Оценка информационных рисков в обеспечении экономической безопасности предприятия

О. Б. Кузнецова

Настоящая статья посвящена актуальной проблеме оценки эффективности управления коммерческих структур, обеспечивающей способность противостоять негативным воздействиям внешней среды. Первостепенной задачей является экономическое обоснование инвестиций для защиты информационных технологий, играющих особую роль в принятии управленческих решений на предприятии.

Сущность понятия «Экономическая безопасность предприятия»

Под «безопасностью» в широком смысле слова понимается свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение.

При определении понятия «экономическая безопасность» рассматривались различные подходы к трактовке этой проблемы, опубликованные в отечественной литературе, основными из которых являются следующие.

1. Экономическая безопасность предприятия рассматривается прежде всего как проблема защиты информации, которая обеспечивается в форме двухуровневой системы. Первый уровень предполагает сохранность секретов силами службы безопасности организации, а второй — предусматривает формирование психологической атмосферы «бдительности и ответственности» персонала организации с помощью так называемых координаторов, назначаемых из лиц среднего руководящего звена и пользующихся среди сотрудников авто-

ритетом. Признавая, что сохранность информации является одним из важных аспектов экономической безопасности предприятия, необходимо отметить, что сведение проблемы экономической безопасности предприятия только к защите коммерческой тайны представляет собой слишком упрощенный вариант решения такой проблемы и не учитывает всего спектра влияния внешней среды как основного источника опасностей для деятельности предприятия [3, 4, 5, 6].

2. Формирование рыночных отношений, изменение функций государства в управлении предприятий позволили рассматривать проблему экономической безопасности предприятия намного шире — как возможность обеспечения его устойчивости в разнообразных, в том числе и в неблагоприятных условиях, которые складываются во внешней среде, вне зависимости от характера ее влияния на деятельность предприятия, масштаба и характера внутренних изменений. Так, экономическая безопасность предприятия определена как «защищенность его деятельности от отрицательных влияний внешней среды, а также как способность быстро устранить разно вариантные угрозы или приспособиться к существующим условиям, которые не сказываются отрицательно на его деятельности» [1, 2]. По существу данное трактование отождествляет понятия экономической безопасности с понятием адаптации к текущим условиям, и тем самым теряется видение перспектив его развития.
3. Экономическая безопасность трактуется как «количественная и качественная характеристика свойств фирмы, отражающая способность „самовыживания“ и развития в условиях возникновения внешней и внутренней угрозы» [1]. Экономическая безопасность предприятия определяется совокупностью факторов, отражающих независимость, устойчивость, возможности роста, обеспечения экономических интересов и т. д. При таком рассмотрении создается мнение, что предприятие и угрозы его деятельности являются разрозненными явлениями, не связанными между собой по своей природе. Реально же угрозы возникают в той же среде, в которой функционирует и само предприятие.
4. В рамках подхода к экономической безопасности предприятия как состоянию, определяемому влиянием внешней среды, следует отметить ресурсно-функциональный подход. Авторы этого подхода экономическую безопасность предприятия рассматривают как «состояние наиболее эффективного использования корпоративных ресурсов

для предотвращения угроз и обеспечения стабильного функционирования предприятия в настоящее время и в будущем» [7]. В ресурсно-функциональном подходе в качестве основных направлений экономической безопасности предприятия различают семь функциональных составляющих: интеллектуально-кадровую, финансовую, технико-технологическую, политико-правовую, экологическую, информационную и силовую.

Изучение сущности ресурсно-функционального подхода к пониманию экономической безопасности предприятия позволяет отметить его основное достоинство — всеобъемлющий, комплексный характер, поскольку в рамках этого подхода исследуются важнейшие факторы, влияющие на состояние функциональной составляющей экономической безопасности предприятия, изучаются основные процессы, влияющие на ее обеспечение, проводится анализ распределения и использования ресурсов предприятия, рассматриваются экономические индикаторы, отражающие уровень обеспечения функциональной составляющей экономической безопасности предприятия, и разрабатываются меры по обеспечению максимально высокого уровня функциональной составляющей экономической безопасности предприятия.

5. Отдельно следует сказать о подходах к экономической безопасности предприятия, которые можно назвать узкофункциональными, т. е. рассматриваемые с позиции отдельного аспекта его деятельности [8]. В этом подходе в качестве основной функции управления, направленной на обеспечение экономической безопасности, признается учет, поскольку именно учет создает информационные условия для эффективного использования ресурсов, предотвращения угроз и финансовой безопасности предприятия. Однако, отсутствие возможности объединить узкофункциональные направления, снижают результативность данного подхода.

Анализ рассмотренных подходов к проблеме экономической безопасности предприятия позволяет сделать следующие выводы:

- экономическая безопасность предприятия складывается из нескольких функциональных составляющих, которые для каждого конкретного предприятия могут иметь различные приоритеты в зависимости от характера существующих угроз.
- основным фактором, определяющим состояние экономической безопасности является обладание предприятием устойчивыми кон-

курентными преимуществами. Эти преимущества должны соответствовать стратегическим целям предприятия и обеспечивать экономическую состоятельность предприятия.

- экономическая состоятельность является отражением отношений между хозяйствующими субъектами, позволяющими им эффективно существовать в бизнесе и адаптироваться к условиям внешней среды (признаки рыночной состоятельности), оптимально использовать производственный потенциал (признаки по показателям производственной состоятельности), обеспечивать сбалансированность внешнего и внутреннего равновесия (признаки финансовой состоятельности).

На основании сделанных выводов можно сформулировать наиболее общее определение: экономическая безопасность предприятия — это наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и организационной структуры предприятия его стратегическим целям и задачам.

Данное определение подчеркивает тот факт, что экономическая безопасность находится на стыке экономики и безопасности предприятия.

Информационная составляющая экономической безопасности предприятия

Исходя из данного выше определения, следует выделить основные функциональные блоки системы экономической безопасности предприятия, обеспечивающие максимальное соответствие менеджмента предприятия и его ресурсного потенциала:

- имущество (активы) предприятия;
- финансы предприятия;
- кадры предприятия;
- технологии и инновации
- информационная система предприятия;
- организационная структура предприятия.

Данная структура функциональных составляющих соответствует структуре механизма обеспечения экономической безопасности предприятия и затрагивает все функциональные области деятельности предприятия: инновационную, ресурсную, инвестиционную, маркетинговую), их цели должны

корреспондироваться со стратегическими интересами предприятия в рассматриваемой функциональной области деятельности, а показатели, характеризующие цели стратегии, должны соответствовать количественной оценке стратегических интересов предприятия. Установление такого соответствия является очень важным, поскольку именно с его помощью обеспечивается единство методической базы организации управления предприятием.

Создание и функционирование любого предприятия представляет собой процесс инвестирования финансовых ресурсов на долгосрочной основе с целью извлечения прибыли. Процесс управления активами (имущественным потенциалом) также направлен на возрастание прибыли и характеризуется понятием операционно-финансового рычага (производственного и финансового левериджа), для которого характерна взаимосвязь экономических показателей: выручки, расходов производственного и финансового характера и чистой прибыли. Оптимальность этой связи обеспечивает запас финансовой прочности и является фактором экономической безопасности предприятия.

Бизнес-процесс предприятия связан с операционной деятельностью, бухгалтерским учетом, управлением финансами и кадрами, существенная роль в которых принадлежит информационным технологиям (совокупность вычислительных и информационных систем, средств связи, программ и т. п.), позволяющим решить эту задачу оптимальным способом, но требующим материальных и временных затрат на ее внедрение. Таким образом бизнес-процесс предприятия зависит от работоспособности информационной системы, а для потребителя безопасность внедряемых информационных технологий — это проблема, связанная с обеспечением их правильного и бесперебойного функционирования.

Информационная система предприятия, как правило, охватывает все сферы его деятельности: административную, производственную, финансовую, выступает как связующее звено при выработке стратегии бизнеса и качества управления предприятием и персоналом. В ней содержатся сведения, касающиеся планов, состояния материальных и финансовых потоков, договорной деятельности, данные финансового и управленческого учета. Такого рода коммерческая информация носит сугубо конфиденциальный характер, а ее утрата может оказаться критичной для работы всего предприятия, поэтому организация работы пользователей с содержащейся в системе информацией требует специальных мер защиты, обеспечивающих конфиденциальность, целостность и доступность данных.

Помимо самой информации к объектом правовой защиты следует отнести все элементы информационной системы предприятия, которые по своей стоимости и значимости являются нематериальными активами, т. е. долгосрочными активами, не обладающими материальной сущностью (формой) и способные приносить доход.

Информационная безопасность — один из главных приоритетов современного бизнеса, поскольку нарушения в этой сфере приводят к гибельным последствиям для бизнеса любой компании. Применение высоких информационных технологий XXI в., с одной стороны, дает значительные преимущества в деятельности предприятий и организаций, а с другой — потенциально создает предпосылки для утечки, хищения, утраты, искажения, подделки, уничтожения, копирования и блокирования информации и, как следствие, нанесение экономического, социального или других видов ущерба, т. е. проблема информационных рисков и нахождения путей снижения ущерба становится с каждым годом все острее.

Цель информационной безопасности — выявить возможные угрозы безопасности информации, определить их последствия и возможный ущерб, обеспечить необходимые меры и средства защиты, и оценить их эффективность.

Поскольку анализ всей информационной инфраструктуры далеко не всегда оправдан с экономической точки зрения, целесообразно сосредоточиться на наиболее важных, одновременно выявляя не только сами угрозы, вероятность из осуществления, размер потенциального ущерба, но и их источники.

Анализ рисков информационной безопасности

Анализ информационных рисков — это процесс комплексной оценки защищенности информационной системы с переходом к количественным или качественным показателям рисков. При этом риск — это вероятный ущерб, который зависит от защищенности системы. Итак, из определения следует, что на выходе алгоритма анализа риска можно получить либо количественную оценку рисков (риск измеряется в деньгах), либо — качественную (уровни риска; обычно: высокий, средний, низкий).

Оценка рисков производится с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие

риски, переводящие потенциальную угрозу в разряд опасных и потому требующих принятия дополнительных защитных мер. Как правило, для каждой подобной угрозы существует несколько решений по ее нейтрализации. При оценке их стоимости и эффективности следует учитывать не только расходы на закупку оборудования и программных средств, но и такие обстоятельства, как стоимость обучения персонала для работы с ним, совместимость с программным обеспечением и т. д.

На сегодня не существует единой методики количественного расчета величин рисков, измеряемой в стоимостной оценки. Это связано в первую очередь с отсутствием достаточного объема статистических данных о вероятности реализации той или иной угрозы. В настоящее время идет активное накопление данных, на основании которых можно было бы с приемлемой точностью определить вероятность реализации той или иной угрозы. К сожалению, имеющиеся справочники опираются на зарубежный опыт и потому с трудом применимы к российским реалиям. К тому же определение величины стоимости информационного ресурса (будь то физический сервер или файлы и записи СУБД) тоже зачастую затруднено. К примеру, если владелец ресурса (в предположении, что таковой идентифицирован) может назвать стоимость оборудования и носителей, то указать точную стоимость находящихся в его ведении данных он практически не в состоянии.

Поэтому наиболее распространенной остается качественная оценка информационных рисков. Его главная задача — определить факторы риска, установить потенциальные области риска и оценить воздействие каждого вида. Анализ рисков проводится экспертным путем.

В расчетах информационных рисков учитываются следующие факторы:

1. Стоимость ресурса Asset Value, AV). Указанная величина характеризует ценность ресурса. При качественной оценке рисков стоимость ресурса чаще всего ранжируется в диапазоне от 1 до 3, где 1 — минимальная стоимость ресурса, 2 — средняя стоимость ресурса и 3 — максимальная стоимость ресурса. К примеру, сервер автоматизированной банковской системы имеет AV = 3, тогда как отдельный информационный киоск, предназначенный для обслуживания клиента, имеет AV = 1 по отношению к информационной банковской системе;
2. **Мера** уязвимости ресурса к угрозе (Exposure Factor, EF). Этот параметр показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе. Например, с точки зрения банка ресурс автоматизированной банковской системы имеет наиболь-

шую доступность. Таким образом, атаки с целью реализации отказа в обслуживании (Denial of Service, DoS) представляют для него максимальную угрозу. При качественной оценке рисков данная величина также ранжируется в диапазоне от 1 до 3, где 1 — минимальная мера уязвимости (слабое воздействие), 2 — средняя (ресурс подлежит восстановлению), 3 — максимальная (ресурс требует полной замены после реализации угрозы);

3. Оценка вероятности реализации угрозы (Annual Rate of Occurrence, ARO) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая).

На основании полученных данных выводится оценка ожидаемых потерь от конкретной угрозы за определенный период времени (Annual Loss Exposure, ALE), которая характеризует величину риска и рассчитывается по формуле:

$$ALE = ((AV \times EF \times ARO).$$

После проведения первичной оценки рисков полученные значения следует систематизировать по степени важности для выявления низких, средних и высоких уровней рисков. Методика управления рисками подразумевает несколько способов действий. Риск может быть:

- принят (assumption), т. е. пользователь согласен на риск и связанные с ним потери. В этом случае работа информационной системы продолжается в обычном режиме;
- снижен (mitigation) — с целью уменьшения величины риска будут приняты определенные меры;
- передан (transference) — компенсацию потенциального ущерба возложат на страховую компанию, либо риск трансформируют в другой риск — с более низким значением — путем внедрения специальных механизмов.

Некоторые методики дополнительно предусматривают еще один способ управления — «упразднение» (avoidance). Он подразумевает принятие мер по ликвидации источника риска. Например, удаление из системы функций, порождающих риск, либо выведение части системы из эксплуатации. Однако, на мой взгляд, такой подход неконструктивен ввиду того, что, если величина риска достаточно велика, порождающий его компонент критичен для информационной системы и, следовательно, не может быть

удален. При низких значениях риска данный метод трансформируется в метод снижения риска(mitigation).

Далее проводится ранжирование рисков, а затем определяются те, которые требуют первоочередного внимания. Оновным методом управления такими рисками является снижение, реже — передача. Риски среднего ранга могут передаваться или снижаться наравне с высокими рисками. Риски низшего ранга, как правило, принимаются и исключаются из дальнейшего анализа.

Диапазон ранжирования рисков принимается исходя из проведенного расчета их качественных величин. Так, например, если величины рассчитанных рисков лежат в диапазоне от 1 до 18, то низкие риски находятся в диапазоне от 1 до 7, средние — в диапазоне от 8 до 13, высокие — в диапазоне от 14 до 18.

Таким образом, управление рисками сводится к снижению величин высоких и средних рисков до характерных для низких рисков значений, при которых возможно их принятие. Снижение величины риска достигается за счет уменьшения одной или нескольких составляющих (AV, EF, SLE) путем принятия определенных мер. В основном это возможно применительно к EF и SLE, так как AV (стоимость ресурса) — достаточно фиксированный параметр. Однако возможно и его снижение, например, если хранящаяся на сервере информация относится к конфиденциальной, но проверка выявила, что гриф «конфиденциально» в силу каких-либо причин может быть снят. В результате стоимость ресурса автоматически уменьшается. В системе Internet-банкинга, например, параметр EF можно уменьшить путем фиксации ответственности сторон в договорном порядке. В этом случае считается, что стороны предупреждены об ответственности, которую может повлечь за собой нарушение правил эксплуатации системы, и, таким образом, фактор уязвимости снижается.

Снижение параметра SLE, т. е. вероятности реализации угрозы, может быть достигнуто за счет технических мер. Например, при наличии угрозы кратковременного отключения электропитания установка источника бесперебойного питания снижает вероятность ее реализации.

Возникшие (оставшиеся) после применения методики управления риски называются остаточными, и именно они применяются для обоснования инвестиций в информационную безопасность.

Перерасчет рисков производится в отношении всех рисков, если они оценены как высокие и средние.

Пример расчета информационных рисков

Расчет качественных значений информационных рисков проведен на примере сервера Web торговой компании, занимающейся продажей компьютерной техники через собственный Internet-магазин. Предположим, что годовой торговый оборот составляет 100 тыс. долл. США в год. В качестве сервера Web используется ПО Microsoft IIS и СУБД Microsoft SQL Server.

Для упрощения расчета примем две модели нарушителей: внешний легальный пользователь и внешний хакер.

Первого обозначим как A1, а второго — A2.

Для них свойственны следующие черты нарушителя:

- для категории A1
- достаточная квалификация для эксплуатации возможностей Internet-магазина;
- отсутствие цели нанести ущерб компании.
- для категории A2
- необходимые технические познания для эксплуатации возможностей Internet-магазина;
- навыки и опыт использования уязвимостей и недекларированных возможностей ОС, распространенного прикладного ПО;
- опыт взлома подобных систем;
- намерение нанести ущерб компании.

В отношении сервера Web могут быть идентифицированы следующие угрозы:

- нарушение целостности информации, хранящейся в СУБД Internet-магазина;
- нарушение доступности сервера Web;
- нарушение конфиденциальности информации, хранящейся в СУБД Internet-магазина.

Каждая из названных угроз может возникнуть в результате во-первых проведения атак SQL Injection и Cross-Site Scripting; и во-вторых эскалации привилегий злоумышленника в системе в результате переполнения буфера ОС или СУБД.

Атака наподобие SQL Injection может быть намеренно осуществлена злоумышленником категории A2, но не может быть проведена ни при каких обстоятельствах злоумышленником категории A1.

Атака Cross-Site Scripting также может быть предпринята злоумышленником категории A2, но ни в коем случае не злоумышленником категории A1.

Эскалация привилегий прав злоумышленника в системе может произойти в результате намеренных действий злоумышленника категории A2 и ненамеренных действий злоумышленника категории A1.

Создание шторма сетевых пакетов, направленных на сервер Web, может стать следствием намеренных действий злоумышленника категории A2 и ненамеренных действий злоумышленника категории A1 (например, вследствие частого нажатия кнопки «Обновить» обозревателя Internet).

Формирование некорректных пакетов, направленных на сервер Web, влекущих за собой крах службы, может произойти в результате намеренных действий злоумышленника категории A2, но ни при каких обстоятельствах не случится в результате действий злоумышленника категории A1.

Ресурс сервера Web является критичным для функционирования компании, поэтому ему присвоено значение AV = 3. Мере уязвимости ресурса к угрозе нарушения целостности (EF) тоже назначено максимальное значение (3), так как нарушение целостности хранимых в СУБД данных влечет за собой срыв поставок, если, например, удалены данные об оформленных, но еще не проведенных заказах. Вероятность реализации угрозы нарушения целостности оценена как средняя ввиду того, что не исключается эксплуатация широко известных уязвимостей и недостатков программирования (SQL Injection, Cross-Site Scripting). Параметры EF и ARO в отношении угроз нарушения конфиденциальности и доступности рассчитывались аналогично. Большинство параметров (кроме AV), как можно видеть, принимались исходя из экспертного мнения аудитора. Все идентифицированные риски являются высокими, поскольку реализация порождающих эти риски угроз неизбежно нанесет существенный ущерб компании. Таким образом, дальнейшие меры подразумевают снижение идентифицированных рисков.

Для снижения меры уязвимости (EF) в части реализации угрозы нарушения доступности рекомендуется пересмотреть исходный код сценариев Internet-магазина и добавить в него функции фильтрации запросов SQL с целью предотвращения внедрения запросов SQL в запросы HTTP GET. Сходные меры могут быть предприняты в отношении атаки Cross-Site Scripting.

Что касается эскалации привилегий злоумышленника, то на этот случай могут быть приняты такие меры, как установка недавно вышедших обновлений безопасности службы сервера Web, а также постоянный аудит

и периодический пересмотр учетных записей пользователей и прав доступа на системном уровне. В результате этих действий автоматически снижается параметр ARO, установка обновлений безопасности уменьшает вероятность реализации описанных угроз.

Снижение степени уязвимости и вероятности реализации угрозы в части нарушения конфиденциальности достигается аналогично.

Риск нарушения доступности понижается путем установки обновлений безопасности, размещения межсетевого экрана перед сервером Web с учетом топологии сети и ограничения количества одновременных соединений со службой сервера Web с одного IP-адреса.

После идентификации перечисленных мер произведем расчет остаточных рисков. Их величина снизится от 66 до 83 %, что является приемлемым уровнем. Затраты на внедрение описываемых мер составят: доработка сценариев сервера Web 56 человекочасов и финансовых вложений 5000 долл. США, установка межсетевого экрана: трудозатраты в 112 человекочасов и 10 тыс. долл. Таким образом, общие затраты на внедрение предложенных мер — 168 человекочасов и 15 тыс. долл..

Затраты на снижение информационных рисков будут экономически оправданы, если уровень экономической безопасности предприятия позволит сохранить стабильность рентабельности анализируемого предприятия.

Оценим эти затраты с позиции экономической безопасности.

Порядок расчета следующий:

1. По данным бухгалтерской отчетности анализируемого предприятия (форма № 2) как минимум за 2 последних года из того периода, в течение которого на предприятии используются оцениваемые информационные системы, определяется рентабельность за каждый i-й год (Ri) и средняя рентабельность по всем годам (Rcp):

$$R_{i(cp)} = П / ВР,$$

где П — прибыль до выплаты процентов и налогов (стр. 050);
ВР — нетто-выручка от реализации (стр. 010).

2. Вычисляется дисперсия рентабельности предприятия:

$$\sigma^2_R = 1/n \sum_{i=1}^{n} (R_i - R_{cp})^2 ,$$

где $n \geq 2$.

Если информация за 2 года отсутствует, можно использовать поквартальную информацию за истекший год.

3. Вычисляется среднее квадратичное отклонение рентабельности предприятия:

$$\sigma_R = \sqrt{\sigma^2 R_{cp}} ;$$

4. Вычисляется коэффициент вариации рентабельности (Кв) анализируемого предприятия:

$$К_в = \sigma_R / R_{ср};$$

5. По данным ГК РФ по статистике или информационно-аналитических агенств (типа AK&M) определяется рентабельность и коэффициент вариации (Кво) крупнейших по рыночной стоимости компаний (среднеотраслевые показатели):

$$К_{во} = \sigma_{Ro} / R_{оср};$$

6. Подсчитывается допустимый уровень надбавки за риск, обеспечивающий стабильный уровень рентабельности (CDR):

$$CDR = \begin{cases} 2{,}5 \times К_в / К_{во}, & \text{при } К_в : К_{во} \le 2 \\ 5, & \text{при } К_в : К_{во} > 2 \end{cases}$$

В нашем примере (см. выше), где годовой оборот Internet-магазина составляет 100 тыс. долл. и среднегодовой уровень рентабельности 38 %, затраты на информационную безопасность (информационный риск) в размере 15 тыс. долл. хотя и высоки, но вполне оправданы.

Критерии и методы оценки экономической безопасности предприятия

Неотъемлемым элементом исследования экономической безопасности предприятия является выбор ее критерия.

Под критерием экономической безопасности предприятия понимаются признак или сумма признаков, на основании которых может быть сделан вывод о том, находится ли предприятие в экономической безопасности или

нет. Такой критерий должен не просто констатировать наличие экономической безопасности предприятия, но и оценивать ее уровень. При этом количественный уровень экономической безопасности должен оцениваться с помощью тех показателей, которые служат для комплексной оценки эффективности хозяйственной деятельности предприятия и его финансового состояния и которые используются в планировании, учете и анализе деятельности предприятия, что обеспечит ей практическую применимость.

В этой связи целесообразно исследовать подходы и методы, используемые в отечественной и зарубежной практике при диагностике предприятия и прогнозировании вероятности его банкротства.

Диагностика предприятия или ситуационный анализ — первый вид анализа, определяющий ситуации, в которых находится предприятие, т. е. выявляющий обстоятельства, воздействующие на весь ход его производственной, хозяйственной и финансовой деятельности.

Диагностика предприятия складывается из анализа внешней и внутренней среды. В первом случае выявляют и изучают возможности и угрозы, которые могут возникнуть для предприятия в будущем с тем, чтобы правильно представить его стратегию и общую политику управления. Такой анализ предусматривает использование метода SWOT-анализа (S — Strengths — сильные стороны, W — Weaknesses — слабые стороны, O — Opportunities — возможности, T — Threats — угрозы).

Во-втором случае осуществляют комплексный анализ внутренних ресурсов предприятия: организационно-управленческий анализ и финансово-экономический анализ. Цель анализа — выявить стратегическую ситуацию внутри предприятия, характеризующую текущее состояние бизнеса, использование ресурсов и факторы (причины) возможной его несостоятельности.

Банкротство (несостоятельность) предприятия предопределено самой сущностью рыночных отношений, которые сопряжены с неопределенностью достижения конечных результатов и риском потерь. Прогнозирование вероятности банкротства предполагает мониторинг ведущих параметров, создание алгоритма раннего предупреждения негативных процессов управления с точки зрения критериев экономической безопасности.

Система критериев для диагностики предприятия и возможности его банкротства включает в себя финансовые показатели, рассчитанные на основании данных бухгалтерской (финансовой) отчетности предприятия, и которые допускают применение разнообразных методов и приемов. Применяемые в настоящее время методы экономической диагностики можно условно разделить на 3 группы:

- анализ обширной системы критериев и признаков (основные и не основные индикаторы);
- анализ ограниченного круга показателей;
- анализ интегральных показателей.

Рассмотрим каждый из них более детально.

1. **Методы анализа обширной системы критериев и признаков**

При использовании данного метода признаки (показатели) банкротства в соответствии с рекомендациями Комитета по обобщению практики аудирования делят на 2 группы.

Первая группа — основные индикаторы — это показатели, свидетельствующие о возможных финансовых затруднениях и вероятности банкротства в недалеком будущем:

- повторяющиеся существенные потери в основной деятельности, выражающиеся в спаде производства, сокращении объемов продаж и хронической убыточности;
- наличие просроченной дебиторской и кредиторской задолженности;
- низкие значения коэффициентов ликвидности и тенденция к их снижению;
- увеличение до опасных пределов доли заемного капитала в обшей его сумме;
- дефицит собственного оборотного капитала;
- систематическое увеличение продолжительности оборота капитала;
- наличие сверхнормативных запасов, сырья и готовой продукции;
- неблагоприятные изменения в портфеле заказов;
- падение рыночной стоимости акций предприятий;
- снижение производственного потенциала и т. д.

Вторая группа — вспомогательные индикаторы — это показатели, неблагоприятные значения которых не дают основания рассматривать текущее финансовое состояние как критическое, но сигнализируют о возможности резкого его ухудшения в будущем при непринятии действенных мер:

- чрезмерная зависимость предприятия от какого-либо одного конкретного проекта, вида актива, рынка сырья или рынка сбыта;
- потеря ключевых контр агентов;
- недооценка обновления техники и технологии;
- потеря опытных сотрудников аппарата управления;
- вынужденные простои, неритмичная работа;
- недостаточность капитальных вложений и т. д.

К достоинствам системы индикаторов можно отнести возможность системной и комплексной оценки экономической безопасности предприятия для принятия управленческих решений, а к недостаткам — высокую степень сложности оценки количественного уровня экономической безопасности, принятия решений в условиях многокритериальной задачи, информативный характер показателей и субъективность прогнозного решения.

2. **Методы анализа ограниченного круга показателей.**

К таким показателям относятся:

- коэффициент текущей ликвидности — характеризует общую обеспеченность предприятия оборотными активами для ведения хозяйственности и своевременного погашения срочных обязательств предприятия;
- коэффициент обеспеченности собственными средствами — характеризует наличие собственных оборотных средств у предприятия, необходимых для его финансовой устойчивости;
- коэффициент восстановления (утраты) платежеспособности — рассчитывается для проверки реальной возможности (или невозможности), у предприятия восстановить свою платежеспособность при неудовлетворительной структуре баланса.

Оценка экономической безопасности предприятия устанавливается по результатам сравнения (абсолютного или относительного) фактических показателей деятельности предприятия с рекомендованными нормативными значениями. Данный метод является существенно важным для оценки неудовлетворительной структуры баланса, но, поскольку уровень нормативных критериев оценки не учитывает специфику бизнеса (например, структуру капитала в различных отраслях) применение указанного метода может привести к неправильному определению уровня экономической безопасности предприятия и принятию управленческих решений.

3. **Методы анализа интегральных показателей.**

Для оценки экономической безопасности предприятия с точки зрения вероятности банкротства могут использоваться интегральные показатели, рассчитанные по методу мультипликативного дискриминантного анализа.

В зарубежной литературе и практике известно несколько многофакторных прогнозных моделей, например, **пятифакторная модель Альтмана, четырехфакторная Таффлера, Тишоу** и др.

Наибольшую известность получила работа известного западного экономиста Э. Альтмана, разработавшего с помощью аппарата множественного

дискриминантного анализа методику расчета индекса кредитоспособности (Z). Этот индекс позволяет в первом приближении разделить хозяйствующие субъекты на потенциальных банкротов и не банкротов. Указанный индекс представляет собой функцию от показателей, характеризующих экономический потенциал предприятия и результаты его работы за истекший период.

Степень вероятности банкротства на основании индекса Альтмана может быть детализирована в зависимости от его уровня как очень высокая, высокая, средняя и низкая. Разработанная модель прогнозирования банкротства требует адаптации к российским условиям, а критические значения коэффициента Z целесообразно рассчитывать по отраслям и подотраслям с помощью математических методов построения оптимальных критериев.

Для усиления прогнозирующей роли моделей можно трансформировать коэффициент Z в коэффициент PAS (Perfomans Analysys Score) — коэффициент позволяющий отслеживать деятельность компании во времени. Изучая PAS-коэффициент как выше, так и ниже критического уровня, легко определить моменты упадка и возрождения компании.

PAS-коэффициент — это просто относительный уровень деятельности компании, выведенный на основе ее Z-коэффициента за определенный год и выраженный в процентах от 1 до 100. Например, PAS-коэффициент, равный 50, указывает на то, что деятельность компании оценивается удовлетворительно, тогда как PAS-коэффициент, равный 10, свидетельствует о том, что лишь 10 % компаний находятся в худшем положении (неудовлетворительная ситуация). Итак, подсчитав **Z-коэффициент** для компании, можно затем трансформировать абсолютную меру финансового положения в относительную меру финансовой деятельности. Другими словами, если Z-коэффициент может свидетельствовать о том, что компания находится в рискованном положении, то PAS-коэффициент отражает историческую тенденцию и текущую деятельность на перспективу.

Сильной стороной такого подхода является его способность сочетать ключевые характеристики отчета о прибылях и убытках и баланса в единое представительное соотношение. Так, компания, получающая большие прибыли, но слабая с точки зрения баланса, может быть сопоставлена с менее прибыльной, баланс которой уравновешен. Таким образом, рассчитав PAS-коэффициент, можно быстро оценить финансовый риск, связанный с данной компанией, и соответственно варьировать условия сделки. В сущности, подход основан на принципе, что целое более ценно, чем сумма его составляющих.

Дополнительной особенностью этого подхода является использование «рейтинга риска» для дальнейшего выявления скрытого риска. Этот рейтинг

статистически определяется только, если компания имеет отрицательный Z-коэффициент, и вычисляется на основе тренда Z-коэффициента, величина отрицательного Z-коэффициента и числа лет, в продолжение которых компания находилась в рискованном финансовом положении. Используя пятибальную шкалу, в которой 1 указывает на «риск, но незначительную вероятность немедленного бедствия», а 5 означает «абсолютную невозможность сохранения прежнего состояния», менеджер оперирует готовыми средствами для оценки общего баланса рисков, связанных с кредитами клиента.

Учеными Иркутской государственной академии предложена модель прогноза банкротства в которой в качестве механизма предсказания банкротства используется цена предприятия.

Цена предприятия (V) определяется капитализацией прибыли по формуле:

$$V = P / K,$$

где P — ожидаемая прибыль до выплаты налогов, а также процентов по займам и дивидендов;

K — средневзвешенная стоимость пассивов (обязательств) фирмы (средний процент, показывающий проценты и дивиденды, которые необходимо будет выплачивать в соответствии со сложившимися на рынке условиями за заемный ыи акционерный капиталы).

Снижение цены предприятия означает снижение его прибыльности либо увеличение средней стоимости обязательств (требования банков, акционеров и других вкладчиков средств).

Прогноз ожидаемого снижения требует анализа перспектив прибыльности и процентных ставок.

Целесообразно рассчитывать цену предприятия на ближайшую и долгосрочную перспективу. Условия будущего падения цены предприятия обычно формируются в текущей момент и могут быть в определенной степени предугаданы (хотя в экономике всегда остается место для непрогнозируемых скачков).

Кризис управления характеризует **показатель Аргенти (А-счет).**

Согласно данной методике, исследование начинается с предложений, что (а) идет процесс, ведущий к банкротству, (б) процесс этот для своего завершения требует нескольких лет и (в) процесс может быть разделен на три стадии:

Недостатки. Компания, скатывающиеся к банкротству, годами демонстрируют ряд недостатков, очевидных задолго до фактического банкротства.

Ошибки. Вследствие накопления этих недостатков компания может совершить ошибку, ведущую к банкротству (компании, не имеющие недостатков, не совершают ошибок, ведущих к банкротству).

Симптомы. Совершенные компанией ошибки начинают выявлять все известные симптомы приближающейся неплатежеспособности: ухудшение показателей (скрытое при помощи «творческих» расчетов), признаки недостатка денег. Эти симптомы проявляются в последние два или три года процесса, ведущего к банкротству, который часто растягивается на срок от 5 до 10 лет.

При расчете А-счета конкретной компании необходимо ставить либо количество баллов согласно Аргенти, либо 0 — промежуточное значение не допускаются. Каждому фактору каждой стадии присваивают определенное количество баллов и рассчитывают агрегированный показатель — А-счет. (см. табл. 1).

Таблица 1

Метод А-счет для предсказания банкротства

Недостатки	**Ваш балл**	**Балл согласно Аргенти**
Ген. директор		8
Председатель совета директоров является также директором		4
Пассивность совета директоров		2
Внутренние противоречия в совете директоров (из-за различия в знаниях и навыках)		2
Слабый финансовый директор		2
Недостаток профессиональных менеджеров среднего и нижнего звена (вне совета директоров)		1
Недостатки системы учета: Отсутствие бюджетного контроля		3
Отсутствие прогноза денежных потоков		3
Отсутствие системы управленческого учета затрат		3
Вялая реакция на изменения (появление новых продуктов, технологий, рынков, методов организации труда и т. д.)		15
Максимально возможная сумма баллов		43
«Проходной балл»		10

Окончание таблицы 1

Метод А-счет для предсказания банкротства

Недостатки	Ваш балл	Балл согласно Аргенти
Если сумма больше 10, недостатки в управлении могут привести к серьезным ошибкам		
Ошибки		
Слишком высокая доля заемного капитала		15
Недостаток оборотных средств из-за слишком быстрого роста бизнеса		15
Наличие крупного проекта (провал такого проекта подвергает фирму серьезной опасности)		15
Максимально возможная сумма баллов		45
«Проходной балл»		15
Если сумма баллов на этой стадии больше или равна 25, компания подвергается определенному риску		
Симптомы		
Ухудшение финансовых показателей		4
Использование «творческого бухучета»		4
Нефинансовые признаки неблагополучия (ухудшение качества, падение «боевого духа» сотрудников, снижение доли рынка)		4
Окончательные симптомы кризиса (судебные иски, скандалы, отставки)		3
Максимально возможная сумма баллов		12
Максимально возможный А-счет		100
«Проходной балл»		25
Большинство успешных копманий		5–18
Компании, исспытывающие серьезные затруднения		35–75
Если сумма баллов более 25, компания может обанкротиться в течение ближайших пяти лет.		
Чем больше А-счет, тем скорее это может произойти		

Интегральная оценка финансовой устойчивости на основе скорингового анализа

Учитывая многообразие показателей финансовой устойчивости, различие уровня их критических оценок и возникающие в связи с этим сложности в оценке кредитоспособности предприятия и риска его банкротства, многие отечественные и зарубежные экономисты рекомендуют использовать метод диагностики вероятности банкротства **— интегральную оценку финансовой устойчивости на основе скорингового анализа.**

Сущность этой методики — классификация предприятий по степени риска исходя из фактического уровня показателей финансовой устойчивости и рейтинга каждого показателя, выраженного в баллах на основе экспертных оценок.

Рассмотрим простую скоринговую модель с тремя балансовыми показателями (см. табл. 2).

- I класс — предприятия с хорошим запасом финансовой устойчивости, позволяющим быть уверенным в возврате заемных средств;
- II класс — предприятия, демонстрирующие некоторую степень риска по задолженности, но еще не рассматривающиеся как рискованные;
- III класс — проблемные предприятия;
- IV класс — предприятия с высоким риском банкротства даже после принятия мер по финансовому оздоровлению. Кредиторы рискуют потерять свои средства и проценты;
- V класс — предприятия высочайшего риска, практически несостоятельные.

Таблица 2

Группировка предприятий на классы по уровню платежеспособности

Показатель	Границы классов согласно критериям				
	1 класс	2 класс	3 класс	4 класс	5 класс
Рентабельность совокупного капитала,%	30 и выше (50 баллов)	29,9–20 (49,9–35)	19,9–10 (34,0–20 баллов)	9,9–1 (19,9–5)	Менее 1 (0 баллов)
Коэффициент текущей финансовой устойчивости	2,0	1,99–1,7	1,69–1,4	1,39–1,1	1 и ниже

При всех особенностях общим постулатом рассмотренных методов признается тот факт, что критерием экономической безопасности предприятия является прибыльность ее бизнеса. В системе рыночных отношений прибыль (абсолютная и относительная) формируется как экономический результат воздействия внешней среды и эффективности использования внутреннего потенциала.

Литература

1. *Иванов А., Шлыков В.* Экономическая безопасность предприятия. М., 1995. 265 с.
2. *Ковалев Д., Сухорукова Т.* Экономическая безопасность предприятия // Экономика Украины. 1998. № 10. С. 48–51.
3. *Ярочкин В. И.* Безопасность информационных систем. М., 1996. 197 с.
4. *Ярочкин В. И.* Предприниматель и безопасность. М., 1994. 132 с.
5. *Ярочкин В. И.* Система безопасности фирмы. М., 1997. 185 с.
6. *Ярочкин В. И.* Система безопасности фирмы. М., 1997. 185 с.
7. Основы экономической безопасности. (Государство, регион, предприятие, личность) / Под. ред. Е. А. Олейникова. М., 1997. 288 с.
8. *Валуев Б. И., Паламарчук А. И.* Возможность углубления интеграции данных оперативного и бухгалтерского учета в основных центрах угроз экономической безопасности предприятия. Одесса, 2000. С. 218–221.
9. *Шеремет А. Д.* Теория экономического анализа. Учебник. М, Инфра-М, 2005
10. *Савицкая Г. В.* Анализ хозяйственной деятельности предприятия. Учебное пособие. М, Инфра-М, 2005
11. *Ковалев В. В.* Финансовый анализ: методы и процедуры. М, Финансы и статистика, 2001.
12. *Азгальдов Г. Г., Карпова Н. Н.* М, Учеба МИСиС, 2006
13. *Николаева С. А.* Нематериальные активы // Бухгалтерское приложение. 1997. № 5
14. *Василевский И. В.* Найти и обезвредить. Техника защиты информации // Система безопасности. 1995. № 6. С. 11–15.
15. *Забродский В., Капустин Н.* Теоретические основы оценки экономической безопасности отрасли и фирмы // Бизнес-информ. 1999. № 15 16. С. 35–37.
16. *Карпова Т. П.* Управленческий учет: Учебник для вузов. М.:, 2000. 350 с.
17. *Крысин А.* Безопасность предпринимательской деятельности. М., 1996. 256 с.
18. Финансовый менеджмент: Учебно-практическое руководство / Под общ. ред. Е. С. Стояновой. М., 1995. 308 с.
19. *Азоев Г. Л.* Конкуренция: анализ, стратегия, практика. М., 1996. 208 с.
20. Закон Российской Федерации от 23.09.1992 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»
21. Закон РФ от 19.11.1992 г. «О несостоятельности (банкротстве) предприятий».
22. Закон РФ от 25.01.1995 г. «Об информации, информатизации и защите информации».