

спроса и риска развития; координатного управления – идентификация параметров в точках инвестирования, временных интервалов изменений, уровней экономического состояния потенциала; параметрического управления - идентификация параметров изменений потенциала, координат роста экономического уровня, временного лага инвестирования по жизненному циклу. Проектирование подсистем осуществляется в рамках модели трехмерной матрицы системы управления, а переходы состояний – с использованием цепной модели переходов состояний экономической системы.

Траектория состояний и переходов экономической системы проектируется в направлениях развития с учетом пограничных значений критериев состояний трех видов: предельному уровню, соответствующему бесприбыльному состоянию системы; допустимому уровню - соответствующему прибыльному уровню и недопустимому уровню - соответствующему состоянию кризисного положения.

Описания параметров трех управлений и трех экономических состояний представляется индикативной моделью, которая используется для оптимизации параметров системы, разработки индикативного плана и управления его реализацией. Оптимизация параметров осуществляется методами многокритериальной оптимизации, в результате которой определяется нормативный индикатор состояния системы. Экономические состояния системы моделируются в соответствии с уровнями внешних и внутренних рисков, а их идентификация служит пространством поиска приоритетов управляющих воздействий.

Границы безопасности назначаются в соответствии с заданными пограничными значениями параметров контурного управления и имеют два вида: структурную – определяемую классами предельного состояния системы и динамическую – определяемую во времени тенденцией изменения структуры этих классов в направлении увеличения качества экономического состояния системы.

ВИКТИМОЛОГИЧЕСКАЯ ПРОФИЛАКТИКА КОММЕРЧЕСКОЙ ИНФОРМАЦИИ В МАЛОМ БИЗНЕСЕ

Милевич А.С.

*Кемеровский государственный
сельскохозяйственный институт
Кемерово, Россия*

Любая предпринимательская деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием информации. Потеря определенной информации или ее части может привести предпринимателя к банкротству. Бизнесмен должен отдавать себе отчет в том, что успех в бизнесе зависит во многом от кон-

фиденциальности как внешней, так и внутренней информации. В современном бизнесе для упрощения труда сотрудников основная информация передается в электронном виде с помощью компьютерных технологий. Это, естественно, повышает эффективность и производительность труда, но открывает информацию. Возникает вопрос: «Как и какую информацию следует защищать информацию?»

Ответ - один: «Защите подлежит не вся информация, а только та, которая представляет ценность для предпринимателя, и которая может быть использована конкурентами, злоумышленниками или хакерами во вред предпринимателю».

Информацию, которая используется в предпринимательской деятельности, можно, достаточно условно, разделить на три основных направления:

- предпринимательская,
- правовая,
- специально-оперативная.

Предпринимательская информация

включает сведения о состоянии экономической системы, в которой действует предприниматель, о факторах, которые могут положительно или отрицательно повлиять на сферу его хозяйствования.

Правовая информация - это сведения о действующем законодательстве, о законах и правовых актах, которые регулируют и охраняют деятельность предпринимателей.

Специально-оперативная информация состоит из сведений о способах, силах и средствах обеспечения безопасности предпринимательской информации от доступа третьих лиц.

Утечка информации - одна из главных проблем в работе с информационными потоками как крупной, так и небольшой фирмы. Анализ анкет предпринимателей позволил выявить основные причины утечки информации в практике малого бизнеса:

- отсутствие «защиты», не говоря уже о нескольких степенях;
- пренебрежение конфиденциальностью информации в пользу ее целостности;
- «экономия» средств на обеспечении безотказной работы наиболее важных узлов своей информационной системы;
- «экономия» средств на дополнительной оплате труда по обновлению или замене устаревшего программного обеспечения;
- потеря определенной части клиентуры и т.д.

Следует отметить, что главный враг любой информационной системы в компьютерном варианте - это вирус, который прямо или косвенно ведет к огромным финансовым потерям. Услуги компьютерных фирм, которые занимаются защитой информации, стоят недешево, но предприни-

матель должен нести определенные затраты по защите собственной информации.

Согласно гражданскому законодательству основная масса предпринимательской информации защитой не обладает. Хотя предпринята попытка узаконить предпринимательскую (коммерческую) информацию в качестве защищаемой. (Статья 139 части первой Гражданского кодекса Российской Федерации "Служебная и коммерческая тайна"). В Кодексе определены такие понятия как коммерческая тайна и ответственность за ее разглашение. Это позволяет сделать следующие выводы:

- субъектом оценки предпринимательской коммерческой информации является ее владелец-собственник;
- поступившие сведения и их источник подлежат обязательной перепроверке;
- ценность информации определяется с помощью таких критериев, как полезность, своевременность и достоверность;
- предпринимательская информация в зависимости от ценности имеет свою стоимость;
- информация подлежит защите при условиях: что ее ценность зависит от сохранности в тайне от третьих лиц, доступ к информации закрыт на законном основании, обладатель информации принимает надлежащие меры по ее охране.

Прежде чем принимать меры к защите определенной информации, необходимо уточнить следующие вопросы: Какие сведения нельзя скрывать, защищать? Какие сведения невыгодно скрывать? Какие сведения подлежат охране?

Ответ на первый вопрос дает Постановление Российского Правительства «О перечне сведений, которые не могут составлять коммерческую тайну». К ним относятся:

- организационные сведения (устав и учредительные документы предприятия, регистрационные удостоверения, лицензии, патенты);
- финансовые сведения (документы об исчислении и уплате налогов, других платежей, предусмотренных законом, документы о состоянии платежеспособности);
- сведения о штате и условиях деятельности (число и состав работающих, их заработная плата, наличие свободных мест, влияние производства на природную среду; реализация продукции, причиняющей вред здоровью населения; участие должностных лиц в предпринимательской деятельности, нарушение антимонопольного законодательства);
- сведения о собственности (размерах имущества, денежных средствах, вложениях платежей в ценные бумаги, облигации, займы, в уставные фонды совместных предприятий).

Предпринимателю следует помнить, что данный перечень не является исчерпывающим, а указанные сведения не являются предметом за-

щиты от ознакомления с ними третьих лиц. Информация такого рода относится к первой группе.

Вторая группа сведений характеризуется тем, что ее невыгодно скрывать от окружения самому предпринимателю. Это касается, в первую очередь, рекламной информации. Но следует помнить, что широкое распространение рекламы имеет не только положительную, но и отрицательную сторону для предпринимателя, если она становится достоянием преступных элементов.

К третьей группе сведений относятся те, которые представляют хозяйственную ценность для предпринимателя, и на них не распространяется законный доступ третьих лиц. Проблема состоит в том, кто и как должен обеспечить сохранность такого рода информации. Ни один из законодательных актов не ставит под свою защиту данный вид собственности.

Любая фирма при организации охраны информации должна определить круг сведений, составляющих коммерческую тайну. Они отражаются в «Перечне сведений, составляющих коммерческую тайну предприятия» и утверждаются руководителем предприятия. Практика показывает, что данный вопрос лучше решать коллегиально. Для разработки Перечня приказом руководителя предприятия создается комиссия из наиболее квалифицированных и компетентных специалистов. Если предприятие имеет небольшой штат, то вопрос о коммерческой тайне решает сам руководитель или приглашает эксперта.

В деловой информации коммерческую тайну могут иметь:

- сведения о заключенных или планируемых контрактах,
- данные о поставщиках и клиентах,
- обзоры рынка, маркетинговые исследования,
- информация о конфиденциальных переговорах,
- планы развития предприятия и его инвестиций,
- калькуляция издержек производства предприятия, структуры цен, уровень прибыли.

Следует отметить, что в отличие от крупных фирм, малый бизнес не располагает достаточными финансовыми и организационными возможностями, чтобы самостоятельно оградить свое дело от внутренних и особенно внешних дестабилизирующих факторов, обеспечить полную защиту своей коммерческой информации от недобросовестных сотрудников, хакеров, нечестных конкурентов и неправомерных действий представителей органов исполнительной власти.

При определении ценности предпринимательской информации, по мнению теоретиков и самих бизнесменов, необходимо руководствоваться такими критериями, как полезность, своевременность, достоверность и полнота поступивших сведений.

Определение стоимости тех или иных сведений требует дифференцированного подхода:

- в одних случаях, дешевле обойдутся собственные ошибки как накопление опыта выживания в мире бизнеса;
- в других - целесообразнее получить (купить) информацию о том, как избежать подобных ошибок;
- в-третьих - необходим анализ, как сохранить ценную информацию от доступа посторонних лиц, чтобы не потерять ее стоимость и ожидаемую от нее прибыль.

Необходимо подчеркнуть, что факт утечки информации напрямую связан с падением ее ценности для владельца. В производственной компании коммерческую тайну для информации технологического характера могут составлять:

- конструкторская документация, чертежи, схемы, записи;
- описания и анализ технологических испытаний производимой продукции;
- «ноу-хау», авторские права и патенты;
- точные данные конструктивных характеристик создаваемых изделий и оптимальные параметры разрабатываемых технологических процессов;
- сведения о материалах, из которых изготовлены отдельные детали, условиях и результатах экспериментов и апробирования оборудования, на котором они проводились и т. д.;
- применяемые на предприятии отдельные новые, либо уникальные измерительные комплексы и приборы, станки, оборудование.

Данная информация реально должна быть защищена специальными мерами как внешними, так и внутренними. Внешние - это изучение и сбор информации о надежности, платежеспособности партнеров, клиентов, поставщиков, с которыми приходится вести хозяйственную, коммерческую деятельность. В ходе осуществления внутренних мероприятий по обеспечению безопасности решается, прежде всего, вопрос об оптимальном подборе кадров. Практика показывает, что претенденты на вакантную должность должны обязательно пройти определенную проверку. В ходе анализа собранных материалов выясняется, нет ли каких-либо в них противоречий. После этого делается вывод о пригодности кандидата к работе в данной фирме.

Анализ практики показывает, что бизнесменам необходимо знание основных проблем по охране информации, умение их предвидеть и решать на этапе возникновения, что поможет предпринимателям сохранить и развить свой бизнес. Для защиты предпринимательских информационных потоков от различного рода посягательств используются как правовые, так и специальные меры, а в необходимых случаях комплексное их применение. Предприниматель должен помнить, что сведения, представляющие для него интерес,

а также источник их поступления должны подвергаться перепроверке.

СПИСОК ЛИТЕРАТУРЫ:

1. Аппенянский А.И. Человек и бизнес. Путь к совершенству. Повышение психологической надежности. - М.: Барс, 1995. - 228с.
2. Гражданский Кодекс Российской Федерации. Ч.1 (действует с 1 января 1995 года). - М.:ИНФРА-М, 1995.
3. Смольков Г.В., Левитан М.И. Предпринимательство и риск: опыт и проблемы // Социально-политический журнал. -1993. -№7. - С. 101-108.
4. Федорова Е. Продолжайте беспокоиться. Ваша внутренняя «спецслужба» полезна, но не давайте ей много власти. //Компания. - 1998. - № 9. - 1 сентября. - С. 57.

СТРАТЕГИЧЕСКИЕ НАПРАВЛЕНИЯ ЛОКАЛИЗАЦИИ НИЗКОГО УРОВНЯ ЖИЗНИ В РОССИЙСКИХ РЕГИОНАХ

Михалкина Е.В.

*Южный федеральный университет
Ростов-на-Дону, Россия*

Повсеместное воспроизводство низкого уровня жизни населения губительно с точки зрения его социально-экономических последствий. Низкий уровень жизни ведет к ухудшению здоровья нации, росту смертности, преступности, снижению рождаемости, изменению типологии семей (растет процент неполных, бездетных семей, семей, имеющих в своем составе инвалидов и др.), повышению процента экономически неактивного населения, деформации социальной психологии, угрозам социальной стабильности и другим деструктивным общественным процессам. Учеными признано, что бедность – это не просто недостаточность средств существования, а сформировавшийся образ жизни, способен к самогенерации в расширенном масштабе, охватывая все большую часть трудоспособного населения. В этих условиях в системе устойчивого социально-экономического развития регионов особое значение должно отводиться реализации стратегических направлений локализации бедности, учитывающей не только социально-демографические особенности ее распространения, но и территориальные, и социально-экономические детерминанты воспроизводства человеческого потенциала. В настоящее время, в условиях преобладанием рентоориентированных интересов олигархических групп над интересами выживания основной части населения, происходит высвобождение движущих сил бедности. Таким образом, проблема бедности давно переросла индустриальные рамки отдельного государства и вышла на уровень проблемы глобальной социальной организации, то есть причины