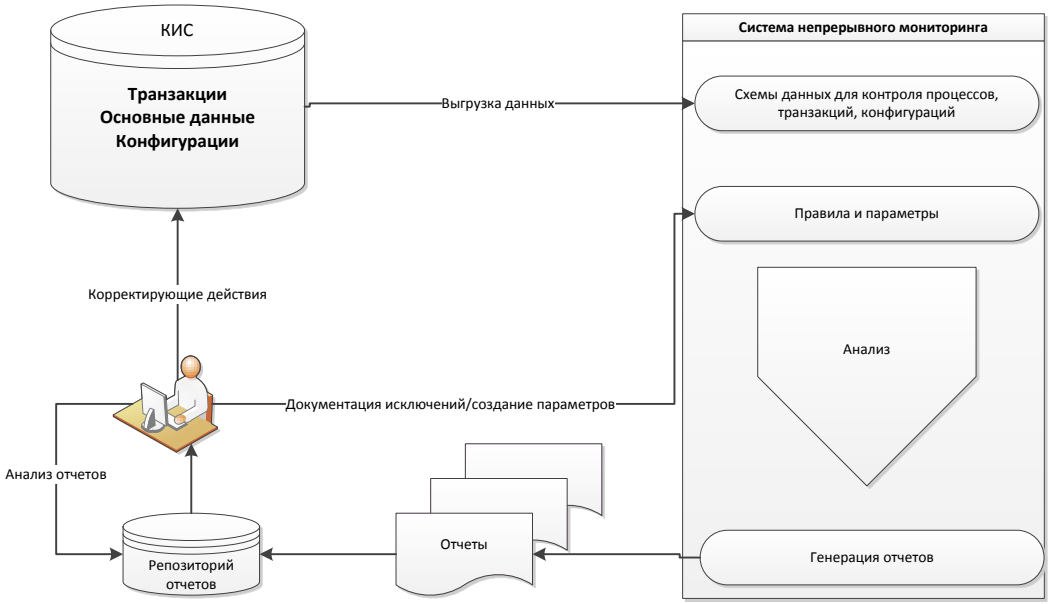


Рис. 1.1. Схема взаимодействия системы непрерывного мониторинга с ERP-системой организации[6]

Система непрерывного мониторинга постоянно отслеживает любые изменения, происходящие в корпоративной информационной системе и анализирует их по заранее настроенным алгоритмам. На схеме видно, что система обрабатывает разные данные (основные, транзакционные и конфигурационные) и анализирует их на предмет соответствия правилам, заложенным в алгоритмах контрольных процедур. То есть конфигурация процедур непрерывного мониторинга основана на подходе, использующем анализ рисков (“risk-based approach”).[7]

Согласно данному подходу, оцененные риски организации подразделяются на четыре группы:

1. Риски, связанные с доступом в систему, управление которыми осуществляется через мониторинг доступа к функциональным возможностям системы.
2. Конфигурационные риски, связанные с неправильной настройкой бизнес-логики в корпоративных системах.
3. Риски, связанные с несанкционированными изменениями основных данных.
4. Транзакционные риски, связанные с возможностью совершения мошеннических транзакций в системах.[8]

Каждой группе рисков соответствует определенный тип контрольного механизма. Используя собственную методологию «магического квадранта», компания Gartner выделила четыре типа контрольных механизмов непрерывного мониторинга:

- непрерывный мониторинг прав доступа в системах;
- непрерывный мониторинг системных конфигураций;

[5] Козырев А.А. Информационные технологии в экономике и управлении СПб: Издательство Михайлова, 2012 С. 540

[6] Пугачев В.В. Внутренний аудит и контроль // В.В. Пугачев. – М.: Дело и сервис, 2010. С. 224

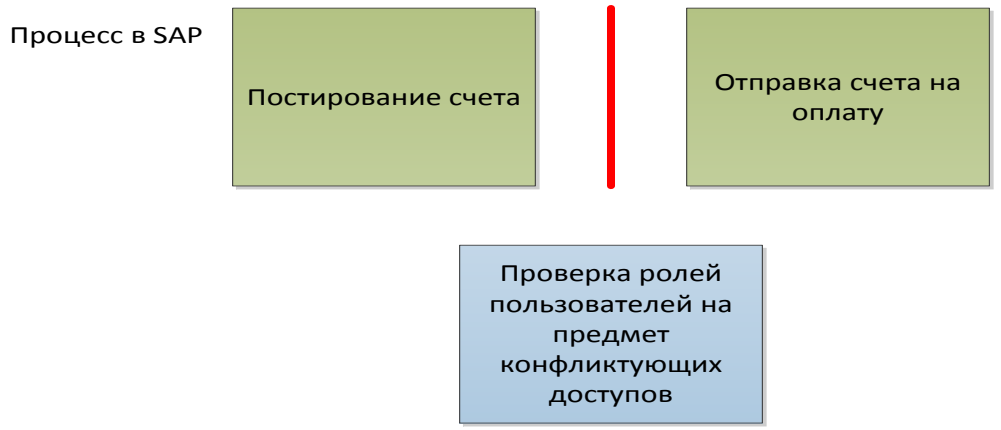
[7] KPMG - Whitepaper. Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance. URL: http://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/cacm080609.pdf

[8] W. Affum. Evaluation of internal controls in Papso Ghana Limited – Study, June 2011 Approva Company. URL: http://ir.knust.edu.gh/bitstream/123456789/4228/1/William%20thesis.pdf

- непрерывный мониторинг основных данных;
- непрерывный мониторинг транзакций.[9]

Непрерывный мониторинг прав доступа в системах

Непрерывный мониторинг прав доступа в системах включает в себя мониторинг разделения полномочий (согласно присвоенным правам доступа) и мониторинг критичных прав доступа. Данные типы контрольных механизмов анализируют права доступа пользователей в системах и создают отчет об инцидентах. Целью таких контрольных механизмов является выявление пользователей, обладающих лишними правами доступа. Наличие подобных прав доступа у пользователей приводит к увеличению риска злоупотребления полномочиями. Рассмотрим пример контрольной процедуры разделения обязанностей (рис 1.2).



Контрольная цель	Возможность постирования счетов и отправки счетов на оплату разделена в целях предотвращения несанкционированных платежей.
Риск	Сотрудники компании могут запостировать несанкционированный счет в системе и отправить его на оплату без возможности отслеживания транзакции.

Рис. 1.2. Пример контрольной процедуры непрерывного мониторинга разделения обязанностей[10]

Мы видим, что наличие у пользователя прав на сохранение счетов в корпоративной системе и прав на оплату счетов является нарушением, приводящим к риску. Механизм непрерывного мониторинга выявит такое нарушение, требующее принятия корректирующих мер. В качестве таких мер могут служить изменения прав доступа пользователя, или изменение системных ролей.

Непрерывный мониторинг системных конфигураций

Контрольные механизмы непрерывного мониторинга системных конфигураций используются для контроля настроек бизнес-логики в системах. Принцип работы таких механизмов заключается в анализе конфигурационных таблиц в корпоративной информационной системе. Примером такой контрольной процедуры является проверка настроек процентного отклонения суммы заказа от суммы счета на оплату (рис. 1.3).

[9] French Caldwell, Paul E. Proctor. Magic Quadrant for Continuous Controls Monitoring. – Gartner, 2010
[10] Benchmarks from SAP's Case Studies and Success Stories URL: http://www.ibs.ru/download/events/101109/SAP_Risk_Management.pdf

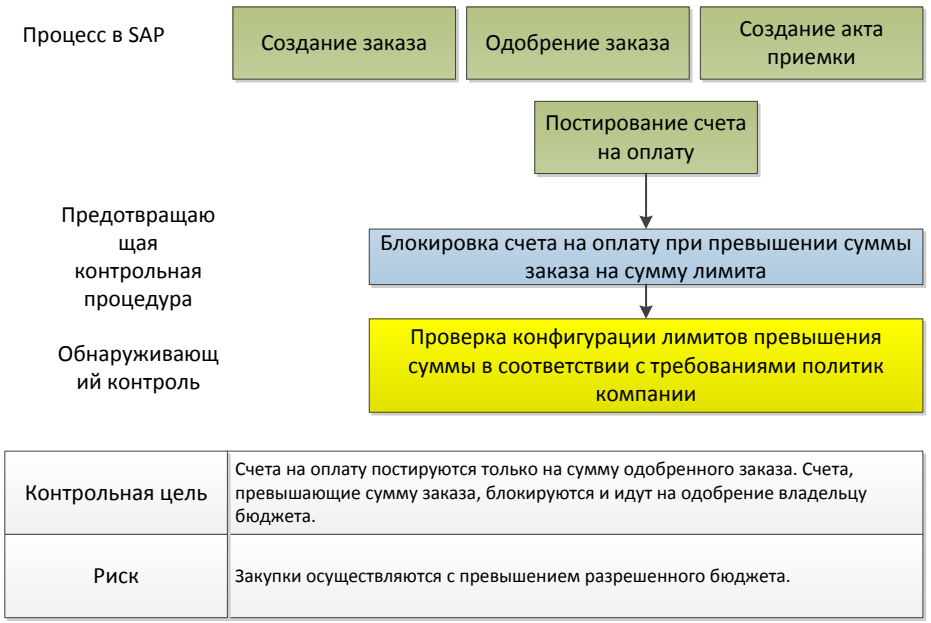


Рис. 1.3. Пример контрольной процедуры непрерывного мониторинга системных конфигураций[11][12]

В рассмотренном примере, контрольная процедура осуществляет проверку конфигурации согласно настроенному правилу, и создает отчет в случае несоответствия конфигурации цели контроля.

Непрерывный мониторинг основных данных

Контрольные механизмы основных данных направлены на отслеживание изменений в основных данных, как-то: данных о поставщиках и покупателях, данных о счетах и т.д. Контрольные механизмы этого типа используют таблицы основных данных. Примером такой контрольной процедуры является контроль над амортизацией основных средств (рис.1.4).

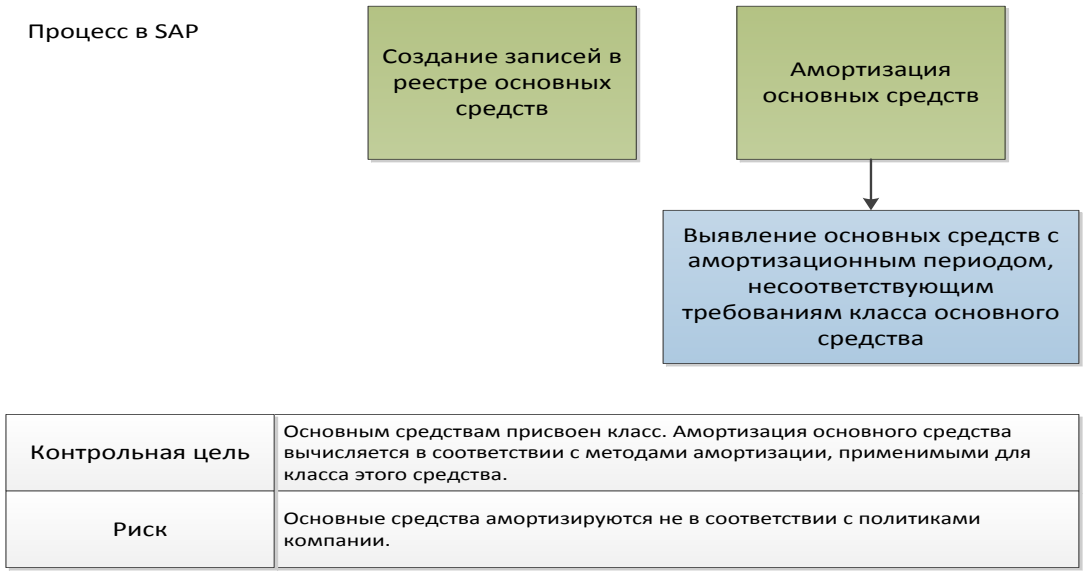


Рис. 1.4. Пример контрольной процедуры непрерывного мониторинга основных данных[13][14]

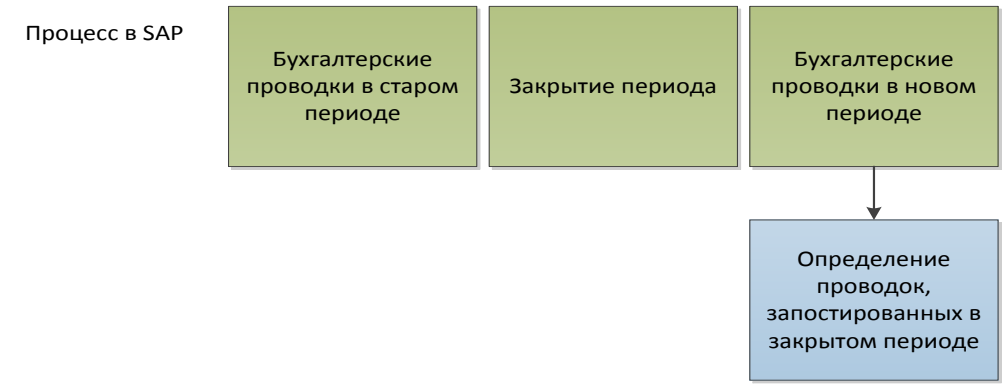
Контрольная процедура анализирует данные об основных средствах и выявляет те, у которых период амортизации не соответствует требованиям класса основного средства.

[11] Gartner Identifies the Top 10 Strategic Technology Trends for 2013 URL: http://www.gartner.com/newsroom/id/2209615
[12] Benchmarks from SAP's Case Studies and Success Stories URL: http://www.ibs.ru/download/events/101109/SAP_Risk_Management.pdf

[13] Gartner Identifies the Top 10 Strategic Technology Trends for 2013 URL: http://www.gartner.com/newsroom/id/2209615
[14] Gyasi K. "Challenges of internal auditing in the era of good governance" Legon business journal, 2010 pg. 13 - 14

Непрерывный мониторинг транзакций

Механизм непрерывного мониторинга транзакций предусматривает полную видимость всех транзакций, что исключает необходимость ручного выбора транзакций (как при проведении аудита). Система непрерывного мониторинга анализирует полный объем транзакций и выявляют исключения в установленных правилах. Подобный контрольная процедура, прежде всего, направлена на выявление единичных случаев мошенничества, которые могут быть пропущены при выборочной проверке транзакций. Примером такого механизма является контроль за бухгалтерскими проводками (рис. 1.5).



Контрольная цель	Финансовые проводки на счетах главной книги не осуществляются в закрытом периоде по US GAAP.
Риск	Некорректное закрытие месяца, как следствие – неправильная финансовая отчетность. Несоответствия в ежемесячной отчетности.

Рис. 1.5. Пример контрольной процедуры непрерывного мониторинга транзакций[15][16]

Данная контрольная процедура направлена на обнаружение проводок, сделанных в закрытом бухгалтерском периоде. Подобные проводки могут приводить к несоответствиям в бухгалтерской отчетности, а, следовательно, должны своевременно выявляться.

Согласно исследованиям SAP, непрерывный мониторинг приводит к снижению рисков организации, которое достигается через расширенное и более последовательное освещение элементов управления в бизнес-процессах. Также, благодаря предотвращению нарушений правил ведения бизнеса, система мониторинга может улучшить ключевые финансовые процессы.

Из приведенных примеров видно, что внедрение непрерывного мониторинга способствует повышению операционной эффективности контрольных процедур.

Среди существующих методов оценки эффективности контрольной среды организации можно выделить два наиболее распространенных:

- расследование инцидентов, по результатам которого выявляются контрольные процедуры, давшие сбой;
- аудиты, представляющие собой регулярные или единовременные процедуры независимой оценки.

Данные методы позволяют оценить работу контрольных процедур в достаточной мере, но обладают некоторыми недостатками. Как правило, при возникновении и расследовании инцидента и проведении аудита наблюдается тенденция к созданию большего числа контрольных процедур, чем необходимо организации. Аудиторы, как правило, рекомендуют внедрять дополнительные контрольные процедуры в соответствии с общепринятыми практиками, а это приводит к дополнительным издержкам.

Что бы оценить эффективность внедренных защитных мер необходимо использовать методологии Д. Брюэра и У. Листа «Оценка эффективности системы внутреннего контроля», которая позволяет оптимизировать использование контрольных процедур для повышения эффективности контрольной среды. Также, методология позволяет оценить экономическую эффективность внедрения защитных мер.

[15] French Caldwell, Paul E. Proctor. Magic Quadrant for Continuous Controls Monitoring. – Gartner, 2010
[16] Benchmarks from SAP's Case Studies and Success Stories URL: http://www.ibs.ru/download/events/101109/SAP_Risk_Management.pdf

Методология Брюэра и Листа путем непосредственных измерений позволяет определить, достигает ли система внутреннего контроля поставленных целей.

Для оценки эффективности, модель использует различные временные переменные. В качестве абсолютной точки измерения используется время наступления инцидента (T_E). Другие переменные определяются относительно T_E:

- T_D – время обнаружения инцидента системой внутреннего контроля;
- T_M – время обнаружения инцидента другими средствами (например, публикация в СМИ);
- T_F – время обработки инцидента;
- T_W – момент во времени, при наступлении которого компания терпит убытки в размере I_P.

Брюэр и Лист вводят некоторые финансовые показатели в представленную модель:

- C_{BA} – стоимость ведения бизнеса организацией;
- C_{ICS} – стоимость внедрения контрольных процедур системы внутреннего контроля;
- I_P – стоимость ущерба при наступлении инцидента;
- C_F – величина расходов на устранение последствий инцидента.[17]

Любые процедуры, направленные на восстановление бизнеса после инцидента, а также на минимизацию ущерба, авторы называют «Планом обеспечения непрерывности бизнеса».

Они считают, что стоимость ведения бизнеса (C_{BA}) может выражаться как в денежном эквиваленте (у.е.), так и в других ресурсах (например, человеческих). Организация производит некоторые товары или услуги, и в случае, если это коммерческая организация, получает прибыль P, которая связана со стоимостью ведения бизнеса через выручку R:

$$P = R - C_{BA}$$

Авторы предполагают, что организация внедряет систему внутреннего контроля, которая увеличивает стоимость ведения бизнеса на C_{ICS}:

$$C_{BA} + C_{ICS}$$

В масштабе организации, это снижает прибыль.

Пусть E – это набор неблагоприятных событий: $E = \{e_1, e_2, e_3, \ldots e_j, \ldots\}$.

При возникновении неблагоприятного события в момент времени $T_{Ej,}$ отсутствие реакции на него со стороны организации ко времени T_{Fj}, где $T_{Fj} < T_{Wj}$ (таким образом, временное «окно» $T_{Wj} = T_{Fj} - T_{Ej}$), приведет к возникновению ущерба I_P. Ущерб может быть выражен в различных формах, однако, для упрощения модели авторы представляют любой ущерб в финансовом эквиваленте.

Инциденты обнаруживаются системой внутреннего контроля в момент T_{Dj}, где $T_{Ej} < T_{D.}$ В случае, если инцидент не обнаруживается системой внутреннего контроля, то руководство организации узнает о нем в момент времени T_{Mj}, где $T_{Ej} < T_{Mj}$.

Стоимость защитных мер, обнаруживающих инцидент, включена в $C_{ICS.}$ Стоимость устранения последствий, вызванных инцидентом равна C_{Fj}. Последствия инцидента невозможно устранить до тех пор, пока событие не будет обнаружено, то есть $T_{Dj} < T_{Fj}$ и/или $T_{Mj} < T_{Fj.}$

Величина ущерба вследствие наступления инцидента зависит от времени обнаружения данного инцидента, а именно:

- если $T_{Fj} < T_{Wj}$, то величина ущерба равна C_{Fj};
- если $T_{Fj} \geq T_{Wj}$, то величина ущерба равна $C_{Fj} + I_{Pj}$.

Во втором случае момент обнаружения инцидента T_{Dj} может наступить до или во время T_{Wj}. Проблема заключается в том, что инцидент будет обнаружен слишком поздно для принятия корректирующих мер, и ущерб будет понесен в любом случае.

Последствия наступления такого события могут оказывать сильное влияние на бизнес до тех пор, пока последствия события не будут исправлены путем принятия некоторых корректирующих действий. В худшем случае, инцидент может привести к остановке бизнеса, или принести ущерб внешней среде организации. В таких

[17] Brewer, D. & List, W. Measuring the effectiveness of an Internal Control System, Gamma Secure Systems Limited, 2004

случаях, данный инцидент может быть классифицирован как катастрофический, а корректирующие действия будут приняты в рамках реализации плана обеспечения непрерывности бизнеса. Авторы замечают, что даже в случае успешной реализации плана обеспечения непрерывности бизнеса, может пройти много времени до полного восстановления бизнеса. В худшем случае, бизнес может и не восстановиться.

Авторы утверждают, что все параметры, представленные выше, могут быть измерены непосредственно с некоторой точностью, позволяющей классифицировать процедуры системы внутреннего контроля по эффективности.

Брюэр и Лист выделяют семь классов контрольных процедур, которые в свою очередь делятся на три типа: предотвращающие, обнаруживающие и корректирующие. Описание классов контрольных процедур и их принадлежность к определенной категории представлены в таблице 1.1.

Таблица 1.1

Описание классов контрольных процедур согласно классификации Брюэра и Листа

Класс	Способность обнаруживать неблагоприятные события и запускать корректирующие меры	Тип
1	Предотвращающие меры, позволяющие предотвратить наступление инцидента или мгновенно его обнаружить до появления ущерба.	Предотвращающие
2	Обнаруживающие меры, позволяющие обнаружить инцидент и отреагировать достаточно быстро для принятия корректирующих мер в пределах «окна» T_{Wj} без существенных затрат и ущерба.	Обнаруживающие
3	Обнаруживающие меры, позволяющие обнаружить инцидент и отреагировать достаточно быстро для принятия корректирующих мер в пределах «окна» T_{Wj} с существенными затратами, но без ущерба.	
4	Обнаруживающие меры, позволяющие обнаружить инцидент, но не позволяющие отреагировать достаточно быстро для принятия корректирующих мер в пределах «окна» $T_{Wj.}$	
5	Корректирующие меры, которые не позволяют обнаружить инцидент, но имеют частично применяемый план обеспечения непрерывности бизнеса.	Корректирующие[18]
6	Корректирующие меры, которые не позволяют обнаружить инцидент, но имеют план обеспечения непрерывности бизнеса.	
7	Корректирующие меры, которые не позволяют обнаружить инцидент и не имеют плана обеспечения непрерывности бизнеса.	

Авторы замечают, что время T_{Wj} не может быть непосредственно измерено. В случае отсутствия ущерба, можно сказать, что $T_{Fj} < T_{Wj.}$ Если же ущерб причинен, то T_{Wj} равняется моменту причинения ущерба. Все другие параметры могут быть непосредственно измерены.

Далее авторы устанавливают взаимосвязь классов контрольных механизмов, определенных в методологии и поведением реальной системы внутреннего контроля.

Брюэр и Лист утверждают, что класс обнаруживающих контрольных процедур может понижаться. Типична ситуация для контрольных процедур класса 2 и 3, когда для принятия корректирующих действий требуется больше времени, чем ожидалось. В такой ситуации контрольная процедура ведет себя как контрольная процедура классом ниже, например, контрольная процедура класса 2 ведет себя как контрольная процедура класса 3, или класса 4. [19]

[18] Brewer, D. & List, W. Measuring the effectiveness of an Internal Control System, Gamma Secure Systems Limited, 2004

[19] Sean Harris. CISSP All-In-One Exam Guide. // McGraw Hill Professional, 2013

Защитной мерой может служить наличие другой контрольной процедуры, который бы обнаруживал инцидент раньше. В таком случае, последовательность защитных мер называется «процедурой самоконтроля», когда ошибка контрольной процедуры на одном этапе, обнаруживается другим контрольным механизмом.

В случае наступления катастрофического события, система внутреннего контроля должна в обязательном порядке иметь защитные меры класса 7 для устранения последствий инцидента.

Базируясь на приведенной классификации, авторы описывают наиболее и наименее эффективную систему внутреннего контроля.

Наименее эффективная система внутреннего контроля:

- отказ любой контрольной процедуры не обнаруживается до наступления последствий инцидента;
- обнаруживающие контрольные процедуры не позволяют выявить инцидент до наступления последствий;
- план обеспечения непрерывности бизнеса отсутствует; любой инцидент становится неожиданностью для руководства компании.[20]

Наиболее эффективная система внутреннего контроля:

- любой отказ контрольной процедуры обнаруживается немедленно и позволяет принять корректирующие меры в пределах «окна» T_{Wj};
- все обнаруживающие контрольные процедуры имеют класс 2 и выше;
- план обеспечения непрерывности бизнеса разработан настолько подробно, что любой инцидент исправляется в пределах «окна» $T_{Wj.}$[21]

Из сравнения этих крайних случаев авторы выделяют 3 критерия, по которым можно определить уровень эффективности системы внутреннего контроля:

A. Способность обнаруживать отказы самих контрольных процедур системы внутреннего контроля;
B. Способность обнаруживать и быстро реагировать на инциденты;
C. Способность противодействовать инцидентам в непредвиденных обстоятельствах.

Брюэр и Лист измеряют эффективность системы внутреннего контроля относительно среднего уровня. Эффективность считается значительно ниже средней, когда два свойства не достигают среднего уровня. По аналогии, эффективность считается выше средней, когда одно из свойств превосходит средний уровень, а эффективность считается значительно выше средней, когда два свойства превосходят средний уровень. Авторы вводят систему баллов для численного измерения эффективности. За выполнение любого из свойств (A, B, C) на среднем уровне начисляются по 3 балла, за превышение уровня +1 балл, а за снижение -1 балл, за значительное превышение +2 балла, а за значительное снижение -2 балла. Таким образом, уровень эффективности системы внутреннего контроля измеряется следующим образом (Таб.1.2):

Таблица 1.2

Шкала измерения эффективности системы внутреннего контроля по Брюэру и Листу

Уровень эффективности	Баллы
Значительно выше средней	≥ 11 (3 балла за каждый из критериев среднего уровня, +1 очко за каждый из критериев уровня выше среднего)
Выше средней	10 (3 балла за каждый из критериев среднего уровня, +1 очко за один критерий уровня выше среднего)
Средний	9 (3 балла за каждый из критериев среднего уровня)
Ниже среднего	6-8 (3 балла за два критерия среднего уровня, или, в случае превышения среднего уровня одним или двумя критериями +1 очко за каждый)
Значительно ниже среднего	≤ 4 (2 балла за достижение двумя критериями уровня ниже среднего)[22]

[20] «Internal Control – Integrated Framework», Committee of Sponsoring Organizations of the Tread way Commission (COSO), 2013. URL: http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

[21] Monitoring of Internal Controls and IT. A Primer for Business Executives, Managers and Auditors on How to Advance Best Practices. - ISACA, 2010.

[22] Brewer, D. & List, W. Measuring the effectiveness of an Internal Control System, Gamma Secure Systems Limited, 2004

Таким образом, методология Д. Брюэра и У. Листа может быть использована для оценки эффективности контрольных процедур и контрольной среды в целом. Она позволяет установить оптимальные контрольные процедуры в необходимом количестве, давая возможность управлять оцененными рисками, а значит - своевременно реагировать на изменения внутренней и внешней среды организации.

Для оценки влияния непрерывного мониторинга на эффективность контрольной среды организации мы предлагаем использовать собственный подход, разработанный на основе методологии Брюэра и Листа.

Данный подход предусматривает усовершенствование методологии в части классификации контрольных процедур, а именно: введение дополнительных критериев оценки эффективности контрольной среды и дополнение существующих. Ниже представим детальное описание усовершенствований

Применение анализа факторов воздействия на бизнес для измерения временных параметров

Момент времени, при наступлении которого организация понесет ущерб, в случае наступления инцидента, не может быть непосредственно измерен. Однако, на наш взгляд, данный параметр является ключевым для оценки критериев эффективности контрольной среды. Мы предлагаем провести количественную оценку временных параметров на основе анализа факторов воздействия на бизнес (Business Impact Analysis), в ходе которого определяется максимально допустимое время простоя (MTD, Maximum Tolerable Downtime) для определенных контрольных процедур; и максимально допустимое время разрешения инцидента контрольной процедуры - $T_{Fj.}$ Это необходимо для понимания негативного воздействия на бизнес, вызванного инцидентом.

Мы предлагаем проводить данный анализ методом экспертных оценок, что позволит нам определить не только максимально допустимое время простоя, но и стоимость ущерба I_P.

Введение шкалы измерения скорости реакции контрольных процедур на инцидент

Введем шкалу измерения скорости реакции контрольных процедур на инцидент, в том числе скорости реакции механизмов непрерывного мониторинга.

Нам известно, что контрольные процедуры выполняются с некоторой регулярностью, заданной владельцем бизнес-процесса. Именно частота выполнения контрольных процедур влияет на время обнаружения инцидента.

Рассмотрим три сценария времени обнаружения инцидента контрольной процедурой.

Предположим, что контрольная процедура выявляет инцидент в момент его возникновения. При таком сценарии $T_{Dj} = T_{Ej,}$ а $T_{Fj} = 0$, так как обработка инцидента осуществляется до возникновения последствий. Согласно классификации Д. Брюэра и У. Листа такая контрольная процедура является предотвращающим и относится к классу 1.

Рассмотрим другой сценарий, когда инцидент обрабатывается обнаруживающей контрольной процедурой успешно, то есть в пределах максимально допустимого времени простоя. При таком сценарии необходимо определить затраты на обработку инцидента. которые зависят от скорости его обработки относительно времени обнаружения, и определяются близостью к одной из границ временного интервала MTD - T_{Dj}:

- затраты несущественны, если время обработки инцидента ближе к MTD, т.е.

$$\Delta T_{F_j} \leq \frac{MTD - T_{D_j}}{2}$$

- затраты существенны, если время обработки инцидента ближе к T_{Dj}, т.е.

$$\Delta T_{F_j} \geq \frac{MTD - T_{D_j}}{2}$$

Таким образом, существуют два сценария обработки инцидентов – с несущественными затратами и без ущерба, с существенными затратами и без ущерба (рис. 1.6).

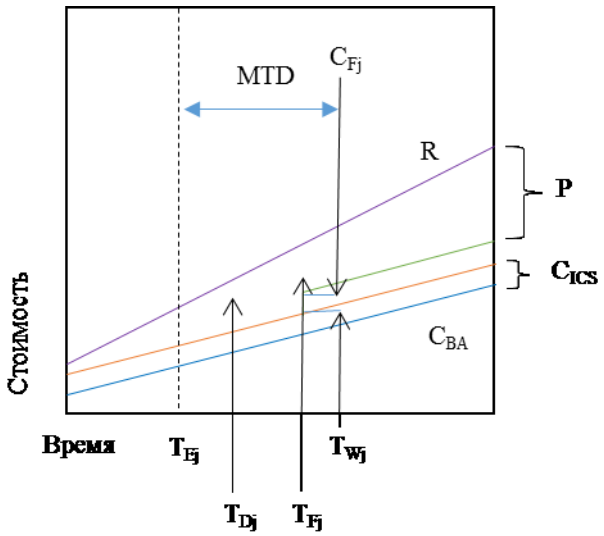


Рис.1.6 Обнаружение инцидента в пределах максимально допустимого времени простоя[23]

В обоих случаях инциденты обрабатываются в пределах максимально допустимого времени простоя.

Согласно классификации Брюэра и Листа, данные контрольные процедуры относятся к классу 2 и классу 3.

При третьем сценарии, инцидент обнаруживается раньше максимально допустимого времени простоя, но обрабатывается уже после того, как организация понесла ущерб. Контрольные процедуры, обрабатывающие инцидент в данном временном промежутке, относятся к классу 4.

Разработка критериев определения независимости контрольных процедур от человеческого фактора

Важным параметром для оценки влияния непрерывного мониторинга на эффективность контрольной среды организации является независимость контрольных процедур от человеческого фактора. Контрольная процедура может быть полностью автоматической, полуавтоматической, или ручной. В последних двух случаях выполнение контрольных процедур зависит от человеческого фактора. Введем критерии оценки независимости и представим их в таблице (таб. 1.3).

Таблица 1.3

Критерии оценки независимости контрольных процедур от человеческого фактора

Оценка независимости	Количество контрольных процедур определенного типа
Значительно выше средней	Ручные (менее 10%) Полуавтоматические (большинство) Автоматические (не менее одного)
Выше средней	Ручные (не более 30%) Полуавтоматические (большинство)
Средняя	Ручные (не более 50%) Полуавтоматические (большинство)
Ниже средней	Ручные (не более 70%) Полуавтоматические (меньшинство)
Значительно ниже средней	Ручные (более 80%)

[23] Deloitte – White paper. Continuous monitoring and continuous auditing. From idea to implementation. URL: https://www2.deloitte.com/content/dam/Deloitte/uy/Documents/audit/Monitoreo%20continuo%20y%20auditoria%20continua.pdf

В связи с введением дополнительного (четвертого) критерия для оценки эффективности контрольной среды организации, мы дополнили шкалу измерения общей эффективности с учетом балльной оценки данного критерия. Представим обновленную шкалу оценки ниже в таблице (таб. 1.4).

Таблица 1.4

Обновленная шкала оценки эффективности контрольной среды организации

Уровень эффективности	Количество баллов
Значительно выше средней	≥ 14 (3 балла за каждый из критериев среднего уровня, +1 очко за каждый из критериев уровня выше среднего)
Выше средней	13 (3 балла за каждый из критериев среднего уровня, +1 очко за один критерий уровня выше среднего)
Средний	12 (3 балла за каждый из критериев среднего уровня)
Ниже среднего	8-11 (3 балла за три критерия среднего уровня, или, в случае превышения среднего уровня двумя или тремя критериями +1 очко за каждый)
Значительно ниже среднего	≤ 6 (2 балла за достижение тремя критериями уровня ниже среднего)

Предложенный подход учитывает особенности применения непрерывного мониторинга, а так же делает методологию Брюэра и Листа более прозрачной в части оценки временных параметров, более точной в части классификации контрольных процедур и учитывает зависимость контрольных процедур от человеческого фактора.

Проанализировав принципы работы непрерывного мониторинга и выявив его преимущества, мы считаем, что внедрение непрерывного мониторинга помогает качественно улучшить контрольную среду организации, а именно позволяет получать достоверные данные в кратчайшие сроки за счет повышения операционной эффективности контрольных процедур. В ряде случаев, автоматизация контрольных процедур с помощью непрерывного мониторинга, приводит к сокращению издержек на контроль и аудит.

После изучения методологии Д. Брюэра и У. Листа были выявлены факторы, влияющие на эффективность контрольной среды организации. Одним из фундаментальных факторов является сочетание контрольных процедур в бизнес-процессах, то есть наличие контрольных процедур, способных обнаруживать отказы или ошибки других контрольных процедур.

Хотя вопрос влияния непрерывного мониторинга на эффективность контрольной среды актуален с точки зрения бизнеса, в современной научной литературе он малоизучен, поэтому представляет научный интерес.

Проанализировав различные источники, а также, основываясь на собственном практическом опыте участия в проектах оптимизации информационных потоков организации, мы пришли к выводам, что контрольная среда имеет большое влияние, как основа безопасного информационного обеспечения организации. Если контрольная среда неэффективна, то она оказывает отрицательное влияние на достижения бизнес - результатов. Кроме того, контрольная среда может повлиять на деловую репутацию организации и инвестиционную привлекательность бизнеса. В случае, если контрольная среда компании эффективна, то она способствует снижению различных рисков, повышает эффективность принятия решений и прозрачность бизнеса.

Список литературы (References)

1. *Пугачев В.В.* Внутренний аудит и контроль // В.В. Пугачев. – М.: Дело и сервис, 2010. С. 224
2. *Сонин А.М.* Внутренний аудит в новой реальности // *Аудитор.* 2012. № 7. с. 39–45
3. *Файоль А., Эмерсон Г., Тейлор Ф., Форд Г.,* Управление – это наука и искусство М.: Республика 1992. С 349

4. *Кастель М.* Информационная эпоха: экономика, общество и культура М.: Высшая школа экономики, 2010 С. 608

5. *Козырев А.А.* Информационные технологии в экономике и управлении СПб: Издательство Михайлова, 2012 С. 540

6. W. Affum. Evaluation of internal controls in Papso Ghana Limited – Study, June 2011 Approva Company. URL: http://ir.knust.edu.gh/bitstream/123456789/4228/1/William%20thesis.pdf

7. Benchmarks from SAP's Case Studies and Success Stories URL: http://www.ibs.ru/download/events/101109/SAP_Risk_Management.pdf

8. Brewer, D. & List, W. Measuring the effectiveness of an Internal Control System, Gamma Secure Systems Limited, 2004 pg. 38

9. Deloitte – White paper. Continuous monitoring and continuous auditing. From idea to implementation. URL: https://www2.deloitte.com/content/dam/Deloitte/uy/Documents/audit/Monitoreo%20continuo%20y%20auditoria%20continua.pdf

10. French Caldwell, Paul E. Proctor. Magic Quadrant for Continuous Controls Monitoring. – Gartner, 2010. Pg. 401

11. Gartner Identifies the Top 10 Strategic Technology Trends for 2013 URL: http://www.gartner.com/newsroom/id/2209615

12. Gyasi K. "Challenges of internal auditing in the era of good governance*"* Legon business journal, 2010 pg. 13 - 14

13. «Internal Control – Integrated Framework», Committee of Sponsoring Organizations of the Tread way Commission (COSO), 2013. URL: http: // www.coso.org / documents / 990025P_Executive_Summary_final_may20_e.pdf

14. KPMG - Whitepaper. Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance. URL: http: // www.kpmg.com/PT/pt/IssuesAndInsights / Documents / cacm080609.pdf

15. Sean Harris. CISSP All-In-One Exam Guide. // *McGraw Hill Professional,* 2013 pg. 168

16. Monitoring of Internal Controls and IT. A Primer for Business Executives, Managers and Auditors on How to Advance Best Practices. ISACA, 2010. Pg. 203.

Статья поступила в редакцию 02.11.2015 г.