
ЭКОНОМИЧЕСКИЕ НАУКИ

УДК 336.025

¹*Л.В. Каширская, ²К.А. Моисеева*

¹Финансовый университет при Правительстве Российской Федерации, Москва,
email: kashirskaya76@mail.ru

²ИП Хаперская Н.С., Москва, email: khaperskaya.karina@yandex.ru

СУЩНОСТЬ И ЗНАЧЕНИЕ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ДЛЯ ЦЕЛЕЙ ВНУТРЕННЕГО КОНТРОЛЯ КОМПАНИИ

Ключевые слова: внутренний контроль; экономическая безопасность; система; угроза; экономический субъект.

Рассматриваются сущность систем экономической безопасности и внутреннего контроля и то, как соотносятся между собой данные два элемента. **Сделан вывод, что текущая экономическая среда требует от организаций создания систем внутреннего контроля.** В свою очередь, неспособность экономических субъектов уделять достаточное внимание вопросам контроля может привести к ослаблению их конкурентной позиции. Внутренний контроль не всегда гарантирует не только эффективное функционирование организации, но и ее устойчивость и максимальное развитие в условиях конкуренции.

¹*L.V. Kashirskaya, ²K.A. Moiseeva*

¹Financial University under the Government of the Russian Federation, Moscow,
email: kashirskaya76@mail.ru

²IP Khaperskaya N.S., Moscow, email: khaperskaya.karina@yandex.ru

THE ESSENCE AND SIGNIFICANCE OF THE ECONOMIC SECURITY SYSTEM FOR THE PURPOSES OF INTERNAL CONTROL OF THE COMPANY

Keywords: internal control; economic security; system; threat; economic entity.

The essence of economic security and internal control systems and how these two elements relate to each other are considered. It is concluded that the current economic environment requires organizations to create internal control systems. In turn, the inability of economic entities to pay sufficient attention to control issues may lead to a weakening of their competitive position. Internal control does not always guarantee not only the effective functioning of the organization, but also its stability and maximum development in a competitive environment.

Учитывая тот факт, что Российская Федерация находится на этапе глобализации экономической системы, в связи с чем важность укрепления экономической безопасности возрастает не только для страны, но и для всех предприятий. Вопросы: «Как обеспечить экономическую безопасность для своего предприятия?», «Как внедрить внутренний контроль?», «При помощи каких методов можно достигнуть состояния экономической стабильности?» – все они

рассматриваются не только в рамках предприятий, но и в контексте экономической глобализации. Наступивший в Российской Федерации финансовый кризис показал существующие на данном этапе экономического цикла недостатки в разрезе рыночных отношений. Основным из которых является отсутствие актуальной информации, касательно финансового положения хозяйствующих субъектов. Этот аспект обусловлен отсутствием в хозяйству-

ющих субъектах должного уровня организации системы внутреннего контроля (СВК) или же его полным неосуществлением. Для устранения этого недочета необходимо создание СВК в компаниях. Следует отметить, что СВК используется во всем мире для минимизации рисков путем выстраивания системы контроля и адекватной линии реагирования на возникшие риски и угрозы. Этот принцип необходим для достижения поставленных высшим руководством целей и задач с целью получения максимальной прибыли в отчетном периоде, а также для правильного и быстрого выхода из различных кризисных ситуаций.

Цель исследования

Цель исследования состоит в получении результатов, направленных на формирование понятийного аппарата специалистов, деятельность которых связана с обеспечением экономической безопасности и осуществлением внутреннего контроля в хозяйствующем субъекте.

Материал и методы исследования

Методологической основой исследования являются труды отечественных ученых и исследования практикующих специалистов в сфере обеспечения экономической безопасности, а также осуществления внутреннего контроля в субъектах хозяйствования.

Несмотря на то, что проблематика внутреннего контроля не является для новой для российской науки, она не изучалась отдельно. Изучая экономическую безопасность на примере субъектов хозяйствования, многие ученые, как теоретики, так и практики, пришли к единому мнению – она (безопасность) может существовать и функционировать только при комплексном использовании защитной стратегии и мер направленных на минимизацию последствий рисков событий и угроз на всех этапах функционирования системы. Авторами также было сделано заключение о том, что экономическая безопасность, в разрезе хозяйствующего субъекта, реализуется путем минимизации риска в условиях наличия:

– стратегии экономической безопасности хозяйствующего субъекта;

– алгоритма действий и «санитарных процедур», направленных на своевременное обнаружение и устранение угроз;

– эффективной СВК, снижающей влияние финансовых рисков [1].

Результаты исследования и их обсуждение

Экономическая безопасность предприятия выступает комплексным понятием, интегрирующим в себя набор факторов, сопряженных с внешней средой функционирования предприятия, ее предметом и воздействием, а не с его внутренним состоянием. В настоящее время существуют различные трактовки термина «экономическая безопасность предприятия».

Согласно Сенчагову В.К. – экономическая безопасность предприятия – способность к защите и воспроизводству научно-технического, производственного и кадрового потенциала предприятия от экономических угроз прямого или косвенного воздействия, например, сопряженных с неэффективной государственной научно-промышленной политикой и неблагоприятным формированием внешней среды [2].

С точки зрения Степичева О.А. и Мамонтова В.Д. под данным термином понимается такое состояние экономики компании и его органов управления, которое позволяет обеспечить защищенность интересов и целевых ориентиров предприятия от возможного действия угрожающих факторов [3].

Гончаренко А.П. трактовал экономическую безопасность предприятия в качестве состояния, при котором ресурсы компании, требуемые для нивелирования угроз и обеспечения его стабильного функционирования, используются наиболее эффективным образом [4].

По мнению Глумвы А.Н. и Кисельца Е.П., экономическая безопасность предприятия представляет собой состояние наиболее эффективного использования ресурсного потенциала, позволяющее нивелировать угрозы, обеспечивать эффективное и стабильное функционирование компании в текущем периоде и на перспективу [5].

Многие определения подходят только для определенных сфер деятельности предприятия, так как полны ав-

торских особенностей и субъективных специализаций. И наоборот, некоторые определения являются очень общими, более приближенным к терминам «эффективность» и «управление». Исходя из этого, можно предположить, что определение «экономическая безопасность хозяйствующего субъекта» можно систематизировать в зависимости от подхода следующим образом:

– системный подход – включает организационные и производственные работы, правовые отношения как материальных, так и интеллектуальных ресурсов. При данном подходе гарантируется стабильность функционирования, финансовую и коммерческую стабильность, а также прогресс в научно-техническом развитии [6];

– ситуационный подход – хозяйствующие субъекты обеспечивают самостоятельное устойчивое социально-экономическое развитие, поддерживая необходимый для них уровень конкурентоспособности [7];

– функциональный подход – включает в себя аккумуляцию финансового, интеллектуального, кадрового, политико-правового, экологического, информационного и энергетического сектора.

– процессный подход: изучает бизнес-процессы, присутствующие на предприятии, и влияние этих бизнес-процессов на экономическую безопасность предприятия [8].

Классификация внешних по отношению к компании угроз представлена на рисунках 1 и 2.

Система экономической безопасности хозяйствующего субъекта должна обеспечивать контроль финансовых, правовых, производственных, имущественных и иных интересов, реализуемых данным субъектом. Экономические интересы субъекта выражаются в потребностях различного рода, удовлетворение которых необходимо для его существования и активного развития.

Удовлетворение данных интересов позволяет поддержать устойчивое и уверенное развитие, которое необходимо для «поддержания на плаву» организации, в условиях экономической турбулентности. Экономическая безопасность субъекта хозяйствования

своеобразное «зеркало», показывающее верность управленческой антирисковой стратегии ТОП менеджмента субъекта. Данная стратегия, при условии ее грамотного составления и осуществления своевременного контроля за ее исполнением, обеспечивает повышение конкурентоспособности компании, устойчивую прибыль и достижение поставленных ТОП менеджментом целей и задач на текущий период.

Управление всегда «ходит бок о бок» с понятием «контроль». Без этого понятия, а главное действия, теряется всякий смысл менеджмента. Это обусловлено тем, что менеджмент (а главное контроль) является одним из этапов управления. В современных реалиях контроль занимает особое место в осуществлении управленческой деятельности, так как он является залогом к функционированию как всей «машины» (хозяйствующего субъекта), так и отдельных ее элементов (финансово-хозяйственной, производственной и иных сфер), что позволяет субъекту устойчиво функционировать. Подводя итог этой мысли, можно выделить главное – контроль не существует отдельно, он является неотъемлемой частью управления.

Термин «контроль» трактуется каждым автором по-разному. К примеру, профессор В.И. Бобошко выбрал для себя «широкую трактовку» данного термина – это «проверка соблюдения и выполнения нормативно установленных заданий, планов и решений» [10; 11, с. 16]. В данном случае особое значение отводится функциональному назначению понятия «контроль» и необходимости вовлечения в управленческий процесс. В узком смысле слова контроль выступает составляющим элементом функционала управленческого процесса.

В управленческом подходе выделяют задачи и функции, которые не являются монументальными, а остаются «мобильными», чтобы отвечать условиям рынка сегодняшнего дня (изменение направления государственной политики, подвижки в финансово-экономическом секторе и прочие турбулентности, связанные с ведением бизнес-деятельности).

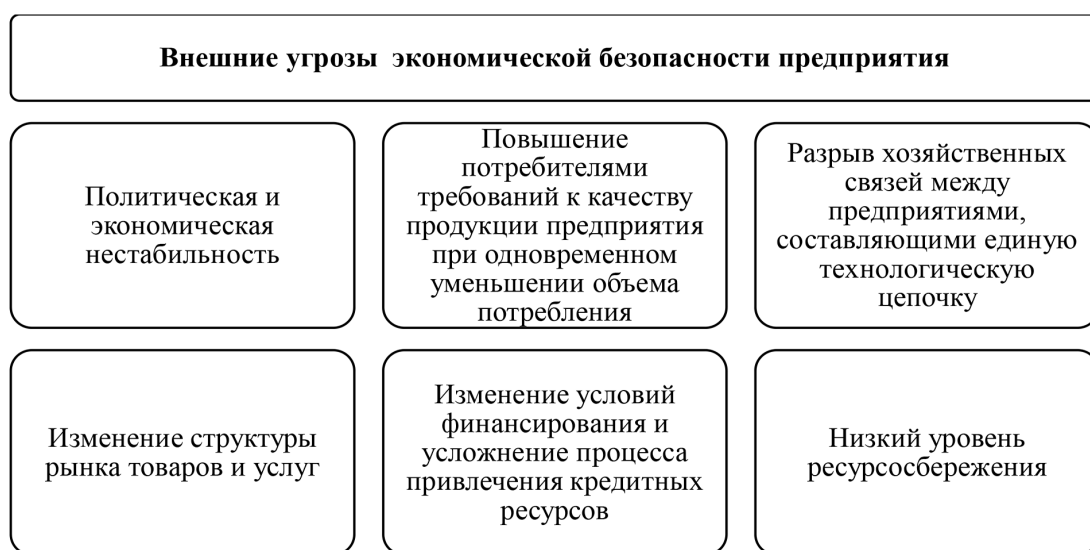


Рис. 1. Классификация внешних по отношению к компании угроз экономической безопасности

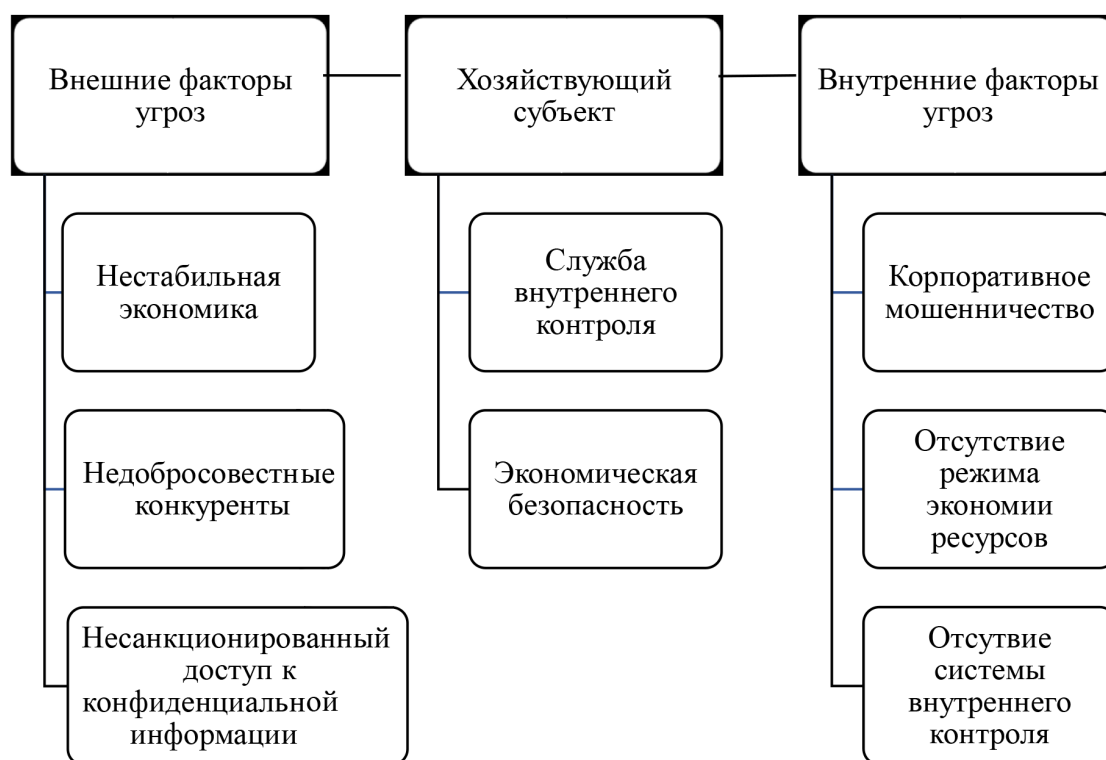


Рис. 2. Состав факторов, оказывающих влияние на экономическую безопасность хозяйствующего субъекта [9]

Однако, существуют обобщенные задачи контроля в целях осуществления экономического управления:

– осуществление экономическими агентами деятельности, опирающейся на действующее в стране законодательство;

– эффективность планирования финансово-хозяйственной деятельности, отвечающая нынешним реалиям рынка;

– ведение бухгалтерского учета и составление отчетности в соответствии с действующим в стране законодательством;

– поддерживать имущество хозяйствующего субъекта в целостном состоянии;

– выявление внутренних резервов роста для достижения эффект от осуществления деятельности хозяйствующего субъекта;

– аналитической оценки осуществления финансово-хозяйственной деятельности субъекта, его состояния, выявление отклонений на своевременной основе и их предотвращение;

– установления наказаний для нарушителей законодательства [10].

СВК включает в себя следующие составные этапы (рис. 3).

В рамках оценки системы экономической безопасности для целей внутреннего контроля необходимо провести мониторинг предусмотренных организацией контрольных мероприятий по ряду направлений, а именно:

1) при проведении контрольных мероприятий в подсистеме управления доступом, в зависимости от целей мероприятий, могут выполняться следующие проверки:

– проверка соответствия установленных прав доступа (в прикладных системах, базах данных и т.п.) полномочиям в рамках трудовых обязанностей работника;

– проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;

– проверка процесса идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам информационных систем);

– проверка механизмов блокирования доступа к средствам защиты от несанкционированного доступа (далее – НСД) при выполнении устанавливаемого числа неудачных попыток ввода пароля;

– проверка системы смены пароля принудительным образом (по истечению срока действия пароля);

– проверка выполнения требований по стойкости пароля.

2) при контрольных мероприятиях в подсистеме регистрации и учета, могут выполняться следующие проверки:

– проверка системных журналов на наличие зарегистрированных попыток несанкционированного доступа;

– проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации и внутренних документах компании;

– имитация попытки несанкционированного доступа в систему, для проверки работы системы регистрации попытки НСД в системном журнале;

– проверка способов защиты системного журнала регистрации от уничтожения или модификации нарушителем (нарушитель (субъект атаки) – лицо (или иницируемый им процесс), проводящее (проводящий) атаку);

– проверка функционирующей системы автоматического непрерывного мониторинга событий в системе, которые могут являться причиной реализации угроз (создание, редактирование, запись, компиляция объектов).

3) при проведении проверок в части учета и хранения носителей персональных данных (далее – ПДн) могут выполняться следующие проверки:

– проверка мест хранения носителей ПДн, сейфов и металлических шкафов, надежность их замков;

– проверка выполнения установленного порядка учета и хранения носителей ПДн;

– проверка фактического наличия всех носителей ПДн, в том числе учетные журналы, дела, документы (поступившие, изданные, переведенные на выделенное хранение);

– проверка фактического наличия всех носителей ПДн, переданных на архивное хранение;

– проверка фактического наличия всех не подшитых в дела и поступивших документов, содержащих ПДн, независимо от даты их регистрации;

– проверка номенклатуры дел с целью выделения документов, содержащих ПДн, для передачи в архив или на уничтожение;

– проверка правильности проставления регистрационных данных носителей, документов и дел, и учетных журналов;

– проверка правильности проставления в журнале отметок о движении носителей.



Рис. 3. Этапы формирования системы внутреннего контроля экономического субъекта [10]

4) при контрольных мероприятиях в подсистеме обеспечения целостности, могут выполняться следующие проверки:

- проверка механизмов контроля целостности пакетов обновлений средств защиты информации с использованием контрольных сумм;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка целостности используемого программного обеспечения, путем вычисления контрольных сумм;
- проверка фактического наличия экземпляров резервных копий;
- проверка целостности сделанных резервных копий путем восстановления данных;
- имитация выполнения резервного копирования и восстановления данных при аварийном режиме функционирования системы.

5) при контрольных мероприятиях в подсистеме антивирусной защиты, могут выполняться следующие проверки:

- проверка рабочих станций и серверов станций на наличие установленных программных средств антивирусной защиты;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;

– проверка механизма своевременного обновления программных средств антивирусной защиты (в т.ч. баз данных вирусных сигнатур) на всех рабочих и серверных станциях;

- запуск полного сканирования системы в режиме реального времени антивирусным средством;
- проверка антивирусным средством используемых отчуждаемых носителей;
- проверка функционирования механизмов принудительной проверки используемых съемных носителей;
- имитация попыток заражения вредоносным программным обеспечением серверных и рабочих станций;
- просмотр системных журналов и отчетов на наличие зафиксированных случаев заражения вредоносным ПО.

6) при проведении контрольных мероприятий в подсистеме обеспечения безопасного межсетевого взаимодействия, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия установленных межсетевых экранов требуемому уровню защищенности;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток проникновения в «закрытый» сегмент сети из открытого, в том числе с применением специального ПО;

– проверка системных журналов на наличие зафиксированных попыток обращения к «закрытым» ресурсам.

7) при проведении контрольных мероприятий в подсистеме анализа защищенности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

– проверка выполнения своевременного обновления ПО, используемого для анализа защищенности, в т.ч. баз данных уязвимостей;

– проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;

– имитация попыток преодоления системы защиты, проверка системных журналов на наличие зафиксированных попыток НСД.

8) при проведении контрольных мероприятий в подсистеме обнаружения и предотвращения вторжений, в зависимости от целей мероприятий, может выполняться проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.

9) при проведении контрольных мероприятий в подсистеме защиты от утечек по техническим каналам, могут выполняться следующие проверки:

– проверка в помещениях, где ведется обработка ПДн, установленных на окна жалюзи, штор и т.п.;

– проверка размещения дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторы, телевизоры и т.п.) таким образом, чтобы исключалась возможность просмотра посторонними лицами текстовой и графической информации, содержащей персональные данные.

10) при проведении контрольных мероприятий в подсистеме физической защиты, могут выполняться следующие проверки:

– проверка введения журналов учета посетителей, проходящих на территорию организации;

– проверка введения журналов посетителей, проходящих в защищаемые помещения;

– проверка электронных журналов СКУД на предмет попыток НСД

в защищаемые помещения сотрудников, не имеющих права доступа в данные помещения;

– проверка наличия ключей (в том числе и электронных пропусков) от защищаемых помещений, а также проверка сохранности вторых экземпляров ключей от защищаемых помещений;

– просмотр всех заявлений об утерянных ключах (в том числе и электронных пропусках) по которым можно получить доступ в защищаемые помещения, а также проверка принятых мер (блокирование электронного пропуска, смена замка);

– проверка надежности замков, установленных в защищаемых помещениях;

– имитация попытки проникновения в защищаемые помещения для проверки срабатывания сигнализации и (или) системы контроля и управления доступом.

11) при проведении контрольных мероприятий в подсистеме криптографической защиты, могут выполняться следующие проверки:

– проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.

– проверка сохранности эксплуатационной и технической документации и ключевых документов на средства криптографической защиты;

– проверка журналов учета средств криптографической защиты и используемых криптоключей на правильность их ведения и хранения;

– проверка знаний работниками, использующими средства криптографической защиты, правил применения этих средств и правил обращения с криптоключами;

– проверка функционирования средств криптографической защиты путем имитации процессов, шифрования и дешифрования информации.

Выводы

Для эффективного функционирования любого экономического субъекта необходимо организованное проведение контроля. Его основная задача – выявление и предотвращение недостатков и нарушений, а также их своевременное устранение. Внутренний контроль, но только при условии его грамотной

организации, существенно повышает экономическую безопасность хозяйствующих субъектов, что непосредственно влияет на общую экономическую безопасность страны. Важно понимать, что экономическая стабильность зависит от хорошо разработанной системы внутреннего и внешнего контроля.

Библиографический список

1. Сажина С.С., Таралина В.В. Внутренний контроль и экономическая безопасность предприятия // Молодой ученый. 2018. № 26 (212). С. 93-95.
2. Сенчагов В.К. Экономическая безопасность России: общий курс: учебник; 3-е изд. М.: БИНОМ. Лаборатория знаний, 2012 813 с.
3. Вестник Тамбовского университета, серия гуманитарные науки. 2011. Т.104. №12–2. С. 445-449.
4. Справочник экономиста. 2004. № 12. С. 31-36. [Электронный ресурс]. URL: https://www.profiz.ru/se/12_2004/ (дата обращения 13.11.2023).
5. Академический вестник. 2013. № 4. [Электронный ресурс]. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_Per_1058723/ (дата обращения 13.11.2023).
6. Буланов С.Ю. Социально-экономические угрозы экономической безопасности России и европейский опыт их предотвращения. М., 2007. 91 с.
7. Глазьев С.Ю. Безопасность экономическая // Политическая энциклопедия. Т. 1 М., 1999. 189 с.
8. Белкин Д.В. Основные подходы к исследованию экономической безопасности предприятий // Вектор науки ТГУ. 2011 № 4 (18). С. 183-186.
9. Свиридова Л.А., Литвинова О.А., Решетова В.В. Внутренний контроль как инструментарий экономической безопасности хозяйствующего субъекта // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей IX Международной научно-практической конференции, г. Пенза, 15 января 2018 г. В 4-х частях. Пенза: МЦНС «Наука и Просвещение», 2018. С. 198-201.
10. Егорова Е.В., Евраев Л.О. Внутренний контроль и экономическая безопасность // Вестник экономической безопасности. 2022. № 3. С. 277-279. DOI: 10.24412/2414-3995-2022.
11. Бобошко В.И. Контроль и ревизия: учебное пособие. М: ЮНИТИ-ДАНА, 2015. 310 с.