3.5. Концептуальный базис информационной составляющей экономической безопасности предприятия в хроноэкономике

В современных условиях становления информационного общества вследствие нестабильности внешней среды и возникновения экстремальных условий функционирования, как на отраслевом уровне, так и на уровне конкретного предприятия возникает необходимость выработки способности хозяйствующих субъектов к сопротивлению негативным воздействиям. Такие воздействия представляют угрозу разрушения ресурсного потенциала предприятия, увеличивают риски и потери при осуществлении управленческих решений, и поэтому представляют собой угрозы устойчивому функционированию и безопасному развитию предприятия. Процессы глобализации международных рынков, рост рисков и волатильности валют, процентных ставок, курсов ценных бумаг и цен на сырьевые товары обуславливают актуальность проблемы экономической безопасности. Достоверный прогноз состояния экономической безопасности и ее составляющих, быстрая реакция экономической систем на происходящие события, а также правильный выбор момента времени для реализации того или иного решения могут дать решающие преимущества в конкурентной борьбе и обеспечить устойчивое развитие бизнеса.

Ведение экономически безопасного бизнеса осуществляется в конкурентной среде через набор стратегических и тактических действий, в ходе которых ситуация постоянно меняется и необходимо ежеминутно представлять себе как можно более реалистичную картину как собственной компании, так и внешней среды. Развитие информационных технологий, сетевой экономики и глобальной сети Интернет привело к резкому возрастанию мобильности капиталов и чувствительности мировых финансово-экономических и социальных процессов к информационным воздействиям [1], которые фактически выступают факторами угроз информационной составляющей экономической безопасности. Тесная взаимосвязь информационной составляющей безопасности и общей системой экономической безопасности предприятия выражается через уязвимость к

угрозам информационных атак в финансово-хозяйственной деятельности. На макроуровне виртуализация мировой экономики обусловливают сильную зависимость финансового сектора от информационных и обслуживающих технологий [3]. Деятельность предприятия в информационное пространство и реализация через него бизнес-транзакций, делает его зависимым от качества информационного поля предприятия и «имиджа» в этом пространстве.

Многообразие и сложность хозяйственной деятельности предприятия обуславливают её уязвимость даже к относительно малой угрозе информационной безопасности внешнего и внутреннего характера, что оказывает дальнейшее воздействие на общую систему экономической безопасности предприятия. В связи с этим происходят процессы трансформации систем управления предприятием. Так, корпоративные системы по своим характеристикам быстро приближаются к архитектурам, построенным по принципам архитектуры общей информационной среды поля боя, которая совершенствуется уже в течение нескольких лет [1]. Всё это даёт основание для постановки проблемы получения принципиально нового знания о времени принятия управленческого решения с целью получения наибольшего эффекта от его реализации.

Комплексный анализ к исследованию проблемы экономической безопасности позволяет ее рассматривать как такое состояние системы корпоративных ресурсов, которое обеспечивает мобилизацию, сбалансированность и оптимальное управления и использования ресурсов предприятия (информации и технологии, капитала, персонала, предпринимательских прав и возможностей) с целью обеспечения устойчивого функционирования, динамического всестороннего развития предприятия, активного противодействия различным негативным воздействиям как со стороны внешней, так и внутренней среды. Для информационной составляющей безопасности, как и для экономической безопасности предприятия в целом, характерен ряд особенностей, которые позволяют раскрыть ее сущность (рис. 1).

Основная идея подхода к ведению бизнеса в рамках концепции «предприятия реального времени» (Real-Time Enterprise) состоит в том, что в управлении задействована не одна или несколько корпоративных информационных

систем предприятия, а своеобразная единая «операционная бизнес-система реального времени» [2]. Основными характеристиками таких систем являются - возможность сбора любых необходимых данных в реальном времени и их обработка в максимально короткий срок или в реальном времени, т. е. задержка между фактом регистрации в системе данных о появлении внутреннего или внешнего события и возможностью сформировать ответную реакцию должна быть минимизирована. Это позволяет качественно повысить эффективность разрабатываемых систем управления информационной безопасностью предприятия.

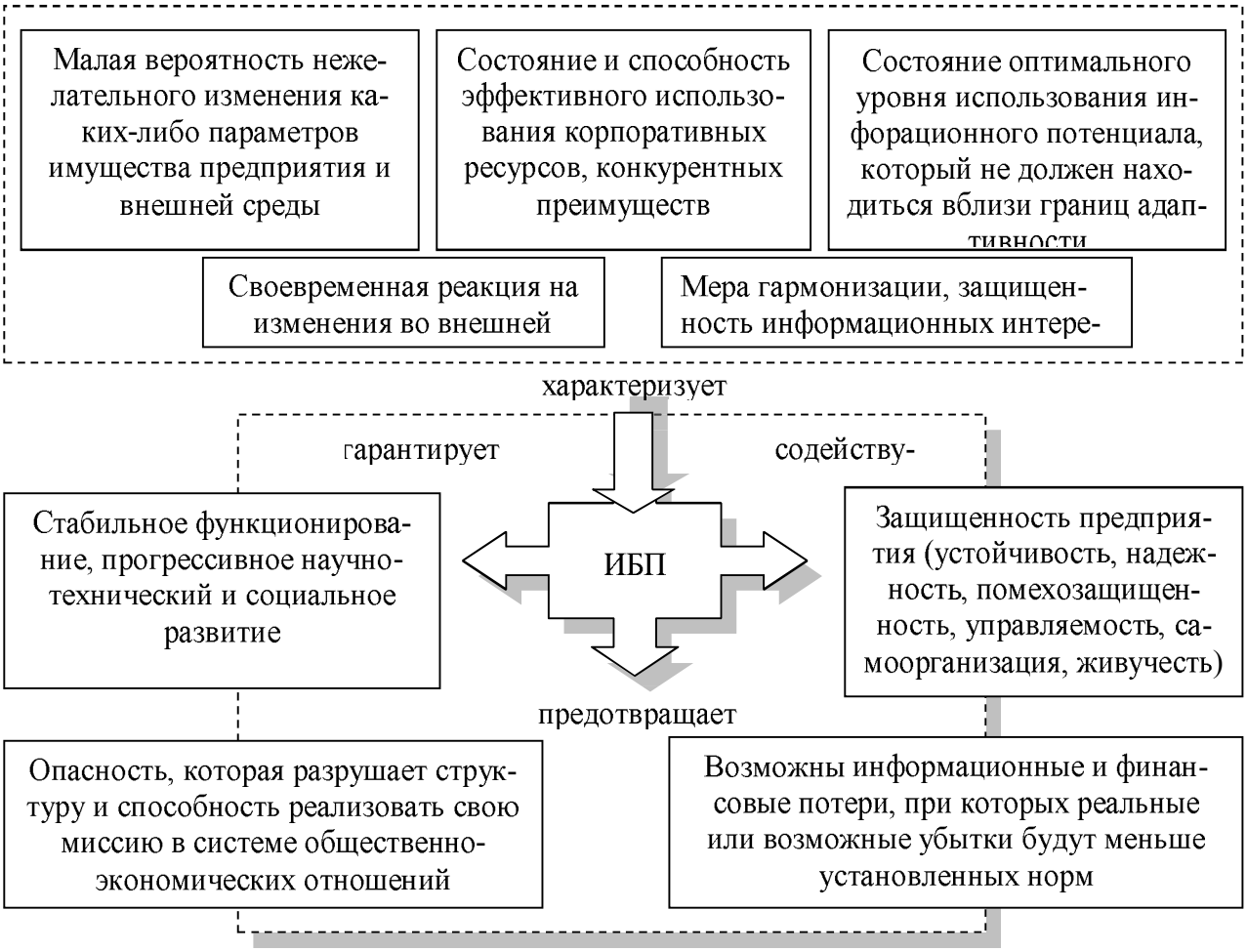

Рис. 1. Характерные особенности информационной безопасности предприятия

Тем не менее, только лишь увеличение производительности и функциональности информационных систем предприятия недостаточно для его управления в соответствии с концепцией RTE. Необходима достоверная и качествен-

ная модель, учитывающая как внутренние, так и внешние факторы. Так как информационные сигналы о событиях в первую очередь влияют на финансовые индикаторы экономической безопасности, которые взаимосвязаны, то последние также можно представить в виде сети финансовых агентов. Общая модель системы экономической безопасности, таким образом, может быть представлена в виде взаимосвязанной системы из трёх сетей: сети ключевых показателей экономической системы (экономических агентов), сети финансовых потоков (финансовых агентов) и сети информационных сигналов (информационных агентов) (рис. 2).

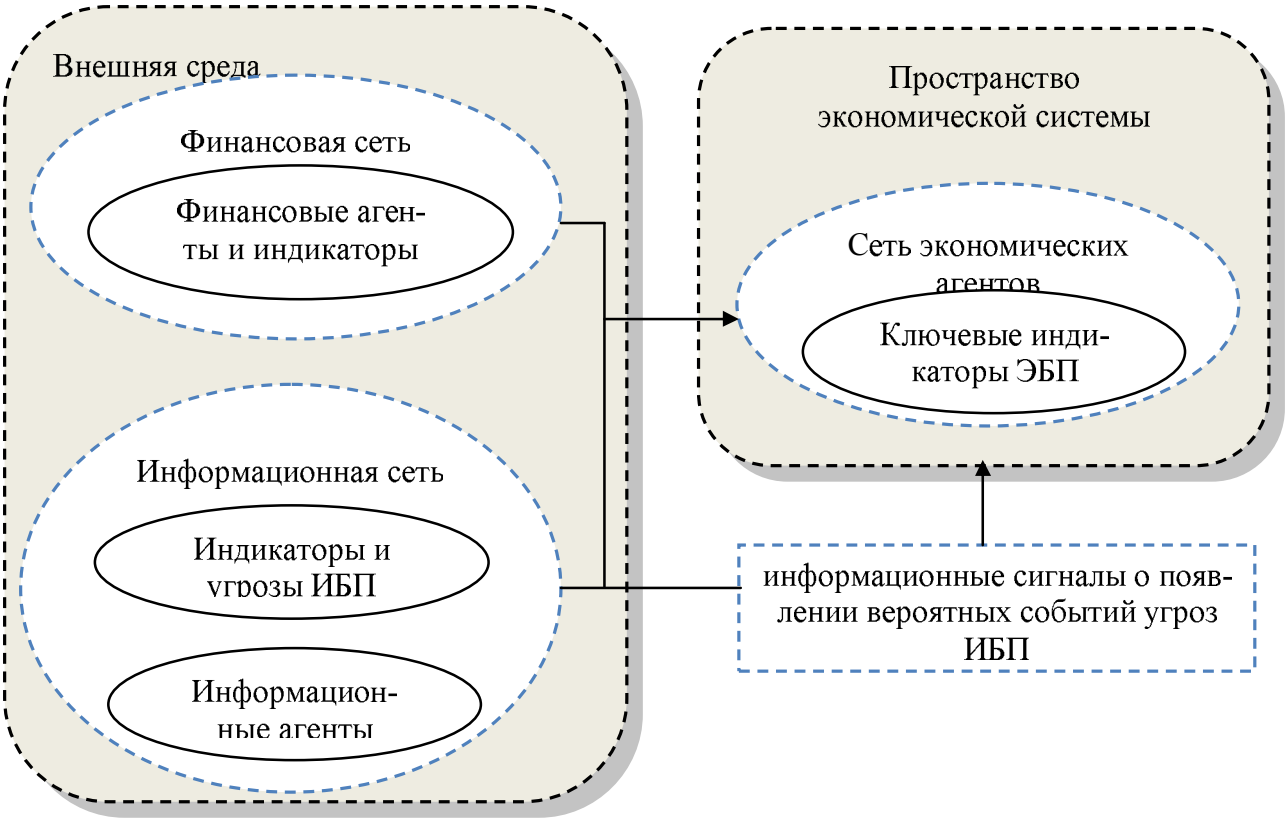

Рис. 2. Схема взаимосвязи информационных, финансовых и экономических агентов в тройственной сети хроноэкономики

Представленная модель характерна для моделей систем хроноэкономики. В отличие от традиционных моделей временного ряда в ней учитывается ряд важнейших положений. Так, для системы информационной безопасности предприятия можно выделить такие концептуальные предпосылки.

1. Ключевые индикативные показатели (КИП) экономической безопасности предприятия рассматриваются как экономические агенты, характеристики которых имеют волновые свойства и подвержены стохастическим изменениям.

2. КИП представляют собой вершины сети, на которые воздействуют внешние информационные и финансовые агенты.

3. Информационные и финансовые сети, в среде которых формируются угрозы ЭБП, обладают волновыми свойствами, а их агенты также подвержены стохастическим изменениям.

На основании этих предположений можно сформировать общую ментальную карты представления системы информационной безопасности (рис. 3).

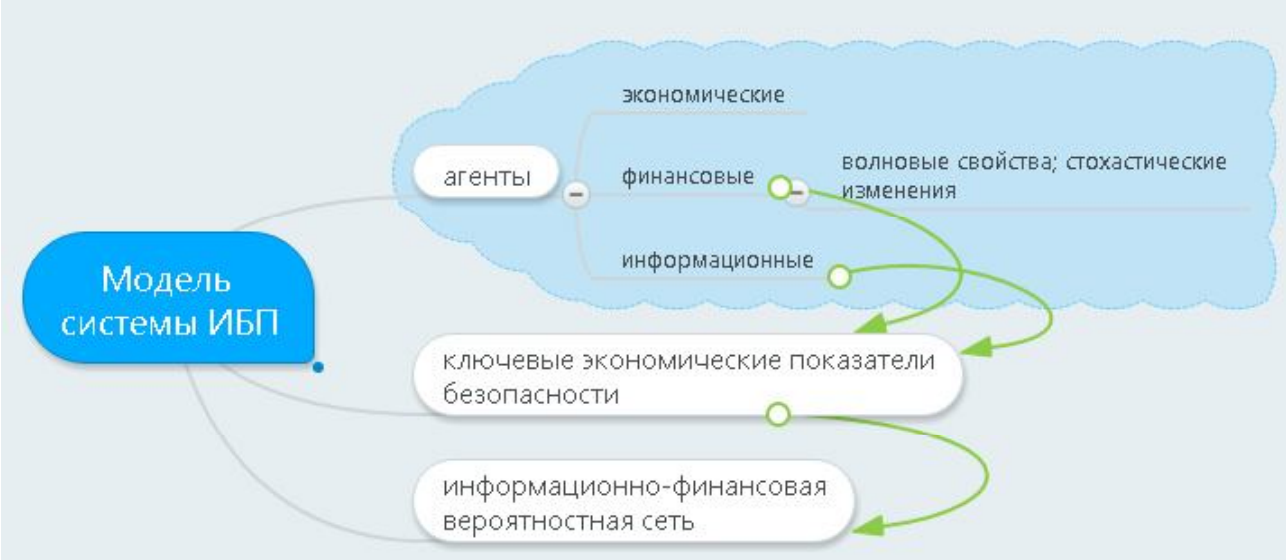

Рис. 3. Ментальная карта модели системы информационной безопасности

Для идентификации информационной угрозы против экономического конкурента особое значение придаётся такому инструменту как резонансное воздействие. Если исходить из фундаментальной гипотезы о волновых свойствах экономических процессов, то и вероятности в виртуальной области событий представляют собой некие «волны вероятности» и событие реализуется, когда эти волны образуют некий резонанс. Явление резонанса получило широкое распространение в среде учёных и специалистов многих областей деятельности, в том числе и экономики, о чём свидетельствует анализ частоты встречаемости слова «резонанс» в поисковых системах сети Internet. Практическое ис-

пользование явления «резонанс» в экономике связано, в первую очередь, с его применением для ослабления или уничтожения конкурента путём резонансного информационного воздействия на его имидж (гудвил) или рейтинг в деловой сфере его партнёров по бизнесу. Резонансная технология воздействия на конкурента может включать в себя [2]:

а) когнитивные схемы,

б) коммуникативные схемы,

в) собственно резонансные схемы.

Использование когнитивной схемы можно представить в виде лавины, когда вброшенный в массовое сознание образ в этом сознании вызывает массу всё увеличивающихся негативных ассоциаций. Мысль, высказанная по поводу конкурента, при определённых условиях начинает существовать в массовом сознании или в сознании его деловых партнёров. Например, присвоение «мусорного» рейтинга предприятию может оказать негативное отношение (ассоциацию) к нему и привести к отказу от сотрудничества с ним.

В кризисные периоды информационные угрозы становятся особенно значимыми, что связано с резким повышением роли информации в это время. Негативные информационные воздействия на конкурента приводят к нарастанию кризисных явлений в его операционной деятельности и в дальнейшем обнаруживаются в неудовлетворительном состоянии его баланса. Основной формой проявления финансового кризиса выступает существенное нарушение финансового равновесия предприятия. Нарушение финансового равновесия предприятия в процессе протекания финансового кризиса характеризуется потерей платежеспособности, снижением финансовой устойчивости и рядом других параметров, обеспечивающих финансовую безопасность предприятия в процессе его развития.

Раннее обнаружение проявления угроз информационной безопасности и последующих кризисных симптомов в финансовой деятельности предприятия является одним из необходимых условий для предотвращения его кризиса. Систему диагностики угроз информационной безопасности предприятия можно представить в виде двух основных подсистем:

1) экспресс-диагностики угроз информационной безопасности;

2) фундаментальной диагностики информационной безопасности.

Подсистема экспресс-диагностики информационной безопасности подразумевает проведение регулярного мониторинга и оценки угроз, осуществляемой на базе данных информационной системы управления предприятием. Основной целью данной диагностики является раннее обнаружение признаков потенциального развития, т.е. угрозы информационных атак на систему предприятия и предварительная оценка масштабов кризисного его состояния. Экспресс-диагностика финансового кризиса осуществляется по следующим основным этапам:

Этап 1. Идентификация объектов наблюдения «кризисного поля», состояние которых может нести угрозу информационной безопасности. В современных экономических условиях присутствуют практически все аспекты хозяйственной деятельности предприятия, которые могут генерировать данную угрозу. Поэтому система наблюдения «кризисного поля» должна строиться с учетом степени генерирования этой угрозы путем выделения наиболее существенных объектов по данному критерию.

Этап 2. Предварительная оценка масштабов кризисного его состояния. На наш взгляд, с учётом возможности действий информационных угроз на систему предприятия, способной в дальнейшем привести к угрозе потери экономической безопасности и банкротства предприятия, вышеприведенный перечень объектов «кризисного поля» должен быть дополнен показателем «уровня информационной угрозы». Гамма «уровня угрозы информационной безопасности может состоять из синего, жёлтого и красного цветов – по нарастающей в зависимости от степени ее вероятности [3]. Каждый из вышеназванных цветов характеризует определенную степень угрозы информационной безопасности и предполагает принятия руководством предприятия экстренных мер информационного и организационного противодействия. При этом заранее должны быть разработаны планы соответствующих мероприятий, как для первого, так и для второго случая:

– повышенный уровень информационной угрозы, когда появляются признаки скрытых попыток негативного воздействия на безопасность предприятия через массовые коммуникационные каналы. При этом аналитики и руководство предприятия предпринимают превентивные меры в соответствии с текущей обстановкой;

– высокий уровень информационной угрозы применяется тогда, когда информация об угрозе нашла свое подтверждение. В этой ситуации предприятие использует свои собственные ресурсы и возможности для его предотвращения в соответствии с ранее разработанными стратегиями;

– очень высокий уровень информационной угрозы, вводится в случаях, когда собственных ресурсов и резервов предприятия не хватает для его предотвращения и необходима внешняя помощь.

В рамках предложенной концепции системы информационной безопасности агенты информационной и финансовой сетей можно рассматривать как взаимосвязанные случайные события. В виртуальной области, в которую мы включаем существенные случайные события, влияющие на ключевые индикативные показатели информационной безопасности, существуют упорядоченные структуры взаимосвязанных событий, и вероятность появления отдельного события можно представить в виде заданного графа Байесовской сети. Формально, байесовская сеть — это направленный ациклический граф, каждой вершине которого соответствует случайная переменная, а дуги графа кодируют отношения условной независимости между этими переменными. Вершинами, в данном случае, выступают индикативные показатели информационной безопасности. Байесовские сети доверия позволяют решать две важные задачи: осуществление диагностики и построение прогноза.

Сложность применения сетей доверия к исследованию реальных экономических процессов заключается в громоздкости вычислений при больших размерах сетей и неточности оценок вероятности появления событий. Данную проблему можно решить, если рассматривать случайные события как бинарные переменные на основе бинарной модели выбора [8]. Модель бинарного выбора,

применяемая в эконометрике, – это модель зависимости бинарной переменной от совокупности факторов. $Y_i = \begin{cases} 0, y_i^* < 0 \\ 1, y_i^* \geq 0 \end{cases}$.

Построение обычной линейной регрессии для таких переменных теоретически некорректно, так как условное математическое ожидание таких переменных равно вероятности того, что зависимая переменная примет значение 1, а линейная регрессия допускает и отрицательные значения и значения выше 1. Поэтому обычно используются некоторые интегральные функции распределения. В логистическом распределении вероятность события определяется функцией

$$Y_i = F(Z_i) = \frac{1}{1+e^{-Z_i}}; \; Z = b_0 + b_1 x_{i1} + \ldots + b_j x_{ij} + \ldots + b_k x_{ik} + e_i,$$

где Y_i – уровень информационной безопасности предприятия;

x_i – индикативные показатели информационной безопасности предприятия;

Z – внутренняя переменная позиционирующая как функция объясняющих переменных.

Таким образом, комбинированный подход к построению модельного базиса оценки информационной составляющей безопасности на основе сетей доверия и бинарных моделей расширяет возможности первого и второго методов и имеет большую объяснительную способность, чем каждый из них в отдельности. В модели экономической безопасности на основе представленной тройственной сети таким фундаментальным свойством происходящих в ней процессов является их колебательный или волновой характер, выраженный в комбинации гармоник, определяемых свойствами элементов этих подсистем. Рассмотренный подход к формированию и построению общей системы информационной составляющей экономической безопасности предприятия позволяет качественно повысить эффективности принятия решений в его управлении, разработках экономически безопасных стратегий функционирования и развития.

ЛИТЕРАТУРА

1. Богомолов А. И. Сетевая модель организационного развития предприятия / А. И. Богомолов, В. П. Невежин // Моделирование организационного развития: сборник докладов круглого стола 10-11 апреля. – 2014. – С. 33-43.
2. Оценка деловой репутации (goodwill) – [Электронный ресурс]. – Режим доступа: http://www.active-consult.ru/ocdelovreputac.htm.
3. Деньщиков А. Экономическая информационная война. – [Электронный ресурс]. – Режим доступа: http://www.u-f.ru/ru/Archive/2007/4/14/Abroad/ID_7374.
4. Горюнова Н. П. Финансовые кризисы на развивающихся рынках / Н. П. Горюнова, П. А. Минакир. – М.: ДВО РАН Институт экономических исследований, Наука, 2006. – 215 с.
5. Константинов Ю. А. Финансовый кризис: причины и преодоление / Ю. А. Константинов, А. И. Ильинский. – М.: ЗАО «Финстатинформ», 1999. – 156 с.
6. Федорова Е. Анализ и оценка каналов распространения финансовых кризисов на развивающихся рынках / Е. Федорова, О. Безрук // Вопросы экономики. – №7. – 2011. – 160 с.
7. Бланк И. А. Основы финансового менеджмента / И. А. Бланк. – К.: Ника-Центр, 1999. – т.1. – 592 с.
8. Управление предприятием в условиях финансового кризиса – [Электронный ресурс]. – Режим доступа: http://www.e-college.ru/xbooks/xbook063/book/index/index.html?go=part-012*page.htm
9. Уровни теругрозы – [Электронный ресурс]. – Режим доступа: http://mosadvokat.org/urovni-terroristicheskoj-ugrozy