

Байдина Марина Борисовна,
магистрант, филиал ФГБОУ ВПО «Российский экономический университет
им. Г.В. Плеханова», г. Воронеж

Тарасова Надежда Борисовна,
старший преподаватель кафедры экономики на предприятиях торговли, филиал
ФГБОУ ВПО «Российский экономический университет им. Г.В. Плеханова»,
г. Воронеж



Сколько стоит безопасность предприятия

Аннотация. Одним из условия обеспечения безопасности является разумная цена. В связи с этим, в статье рассмотрены основные расходы, связанные с обеспечением экономической безопасности, представлена формула расчета формулу затрат на экономическую безопасность. Система экономической безопасности не должна быть излишне дорогой, формализованной и сложной. В связи с этим в статье рассмотрены основные этапы построение системы экономической безопасности. Кроме этого, в статье затронут вопрос автоматизации деятельности службы экономической безопасности как инновационной деятельности.

Ключевые слова: показатели, экономическая безопасность, анализ, оценка.

Раздел: (04) экономика.

Одним из условия обеспечения безопасности является разумная цена. В связи с этим, рассмотрим основные расходы, связанные с обеспечением экономической безопасности (Б):

- суммарные затраты на реализацию автоматизации экономической безопасности (Z_a);
- стоимость подготовки проекта по внедрению автоматизированной системы для обеспечения экономической безопасности (Z_n);
- стоимость внедрения автоматизированной системы (Z_v) [2, с. 56];
- затраты на содержание персонала ($Z_{с.п.}$);
- затраты на аудит состояния существующей системы безопасности (Z_a) [3, с. 8].

Таким образом, представим формулу затрат на экономическую безопасность:

$$ЭБ = Z_a + Z_n + Z_v + Z_{с.п.} + Z_a. (1)$$

Теперь, затронем вопрос автоматизации деятельности.

Автоматизация деятельности относится к информационным технологиям.

Как отмечает Ю. В. Юрошкин, понятие «инновации» (нововведения) современная экономическая наука трактует как «...конечный результат инновационной деятельности, получивший воплощение в виде нового или усовершенствованного продукта, внедренного на рынке, нового или усовершенствованного технологического процесса, используемого в практической деятельности, либо в новом подходе к социальным услугам» [4, с. 49].

Как отмечает А. А. Ситнов, под информационной технологией понимают систему правил, определяющих способ сбора, накопления, регистрации, передачи, обработки, хранения, поиска, модификации, анализа, защиты, выдачи необходимой информации всем заинтересованным подразделениям или отдельным пользователем [5, с. 45].

Необходимо отметить, что система экономической безопасности не должна быть излишне дорогой, формализованной и сложной.



В связи с этим рассмотрим основные этапы построение системы экономической безопасности:

- 1 этап – разграничение полномочий между субъектами;
- 2 этап – анализ рисков планирование внутренних проверок экономической безопасности;
- 3 этап – организация работы системы экономической безопасности;
- 4 этап – проведение процедур по контролю за системой экономической безопасности в соответствии с утвержденным планом и представление отчетов.

На первом этапе разграничиваются не только полномочия, обязанности, но и ответственность.

На втором этапе проводятся утверждения политики и процедур оценки экономической безопасности предприятия, уточнение целей и задач такой оценки, оценка рисков и их классификация, утверждение календарного плана оценочных и контрольных мероприятий.

На третьем этапе производится согласование сроков и условий оценочных и контрольных процедур и разработка плана текущей оценки и контроля.

На четвертом этапе проводятся мероприятия согласно плану оценки и контроля экономической безопасности и оценивается эффективность системы экономической безопасности.

В качестве оценке экономической безопасности в Сбербанке внедрена организация системы интегрированного управления рисками.

Система интегрированного управления рисками Группы удовлетворяет следующим основным принципам:

1. Осведомленность о риске. Процесс управления рисками затрагивает каждого сотрудника организаций-участников Группы. Принятие решений о проведении любой операции производится только после всестороннего анализа рисков на уровне организаций-участников Группы, возникающих в результате такой операции. Сотрудники организаций-участников Группы, совершающие операции, подверженные рискам, осведомлены о риске операций и осуществляют идентификацию, анализ и оценку рисков перед совершением операций. В организациях-участниках Группы действуют нормативные документы, регламентирующие порядок совершения всех операций, подверженных рискам. Проведение новых банковских операций при отсутствии нормативных, распорядительных документов или соответствующих решений коллегиальных органов, регламентирующих порядок их совершения, не допускается.

2. Разделение полномочий. В организациях-участниках Группы реализованы управленческие структуры, в которых отсутствует конфликт интересов: на уровне организационной структуры разделены подразделения и сотрудники, на которых возложены обязанности по проведению операций, подверженных рискам, учету этих операций, управлению и контролю за рисками.

3. Контроль за уровнем риска. Руководство Банка, коллегиальные органы Банка на регулярной основе получают информацию об уровне принятых Группой рисков и фактах нарушений установленных процедур управления рисками, лимитов и ограничений.

На уровне Группы, а также на уровне каждой организации-участника Группы функционирует система внутреннего контроля, позволяющая осуществлять эффективный контроль за функционированием системы управления рисками каждой организации-участника Группы и Группы в целом.

4. Необходимость обеспечения «трех линий защиты». Устанавливается коллективная ответственность за действия по принятию рисков:



– принятие рисков (1-я линия защиты): Бизнес-подразделения должны стремиться к достижению оптимального сочетания доходности и риска, следовать поставленным целям по развитию и соотношению доходности и риска, осуществлять мониторинг решений по принятию риска, учитывать профили рисков клиентов при совершении операций/сделок, внедрять и управлять бизнес-процессами и инструментами, участвовать в процессах идентификации и оценки рисков, соблюдать требования внутренних нормативных документов, в том числе в части управления рисками;

– управление рисками (2-я линия защиты): функции Рисков и Финансов – разрабатывают стандарты управления рисками, принципы, лимиты и ограничения, проводят мониторинг уровня рисков и готовят отчетность, проверяют соответствие уровня рисков аппетиту к риску, консультируют, моделируют и агрегируют общий профиль рисков;

– аудит (3-я линия защиты): функция внутреннего и внешнего аудита – проводят независимую оценку соответствия процессов управления рисками установленным стандартам, внешнюю оценку решений по принятию рисков.

5. Сочетание централизованного и децентрализованного подходов к управлению рисками Группы.

В Группе сочетаются централизованный и децентрализованный подходы управления рисками. Уполномоченные коллегиальные органы Банка по управлению рисками определяют требования, ограничения, лимиты, методологию в части управления рисками для территориальных банков, организаций-участников Группы. Территориальные банки, организации-участники Группы осуществляют управление рисками в рамках установленных для них уполномоченными органами и/или должностными лицами ограничений и полномочий.

6. Формирование комитетов по рискам высокого уровня.

– специализированные комитеты высокого уровня принимают решения по управлению рисками;

– система комитетов сформирована с учетом структуры бизнес-модели Группы.

7. Необходимость обеспечения независимости функции Рисков.

– обеспечение независимости профильных подразделений оценки и анализа рисков от подразделений, совершающих операции/сделки, подверженные рискам;

– включение функции Рисков в процесс принятия решений на всех уровнях, вовлечение функции Рисков как в высокоуровневый процесс принятия стратегических решений, так и в управление рисками на операционном уровне;

– обеспечение независимости функции валидации.

8. Использование информационных технологий. Процесс управления рисками строится на основе использования современных информационных технологий. В организациях-участниках Группы применяются информационные системы, позволяющие своевременно идентифицировать, анализировать, оценивать, управлять и контролировать риски.

9. Постоянное совершенствование систем управления рисками.

Организации-участники Группы постоянно совершенствуют все элементы управления рисками, включая информационные системы, процедуры и методики с учетом стратегических задач, изменений во внешней среде, нововведений в мировой практике управления рисками.

10. Управление деятельностью Группы с учетом принимаемого риска.



Группа осуществляет оценку достаточности имеющегося в ее распоряжении (доступного ей) капитала, то есть внутреннего капитала (далее ВК) для покрытия принятых и потенциальных рисков. Внутренние процедуры оценки достаточности капитала (далее – ВПОДК) также включают процедуры планирования капитала исходя из установленной стратегии развития Группы, ориентиров роста бизнеса и результатов всесторонней текущей оценки указанных рисков, стресс-тестирования устойчивости Банка и Группы по отношению к внутренним и внешним факторам рисков.

Группа выделяет приоритетные направления развития и распределения капитала с использованием анализа скорректированных по риску показателей эффективности отдельных подразделений и направлений бизнеса. Группа включает риск-метрики в укрупненные Бизнес-планы.

11. Ограничение принимаемых рисков посредством установления значений лимитов в рамках сформированной системы лимитов.

В Группе действует система лимитов и ограничений, позволяющая обеспечить приемлемый уровень рисков по агрегированным позициям Группы. Система лимитов Группы имеет многоуровневую структуру:

- общий лимит по Группе, который устанавливается исходя из аппетита к риску, определенного согласно стратегии управления рисками;
- лимиты по видам существенных для Группы рисков (например, лимиты в отношении кредитного и рыночного рисков);
- лимиты по организациям-участникам Группы, структурным подразделениям организаций-участников Группы, ответственных за принятие существенных для Группы рисков;
- лимиты на отдельных заемщиков (контрагентов), по инструментам торгового портфеля и т.п.

12. Методология идентификации, оценки и управления рисками в организациях-участниках Группы формируется на основе единства методологических подходов, применяемых в рамках Группы.

Ссылки на источники

1. Власенко М. Экономика безопасности предприятия / М. Власенко // Директор по безопасности. № 27. – 2014. – С.12–16.
2. Волкова М. Н. Организация и методика аудита качества управления коммерческими структурами: автореферат диссертации на соискание ученой степени кандидата экономических наук / М. Н. Волкова // Воронежский государственный аграрный университет им. К.Д. Глинки. Воронеж, – 2007. – 204 с.
3. Волкова М. Н. Методологические аспекты взаимосвязи аудиторских процедур: запросов и подтверждении / М. Н. Волкова // ФЭС: Финансы. Экономика. Стратегия. 2010.– № 11. – С. 7–10.
4. Ерошкин Ю. В. Инновационный риск в системе банковских рисков / Ю. В. Ерошкин // Аудиторские ведомости, – № 4. – 2012. – С.49–54.
5. Ситнов А. А. Стандарт COBI T: новые возможности российского аудита, № 6, – 2012. – С.15–18.

Marina Baidina,

Master student, branch of Russian University of Economics after G.V. Plekhanov, Voronezh

Nadezhda Tarasova,

Senior lecturer at the chair of economics of trade enterprises, branch of Russian University of Economics after G. V. Plekhanov in Voronezh, Voronezh





ART 14647

УДК 339

How much is the security of the enterprise

Abstract. One of the security conditions is a reasonable price. In this regard, the article considers the main costs associated with the provision of economic security, presented a formula for calculating the cost of formula economic security. The system of economic security should not be too expensive, formal and complex. In this regard, the article describes the main steps of building a system of economic security. In addition, the article raised the issue of automation of activity economic security as innovation.

Key words: Economic Security Service, security automation, calculation of economic security.

Рекомендовано к публикации:

Горевым П.М., кандидатом педагогических наук, главным редактором журнала «Концепт»