Тема 7. Экономическая безопасность государства

Вопросы к изучению:

7.1. Система обеспечения экономической безопасности предприятия

7.2. Методы анализа и оценки уровня экономической безопасности предприятия

7. 3. Основные типы рисков и угроз экономической безопасности предприятия

7.4. Кадровая безопасность предприятия

7.5. Информационная безопасность предприятия

7.1. Система обеспечения экономической безопасности предприятия

Экономическая безопасность предприятия – это состояние наиболее эффективного использования ресурсов для предотвращения угроз и обеспечения его стабильного функционирования. Очевидно, что экономическая безопасность предприятия базируется на том, насколько эффективно службам данного предприятия удается предотвращать угрозы и устранять ущербы от негативных воздействий на различные аспекты экономической безопасности. Источниками таких негативных воздействий могут являться осознанные или неосознанные действия людей, организаций, в том числе органов государственной власти, международных организаций или прсдприятий-конкурснтов, а также стечение объективных обстоятельств, как-то: состояние финансовой конъюнктуры на рынках данного предприятия, научные открытия и технологические разработки, форсмажорные обстоятельства и т.д.

В зависимости от субъективной обусловленности негативных воздействий на экономическую безопасность предприятия может применяться следующая их классификация:

1) объективные негативные воздействия – такие негативные воздействия, которые возникают без участия и помимо воли предприятия или его служащих;

2) субъективные негативные воздействия – негативные воздействия, возникшие как следствие неэффективной работы предприятия в целом или его работников.

При оценке экономической безопасности предпринимательства необходимо также учитывать риски конкретной предпринимательской деятельности.

В известной степени риском можно управлять, т.е. использовать различные меры, позволяющие в определенной степени прогнозировать наступление рискового события, и принимать меры к снижению степени риска. При этом каждому риску соответствует своя система приемов управления риском. Эффективность организации управления риском во многом определяется классификацией риска.

Экономическая безопасность предприятия характеризуется совокупностью качественных и количественных показателей, важнейшим среди которых является уровень экономической безопасности. Уровень экономической безопасности предприятия – это оценка состояния использования корпоративных ресурсов по критериям уровня экономической безопасности предприятия. С целью достижения наиболее высокого уровня экономической безопасности предприятие должно следить за обеспечением максимальной безопасности основных функциональных составляющих системы экономической безопасности предприятия.

Функциональные составляющие экономической безопасности предприятия – это совокупность основных направлений его экономической безопасности, существенно отличающихся друг от друга по своему содержанию.

Примерная структура функциональных составляющих экономической безопасности предприятия:

- финансовая;
- интеллектуальная и кадровая;
- технико-технологическая;
- политико-правовая;
- экологическая;
- информационная;
- силовая.

Каждая из вышеперечисленных функциональных составляющих экономической безопасности предприятия

характеризуется собственным содержанием, набором функциональных критериев и способами обеспечения.

Для обеспечения экономической безопасности предприятие использует совокупность своих корпоративных ресурсов.

Корпоративные ресурсы – факторы бизнеса, используемые владельцами и менеджерами предприятия для выполнения целей бизнеса.

Среди них выделим:

а) ресурс капитала. Акционерный капитал предприятия в сочетании с заемными финансовыми ресурсами является кровеносной системой предприятия и позволяет приобретать и поддерживать остальные корпоративные ресурсы, изначально отсутствующие у создателей данного предприятия;

б) ресурс персонала. Менеджеры предприятия, штат инженерного персонала, производственных рабочих и служащих с их знаниями, опытом и навыками являются

основным проводящим и связующим звеном, соединяющим воедино все факторы данного бизнеса, обеспечивающим проведение в жизнь идеологии бизнеса, а также достижение целей бизнеса;

в) ресурс информации и технологии. Информация, касающаяся всех сторон деятельности предприятия, является в настоящее время наиболее ценным и дорогостоящим из ресурсов предприятия. Именно информация об изменении политической, социальной, экономической и экологической ситуации, рынков предприятия, научно-техническая и технологическая информация, конкретные ноу-хау, касающиеся каких-либо аспектов данного бизнеса, новое в методах организации и управления бизнесом позволяют предприятию адекватно реагировать на любые изменения внешней среды бизнеса, эффективно планировать и осуществлять свою хозяйственную деятельность;

г) ресурс техники и оборудования. На основе имеющихся финансовых, информационно-технологических и кадровых возможностей предприятие приобретает технологическое и другое оборудование, необходимое, по мнению менеджеров предприятия, и доступное исходя из имеющихся ресурсов;

д) ресурс прав. С развитием цивилизации, истощением природных ресурсов и повышением ценности для бизнеса нематериальных активов резко выросла роль ресурса прав. Этот ресурс включает в себя права на использование патентов, лицензии и квоты на использование природных ресурсов, а также экспортные квоты, права на пользование землей. Причем в настоящее время крайне повысилась ценность городских территорий, не предназначенных для земледелия, а используемых под административную застройку. Использование этого ресурса позволяет предприятию приобщиться к передовым технологическим разработкам, не проводя собственных дорогостоящих научных исследований, а также получить доступ к необщедоступным возможностям развития бизнеса.

Основной причиной необходимости обеспечения экономической безопасности предприятия является стоящая перед каждым предприятием задача достижения стабильности своего функционирования и создания перспектив роста для выполнения целей данного бизнеса.

Под целями бизнеса следует понимать систему побудительных мотивов, заставляющих людей начинать

новое дело. К таким побудительным мотивам относятся:

• сохранение и приумножение капитала акционеров предприятия из расчета превышения процентной депозитной ставки банков;

• самореализация через данный бизнес сто инициаторов и высшего менеджмента предприятия;

• удовлетворение различных потребностей людей и общества в целом. Данный мотив особенно часто является доминирующим в деятельности государственных или муниципальных предприятий.

Формируясь на основе видения инициаторами бизнеса его целей, философия бизнеса представляет собой систему ценностей и норм поведения, принятых на данном предприятии, а также место и роль предприятия в системе бизнеса и в обществе в целом.

Главной целью экономической безопасности предприятия является обеспечение его устойчивого и максимально эффективного функционирования в настоящее время и обеспечение высокого потенциала развития и роста предприятия в будущем. Наиболее эффективное использование корпоративных ресурсов предприятия, необходимое для выполнения целей данного бизнеса, достигается путем предотвращения угроз негативных воздействий на экономическую безопасность предприятия и достижения следующих основных функциональных целей экономической безопасности предприятия:

• обеспечение высокой финансовой эффективности работы предприятия и его финансовой устойчивости и независимости;

• обеспечение технологической независимости предприятия и достижение высокой конкурентоспособности его технологического потенциала;

• достижение высокой эффективности менеджмента предприятия, оптимальности и эффективности его организационной структуры;

• обеспечение высокого уровня квалификации персонала предприятия, использование его интеллектуального потенциала, эффективности корпоративных НИОКР;

• достижение высокого уровня экологичности работы предприятия, минимизации разрушительного влияния результатов производственной деятельности на состояние окружающей среды;

• обеспечение качественной правовой защищенности всех аспектов деятельности предприятия;

• обеспечение защиты информационной среды предприятия, коммерческой тайны и достижение высокого уровня информационного обеспечения работы всех его служб;

• обеспечение безопасности персонала предприятия, его капитала, имущества и коммерческих интересов.

Выполнение каждой из вышеперечисленных целей экономической безопасности предприятия является существенно важным для достижения ее главной цели. Кроме того,

каждая из целей экономической безопасности имеет собственную структуру подцелей, обусловливаемую функциональной целесообразностью и характером работы предприятия.

Подробная разработка и контроль за выполнением целевой структуры экономической безопасности предприятия являются весьма важной составной частью процесса обеспечения его экономической безопасности.

Обеспечение экономической безопасности предприятия – это процесс реализации функциональных составляющих экономической безопасности с целью предотвращения возможных ущербов и достижения максимального уровня экономической безопасности предприятия в настоящий момент времени и в будущем.

Способы обеспечения экономической безопасности предприятия – это набор мер и система организации их выполнения и контроля, которые позволяют достигать наиболее высоких значений уровня экономической безопасности предприятия.

Важнейшим этапом обеспечения экономической безопасности предприятия является стратегическое планирование и прогнозирование его экономической безопасности. Этот этап включает в себя разработку стратегического плана обеспечения экономической безопасности предприятия. В этом документе необходимо задать качественные параметры использования корпоративных ресурсов предприятия в сочетании с его организационно-функциональной структурой и взаимосвязями структурных подразделений, а также некоторые количественные ориентиры обеспечения функциональных составляющих и экономической безопасности предприятия в целом.

На основе разработанного стратегического плана необходимо выработать общие и функциональные рекомендации по реализации плановых установок, которые, если это представляется возможным, должны содержать определенные количественные характеристики и оформляться специальными приложениями к стратегическому плану обеспечения экономической безопасности предприятия.

После разработки стратегического плана обеспечения экономической безопасности предприятия и выработки рекомендаций по его реализации в соответствии с данными документами осуществляется стратегическое планирование финансово-хозяйственной деятельности. Создаются стратегические финансовые, производственные планы, осуществляется планирование персонала, поставок и др.

После разработки стратегических планов деятельности предприятия необходимо провести оперативную оценку уровня обеспечения и текущее тактическое планирование экономической безопасности предприятия. Анализ уровня экономической безопасности предприятия проводится на основе оценки эффективности мер по предотвращению

ущербов и расчета функциональных и совокупного критериев экономической безопасности предприятия.

Текущее планирование экономической безопасности предприятия осуществляется на основе разработки нескольких альтернативных сценариев развития ситуации и расчета значений совокупного критерия экономической безопасности по каждому из них. После выбора по результатам расчетов лучшего варианта и анализа остальных вырабатываются оперативные рекомендации по текущему планированию деятельности предприятия. Эти рекомендации не носят в отличие от стратегических долгосрочного характера и задают не только качественные ориентиры текущей деятельности предприятия, но и содержат количественные задания.

На основе оперативной оценки уровня экономической безопасности предприятия и выработанных рекомендаций осуществляется оперативное планирование финансово-хозяйственной деятельности предприятия, после чего производится практическая реализация разработанных планов.

В процессе осуществления предприятием своей финансово-хозяйственной деятельности появляется информация для анализа состояния его экономической безопасности. На основе этой информации осуществляется оценка функциональных и совокупного критериев экономической безопасности этого предприятия, их отклонений от плановых значений, анализируются причины возникновения этих отклонений. После этого вырабатываются рекомендации по корректировке набора корпоративных ресурсов, систем стратегического и текущего планирования финансово-хозяйственной деятельности предприятия, а также системы оперативного управления его деятельностью.

Корректировки могут вноситься и в систему планирования экономической безопасности предприятия. В этом случае нужно заново использовать описанные выше методы планирования экономической безопасности предприятия и вносить соответствующие изменения в хозяйственные планы предприятия и систему их реализации.

7.2. Методы анализа и оценки уровня экономической безопасности предприятия

Для оценки динамики реализации и анализа устойчивости предприятия рассчитаем следующие показатели:

1) абсолютное отклонение объемов реализации по годам в сопоставимых ценах (цепное)

$$\Delta y_i = y_i - y_{i-1},$$

где ***y***i – объем реализации;

2) темп роста объемов реализации по годам (цепное)

$$\text{Тр} = \frac{y_i}{y_{i-1}} 100;$$

3) темп прироста объемов реализации по годам (цепное)

$$\text{Тпр} = \frac{y_i - y_{i-1}}{y_{i-1}} 100.$$

Оценка уровня экономической безопасности предприятия по всем функциональным составляющим на основе статистических методов обработки информации сильно затруднена, так как большинство аспектов данной проблемы крайне сложно поддается математической формализации, а некоторые из них не поддаются вовсе.

Важность проблемы оценки уровня экономической безопасности предприятия для эффективного функционирования последнего очень велика, поэтому предлагается оценивать уровень экономической безопасности предприятия на основе определения совокупного критерия экономической безопасности, рассчитываемого на основе мнений квалифицированных экспертов по частным функциональным критериям экономической безопасности предприятия.

Частный функциональный критерий представляет собой оценку уровня экономической безопасности предприятия по одной из ее составляющих: финансовой, интеллектуальной и кадровой, информационной и т.д. Данные критерии рассчитываются на основе оценки ущербов экономической безопасности предприятия но каждой составляющей и эффективности мер по их предотвращению.

Формула расчета совокупного критерия экономической безопасности предприятия (СКЭБ):

$$\text{СКЭБ} = \sum_{i=1}^{n} K_i d_i,$$

где ***K***i –значения частных функциональных критериев экономической безопасности предприятия; ***d***i – удельные веса значимости функциональных составляющих экономической безопасности предприятия. Причем, $\sum d_i = 1$; ***n*** –количество частных функциональных критериев.

Удельные веса частных функциональных критериев экономической безопасности предприятия в совокупном критерии экономической безопасности предприятия рассчитываются на основе оценки совокупных ущербов по функциональным составляющим его экономической безопасности, которая подробнее рассматривается ниже.

Из приведенного здесь метода расчета совокупного критерия экономической безопасности предприятия видно, что в расчете этого критерия содержится значительная доля субъективного фактора – мнений экспертов, проводящих оценку уровня экономической безопасности предприятия. Субъективизм предлагаемого метода

проявляется как в оценке ущербов при определении частных функциональных критериев экономической безопасности предприятия, так и в процессе распределения удельных весов функциональных составляющих при расчете совокупного критерия экономической безопасности предприятия. Однако именно отсутствие строгого "прокрустова ложа" четко заданных параметров оценки и позволяет наиболее эффективно настроить данный гибкий инструмент всесторонней оценки деятельности предприятия и окружающей его среды бизнеса на специфику конкретной организации.

Например:

– финансовая – 0,3;

– интеллектуально-кадровая – 0,1;

– технико-технологическая – 0,15;

– политико-правовая – 0,1;

– информационная – 0,2;

– экологическая – 0,05;

– силовая – 0,1.

Разумеется, приведенные примерные варианты распределения удельных весов функциональных составляющих экономической безопасности предприятия могут и должны подвергаться критическому осмыслению и корректировке при практическом расчете критерия экономической безопасности исходя из специфики конкретного анализируемого предприятия.

Конкретные виды рисков:

– падение цены и спроса на продукцию. Этот риск снижается за счет хорошо продуманной ценовой политики и поддержания более низких, чем у конкурентов, цен;

– невыплата денег покупателем. Снижается за счет юридически грамотных договоров, заключенных с покупателем, и внимательного изучения возможностей каждого клиента;

– дорожно-транспортные происшествия при доставке товара. Снижается за счет профессионализма водителя и вывоза крупных партий самим покупателем.

Опенка риска может проводиться двумя методами:

– методом экспертных оценок рисков;

– оценкой функциональных составляющих экономической безопасности.

Для оценки влияния каждой из составляющих необходимо определить частный функциональный критерий. Частный функциональный критерий экономической безопасности предприятия по предлагаемой методике необходимо рассчитывать как отношение совокупного предотвращенного ущерба по данной составляющей экономической безопасности предприятия к сумме затрат на реализацию мер по

предотвращению ущербов от негативных воздействий и общего понесенного ущерба по составляющей. Данному расчету частного функционального критерия экономической безопасности предприятия соответствует следующая формула:

$$ЧФК = \frac{У_{пр}}{З + У_{по}},$$

где ЧФК – частный функциональный критерий уровня обеспечения функциональной составляющей экономической безопасности предприятия; Упр – совокупный предотвращенный ущерб по составляющей; З – суммарные затраты в анализируемом периоде на реализацию мер по предотвращению ущербов по данной функциональной составляющей экономической безопасности предприятия; Упо – общий понесенный ущерб по данной функциональной составляющей экономической безопасности предприятия.

Несомненно, задача достоверной оценки всех возможных понесенных и предотвращенных ущербов по каждой из реализуемых мер является крайне сложной, однако именно такая методика соотношения различных аспектов экономической безопасности предприятия по однородному критерию оценки ущербов, к тому же измеряемому в тех же стоимостных единицах, что и затраты на реализацию принимаемых мер, является наиболее адекватной при расчете получаемого эффекта от мер по обеспечению функциональных составляющих экономической безопасности предприятия.

7. 3. Основные типы рисков и угроз экономической безопасности предприятия

После многократного анализа финансового и технологического потенциала российских предприятий различных отраслей было получено примерное соотношение значимостей функциональных составляющих экономической безопасности, основываясь на следующих положениях.

1. В обеспечении экономической безопасности и эффективного функционирования торговых предприятий и предприятий, работающих на финансовых рынках, включая банки, предприятий, работающих на фондовых рынках, осуществляющих страховую и инвестиционную деятельность, важную роль играет информационное обеспечение бизнеса, а также фактор финансовой деятельности. Для обеспечения экономической безопасности предприятий, работающих на финансовых рынках, весьма важную роль играет уровень персонала. При этом как для предприятий, работающих на финансовых и фондовых рынках, так и для торговых предприятий более высока по сравнению с промышленными и сельскохозяйственными предприятиями роль силовой составляющей экономической безопасности при существенно меньшей значимости для них влияния экологических проблем.

2. Для промышленных и сельскохозяйственных предприятий примерно одинаково важна роль финансового обеспечения их производственной деятельности. В то же время для промышленных предприятий существенно выше по сравнению с сельскохозяйственными роль интеллектуальной и кадровой составляющей, а также системы информационного обеспечения производства (особенно важна новейшая технологическая информация и информация о движении рынков предприятия). При этом для сельхозпроизводителей экологическая составляющая гораздо более значима по сравнению с промышленными предприятиями. Это вызвано тем, что для сельскохозяйственных предприятий земля является основным фактором производства и экологическая обстановка существенно влияет на результаты сельскохозяйственного бизнеса, в то время как промышленных предприятий экологические проблемы касаются только через системы штрафных санкций за загрязнение окружающей среды и нарушение экологических стандартов на выпускаемую продукцию.

Риском в хозяйственной деятельности называется возможность финансовых потерь (снижение прибыли, доходов, потеря капитала и т.д.) при неопределенных условиях инвестиционной деятельности. Риск возникает вследствие неопределенности внешней и внутренней среды.

Избежать риска в хозяйственной деятельности невозможно, но можно и даже необходимо уметь им управлять, стараясь предотвращать негативные последствия.

Рассмотрим основные методы борьбы с риском.

Метод уклонения от риска. Им пользуются предприниматели, предпочитающие действовать не рискуя. Суть данного метода состоит в выборе консервативной стратегии. Принятие решения о выборе такой стратегии принимается, как правило, на этапе разработки проекта.

Метод компенсации риска. Это упреждающий метод. В отличие от предыдущего он не предполагает избежания риска, а подразумевает создание и активное использование различного инструментария борьбы с рисками и их негативными последствиями. Это использование в деятельности предприятия системы прогнозирования и стратегического планирования, проведение активного маркетинга, создание резервных фондов.

Метод диверсификации риска. Данный метод предполагает распределение рисков по срокам, структуре, источникам возникновения и пр. При финансовом инвестировании речь идет о диверсификации портфеля, когда инвестиционный капитал распределяется между ценными бумагами с различными рисками, доходностями и корреляциями с целью минимизации несистематического риска.

При диверсификации рисков предпринимательской деятельности (реальное инвестирование) к этой группе методов управления риском относятся различные варианты диверсификации:

• ***диверсификация деятельности,*** понимаемая как увеличение числа используемых или готовых к использованию технологий, расширение ассортимента выпускаемой продукции или спектра предоставляемых услуг, ориентация на различные социальные группы потребителей и т.п.;

• ***диверсификация рынка сбыта,*** т.е. работа одновременно на нескольких товарных или региональных рынках;

• ***диверсификация закупок сырья и материалов*** предполагает взаимодействие со многими поставщиками, что позволяет снизить зависимость предприятия от ненадежности отдельных поставщиков сырья, материалов и комплектующих.

Метод страхования риска. Данный метод в отличие от предыдущих предполагает не использование инструментов управления рисками, а возмещение полного или частичного ущерба вследствие наступления рисковой ситуации (страхового случая).

Перечисленные методы могут и должны использоваться комплексно.

На рис. представлена обобщенная схема предпринимательских рисков по природе их возникновения (риски здесь поделены на внешние и внутренние с точки зрения подхода к управлению рисками).

Рис. **Предпринимательские риски**

7.4. Кадровая безопасность предприятия

Место кадровой безопасности в системе экономической безопасности и управления персоналом

Исследования специалистов показывают, что самое сложное звено в системе безопасности – это человек, и именно человеческий фактор может оказать критическое влияние на успешность деятельности и само существование компании.

Именно поэтому кадровая безопасность занимает в структуре экономической безопасности ведущее место. Кадровую безопасность можно определить как процесс предотвращения потенциальных и реальных угроз (рисков), связанных с персоналом (использованием трудового потенциала, развитием человеческого капитала, управлением человеческими ресурсами, совершенствованием трудовых отношений и т.д.).

В этом случае речь может идти, с одной стороны, о неосознанной угрозе со стороны персонала (например, некомпетентности, халатности, случайной ошибке), а с другой – об осознанных действиях, связанных с воровством, мошенничеством, саботажем, взяточничеством, разглашением коммерческой тайны и другими противоправными действиями сотрудников.

Изучением и управлением кадровыми рисками (кадровой безопасностью) занимается служба управления персоналом (служба управления человеческими ресурсами, ***HR***-менеджеры), которая является субъектом кадровой безопасности. Ее основная цель – выявление, анализ, предотвращение и прогнозирование потенциальных угроз со стороны сотрудников организации, способных нарушить устойчивость, развитие и привести к остановке ее деятельности.

Важнейшим элементом кадровой безопасности следует считать комплектование самой службы управления персоналом грамотными, высококвалифицированными специалистами, которые компетентны в решении всего комплекса вопросов ***HR***-менеджмента. В противном случае возможны ситуации риска в результате ошибок в подборе персонала, найме и увольнении, в планировании, оценке, развитии, мотивации и стимулировании персонала.

С позиции службы управления персоналом каждый кандидат на вакансию в организации, так же как и каждый работник предприятия, должен постоянно рассматриваться как источник кадрового риска и потенциальной угрозы. В настоящее время к рискам, возникающим в подсистеме управления персоналом организации, относят следующие угрозы со стороны сотрудников:

– прямое хищение имущества предприятия;

– использование ресурсов предприятия в собственных целях;

– умышленная порча и уничтожение имущества предприятия;

– получение заработной платы за невыполняемую работу;

– шантаж компетентностью (незаменимый работник, ключевая фигура в компании);

– шантаж полномочиями (это возможно, если они сосредотачиваются в одних руках);

– торговля сведениями, составляющими коммерческую тайну;

– нарушения трудовой дисциплины;

– создание в коллективе неблагоприятного моральнопсихологического климата.

При этом под **кадровой угрозой** понимается негативное воздействие кадровой функциональной составляющей на экономическую безопасность предприятия.

Выделяют два вида угроз:

– внешние, которые не зависят от воли и сознания работников организации;

– внутренние, определяемые действиями (умышленными или нет) сотрудников компании.

Выделяют следующие основные источники угроз из ***внешней среды:***

– коррумпированные представители органов власти (проведение проверок или оперативных мероприятий в инициативном порядке или по заказу конкурентов с целью закрытия предприятия или вымогательства взяток);

– предприятия-конкуренты, осуществляющие различного рода акции (в том числе прямые угрозы, шантаж, экономический шпионаж и т.п.);

– криминальные структуры (прямое давление на предприятие и его партнеров, организация нападений на предприятие и его собственность и т.п.);

– предприятия-поставщики (изменение ценовой политики и изменение условий поставки ресурсов, сырья и комплектующих);

– предприятия-потребители (отказ от закупок продукции, требования об изменении цен и условий поставки и т.п.);

– специалисты по информационным технологиям, не являющиеся сотрудниками предприятия, несанкционированно проникающие в систему информационных ресурсов;

– финансово-кредитные учреждения (неожиданный отказ в кредите или задержка проводки платежей).

Источниками ***внутренних угроз*** могут быть сотрудники компании. При этом можно выделить следующие три уровня:

– первые руководители и топ-менеджеры (прямое мошенничество, фальсификация отчетности, хищение имущества, получение откатов, предоставление или продажа конкурентам информации, являющейся коммерческой тайной предприятия);

– менеджеры, сотрудники-специалисты основных и вспомогательных производств (прямое воровство финансовых, информационных средств и продукции, нецелевое

использование техники, оборудования, информационно-вычислительных средств и пр., продажа сведений, составляющих коммерческую тайну предприятия, и др.);

– рабочие (воровство готовой продукции, сырья, комплектующих, финансовых средств, нецелевое использование транспортных средств и специальной техники и оборудования, умышленный вывод из строя техники

Проблемы контроля кадровых рисков

В настоящее время более 80% функционирующих организаций не относятся к государственному сектору, поэтому жесткая регламентация основой их деятельности не является, а все вопросы управления персоналом находятся в ведении владельцев, учредителей, акционеров, что способствует росту рисковых ситуаций.

Одно из наиболее распространенных определений риска – возможная опасность (вероятность) получения потерь. Риск обусловлен отклонениями действительных данных оценки настоящего состояния и прогнозов будущего развития политических, климатических, экономических, социальных и прочих ситуаций.

В последние годы акцент сделан на риски, которым подвержены компании, и как результат – на методы управления рисками. Особое внимание при этом уделяется так называемым социальным рискам, большинство из которых связано с персоналом компании. Социальные риски предпринимательской деятельности в зависимости от субъекта риска подразделяются:

– на ***социальные риски предпринимателя*** (риски подбора неквалифицированного персонала, несоблюдения трудовой дисциплины, забастовок, стихийного увольнения, текучести кадров и т.д.);

– ***социальные риски наемного работника*** (риски нарушения трудовых прав наемных работников со стороны предпринимателя и недостойного вознаграждения за труд, нарушения условий труда и деятельности по охране труда, угрозы здоровью на рабочем месте; несоблюдения любых прав человека, имеющих отношение к деятельности организации, и т.д.);

– ***социальные риски предпринимательства с позиции общества*** (риски нарушения экологической безопасности производства, неэкономного потребления природных ресурсов, отсутствия системы по утилизации отходов и т.д.);

– ***социальные риски предпринимательства в регионе*** (несоблюдение этических норм ведения бизнеса, нарушение взаимодействия с местным сообществом и властью; риск неподдержания гражданских инициатив, благотворительных программ социального и культурного развития населения).

Отсюда особо актуальными становятся вопросы управления рисками, в частности использования риск-менеджмента, в том числе в области управления персоналом.

Действие организаций в условиях изменяющейся бизнес-среды предполагает, что компании для повышения конкурентоспособности стремятся повысить результативность деятельности организации, а это, в свою очередь, ведет к принятию дополнительных рисков. Поэтому возникает объективная необходимость обеспечить персонал организации четкими процедурами по принятию и выполнению решений, учитывающих влияние риска на результаты деятельности.

Необходимость управления кадровыми рисками (кадровой безопасностью) ставит на повестку дня вопрос разработки концепции кадровой безопасности организации, которая должна быть направлена на построение многоуровневой системы барьеров на пути опасности (потенциальных и реальных рисков) со стороны персонала компании.

Управление кадровыми рисками предполагает ***контроль персонала*** в случаях набора персонала, в условиях трудовой деятельности и при увольнении сотрудников.

Важнейшим элементом концепции кадровой безопасности является ***система набора персонала,*** поскольку первые риски возникают на этапе найма сотрудников. В этой области специалисты выделяют следующие направления: неправильный выбор источника подбора кандидатов (сферы деятельности, должности); неправильно сформулированная задача при обращении к рекрутерам; неточная оценка кандидатов на этапе отбора: низкий профессионально-квалификационный уровень кандидата, уровень его компетентности, социально-психологическая несовместимость с уже сложившимся коллективом и имеющейся организационной культурой компании, низкая мотивация кандидата работать именно в данной компании, несоответствие целей компании и личных целей будущего сотрудника.

Сотрудники службы управления персоналом при найме должны ориентироваться на бизнес-стратегию компании, на совпадение целей и ценностей сотрудников с целями и ценностями организации (управление по целям и управление по ценностям), учитывать при приеме группы риска. Согласно исследованиям специалистов в эти группы риска входят люди, которые попали под влияние какой-либо из зависимостей, в результате чего становятся неблагонадежными и демонстрируют противоправное деструктивное поведение. Попадание в зависимость обычно связывают с желанием человека уйти из реальной жизни путем изменения своего сознания или переключения его в виртуальный мир. Зависимости бывают:

1) фармакологические (химические) – алкоголизм, наркомания, табакокурение, токсикомания;

2) субстанциональные – компьютерные, игорные, эмоциональные (любовь и секс), трудоголизм, религиозные секты;

3) пищевые.

Определение подобных групп риска должно осуществляться еще на этапе отбора персонала, в том числе через использование ряда тестовых методик. Анализ результатов тестов службой управления персоналом и службой безопасности позволяет определить некоторые психологические особенности претендента. Так, существуют специальные методики тестирования, которые помогают определить морально-этические качества кандидата, его слабости, устойчивость психики, возможные преступные наклонности, умение хранить секреты и пр. Наиболее популярными и используемыми из них являются опросники Г. Айзенка и Р. Кеттела; Миннесотский многопрофильный личностный опросник (***MMPI***), тематический апперцептивный тест (ТАТ).

По мнению Г. Айзенка, совокупность описывающих человека черт можно представить посредством двух главных

факторов: экстраверсии (интроверсии) и невротизма, которые представляют собой характеристику индивидуально-психологического склада человека. Принято считать, что экстравертам свойственны общительность, импульсивность, гибкость поведения, широкий круг знакомств, большая инициативность (но малая настойчивость) и высокая социальная адаптация. Интровертам же, наоборот, присущи необщительность, замкнутость, это спокойные, застенчивые люди, которым свойственна социальная пассивность (при достаточно большой настойчивости), склонность к самоанализу и затруднения при социальной адаптации. Выявление этих характеристик позволяет отнести человека к одному из четырех типов темперамента, что бывает значимо при приеме на работу.

Психодиагностический тест 16-PFP. Кеттела может быть использован для многостороннего и углубленного изучения личности человека, его характера, темперамента, интеллекта, эмоциональных, волевых, моральных, коммуникативных и других особенностей, что предполагает его применение в областях профориентации, отбора и расстановки кадров, научных исследований и т.д.

Миннесотский многопрофильный личностный опросник (***MMPI)*** – один из самых широко распространенных опросников, основанных на самооценке и для оценки личности. ***MMPI*** стал чрезвычайно значимым в исследованиях социальных и личностных проблем. В настоящее время имеется более 200 отдельных шкал, которые были разработаны на основе оригинального набора пунктов ***MMPI,*** измеряющих такие черты и

качества, как тревога, сила "я" ***(ego),*** маскулинность/фемининность и интернальность/экстернальность.

Следует отметить, что в рядовых ситуациях сравнительно массового психодиагностического обследования применение тематических апперцептивных тестов, как правило, не оправдывает затраченных усилий. Специалисты рекомендуют его применять в случаях, вызывающих сомнения, требующих тонкой дифференциальной диагностики, а также в ситуациях максимальной ответственности, например при отборе космонавтов, пилотов, кандидатов на руководящие посты и т.п.

При применении тестов могут возникнуть проблемы юридического характера. Так, существующая в США Единая комиссия по занятности и суды, регулирующие эти вопросы, постоянно указывают, что выбор тестов должен быть структурирован таким образом, чтобы соответствовал положенным процедурам по отбору и не наносил ущерба

Контроль персонала в процессе трудовой деятельности

Подобный контроль представляет собой комплекс мер из установленных для персонала всех уровней регламентов, ограничений, режимов, оценочных операций и процедур безопасности. Этот комплекс воздействия на персонал имеет целью ликвидацию возможности причинения ущерба со стороны работников. Как правило, такой контроль осуществляется службой безопасности или другими подразделениями, в меньшей степени службой управления персоналом.

Основными направлениями контроля персонала в процессе трудовой деятельности с позиции безопасности являются:

– контроль результатов деятельности (достижений);

– контроль использования рабочего времени;

– информационный контроль.

Контроль результатов деятельности (***достижений***) ***и использования рабочего времени сотрудника*** важен в плане повышения качества управления организационной эффективностью и снижения риска недоиспользования трудового потенциала личности. Значимый элемент управления достижениями работника – грамотно построенная система мотивации и стимулирования, основанная на результате, который необходимо постоянно контролировать. Если необходимый результат не достигается, важно выявить причины подобной ситуации. Возможно, работник недостаточно компетентен, поэтому следует направить его на обучение или повышение квалификации. Может быть, следует изменить систему мотивации, принятую в компании. Еще одна причина – нереально определенные показатели деятельности ***(KPI)*** для конкретного сотрудника, а возможно, он сам

неэффективно использует свое рабочее время. Поэтому так важен контроль не только самого результата, но и процесса достижения этого результата.

Для контроля процесса трудовой деятельности используются следующие традиционно используемые в нормировании труда методы. В частности, фотография рабочего дня, представляющая собой способ непрерывного наблюдения за рабочим процессом на предприятии для изучения использования всего рабочего времени, а также измерения затрат времени на протяжении каждой смены. Целью данного наблюдения является повышение производительности труда. В ряде случаев полезно использовать метод самофотографии рабочего дня, когда работник самостоятельно фиксирует только потери рабочего времени по вине организации.

Фотография рабочего дня необходима при решении некоторых задач:

– определение темпов производства продукции в течение одной производственной смены;

– определение баланса использования времени, затраченного на работу;

– определение возможных причин потерь рабочего времени;

– определение времени, предоставленного для отдыха, времени для обслуживания рабочего места, а также времени для заключительных работ.

Актуальным является и метод нормирования труда на основе микроэлементных нормативов, предусматривающих дробное расчленение трудовых действий на простейшие, заранее пронормированные стандартные движения (рук, глаз, корпуса и ног), с помощью которых появляется возможность моделирования рациональных ручных приемов и расчета норм времени, необходимых для их выполнения. Системы микроэлементных нормативов позволяют в условиях применения компьютерных технологий одновременно с автоматизированным проектированием технологического процесса производить расчет норм времени, определять еще до начала производства необходимые затраты труда, сравнивать их с предельно допустимыми, изыскивать возможности снижения затрат труда.

Одна из современных особенностей контроля персонала в процессе трудовой деятельности и обеспечения кадровой безопасности связана с формированием системы слежения за сотрудниками. Специалисты отмечают, что, скорее всего, подобная система имеет корни в США, где в основе корпоративной культуры лежит понятие "эффективность". Поэтому, чтобы добиться ее повышения, в организации идут на любые меры, в том числе на изучение деловой и личной переписки, прослушивание телефонных разговоров, наблюдение за посещением интернет-сайтов.

Служба безопасности может отслеживать и оперативно ставить в известность ***HR***-менеджеров о ***негативных явлениях*** в организации со стороны сотрудников. В частности, речь может идти:

– о намеренном разжигании конфликтных ситуаций со стороны некоторых работников;

– нарушениях требований корпоративной политики использования информационных ресурсов;

– нелояльном поведении отдельных работников – рассылке резюме, назначении встреч с новыми работодателями, незаконной передаче за пределы компании информации ограниченного доступа;

– негативном поведении отдельных сотрудников, выражающемся в грубости, оскорблениях, моббинге по отношению к другим работникам.

Сегодняшний день предоставляет работодателям современные электронные системы учета и регистрации рабочего времени, которые позволяют практически определить затраты рабочего времени непосредственно на работу, на отдых, потери рабочего времени по вине работника и но вине организации. Это осуществляется через системы контроля доступа, видеонаблюдение (может носить скрытый и открытый характер) и т.д.

В настоящее время использование DAP-систем становится обычной практикой большинства корпоративных служб безопасности. Основная задача подобных систем на современном этапе – сбор и протоколирование всей информации о деятельности сотрудника в автоматизированной системе предприятия, а также обработка этой информации для выявления инсайдерства, мошенничества и других подозрительных действий.

Специалисты отмечают, что согласно статистике сегодня около трети крупных российских компаний внедряю

внедряют использование систем "контроля" за деятельностью своих работников. В связи с этим возникает вопрос о законности и оправданности подобного контроля. В трудовом договоре между работодателем и работником обычно записано, что все созданное сотрудником компании принадлежит компании. Если сотрудник в рабочее время (оплачиваемое фирмой) занимается личными делами, то этим он наносит урон работодателю, а если пользуется Интернетом в своих целях, то еще и крадет деньги. Поэтому в любой серьезной компании, в которой не принято доверять сотрудникам, есть юрист, который любой, даже чрезмерный, контроль объяснит заботой о подчиненных. К сожалению, контроль может перейти в тотальную слежку. Поэтому единственным пунктом, который может использовать сотрудник при защите своих прав, является обязанность компании при найме работников сообщать о том, что все их коммуникации в

рабочее время не являются конфиденциальными, а работники обязаны подписать соответствующий документ, подтверждающий их согласие с корпоративными правилами. Такая система предполагает, что, с одной стороны, работодатель имеет право внедрять всевозможные системы контроля за деятельностью своих сотрудников, а с другой – обязан осуществлять контроль открыто, что может стать важным элементом концепции обеспечения кадровой безопасности компании.

Информационный контроль персонала связан с угрозами информационной безопасности, которая охватывает совокупность программных, аппаратных и организационно-правовых методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий.

Анализ основных угроз информационной безопасности России показывает, что на первом месте стоит утечка данных – 76%, на втором – халатность сотрудников – 67%, на третьем – вирусы – 59%. Специалисты считают, что в первую очередь необходимо защищаться от непредумышленных утечек информации: в 90% случаев они происходят в результате ошибок персонала или банальной кражи носителей данных, т.е. речь идет о внутренних угрозах. При этом типичный инсайдер – это обычно мужчина в возрасте от 31 до 40 лет, имеющий высшее образование и обладающий достаточно весомым положением в компании.

Контроль персонала при увольнении

В ТК РФ четко прописана процедура выхода сотрудника из компании. Однако, если сама процедура была некорректной, компания может понести значительный моральный и материальный ущерб. Моральный ущерб может быть нанесен через антирекламу организации, а материальный – в случае обращения уволенного сотрудника в суд. Юридическая практика показывает, что лучше не доводить трудовые споры до суда, так как финансовые издержки в любом случае лягут на работодателя.

В процессе расторжения трудовых отношений с работником могут возникать деструктивные конфликты. Здесь речь может идти как о преднамеренном увольнении сотрудника по сто собственному желанию – с целью причинения ущерба компании, так и об увольнении по инициативе руководства. Однако обе эти ситуации создают предпосылки к возникновению деструктивных конфликтов в организации. Подобную ситуацию гораздо легче предупредить специалистам службы безопасности и службы управления персоналом, чем потом тратить время и ресурсы на поиск позитивных решений, которые для компании не всегда будут приемлемыми.

Значительные проблемы могут возникнуть в организации, когда при увольнении (уходе в отпуск) сотрудник не передал информацию, а тот, кто его заменяет, или вновь принятый на эту должность работник не имеет опыта работы в этом направлении. В этом случае негативные последствия могут коснуться не только какого-либо подразделения компании, но всей организации в целом (потеря клиентской базы и т.д.).

Особый контроль должен осуществляться при увольнении персонала, имеющего отношение к информации компании. Значительный урон организации может быть нанесен, если уволенный или уволившийся сотрудник забирает с собой максимум информации через клиентскую базу и налаженные контакты. При этом, если увольнение работника произошло за разглашение коммерческой тайны, это относится к разновидности мер дисциплинарной ответственности, основанием которой служит дисциплинарное правонарушение, т.е. противоправное, виновное поведение субъекта (работника), предусмотренное нормами ТК РФ.

В любом случае с такими работниками следует расставаться максимально по-дружески, поскольку вполне возможен вариант перехода сотрудника в конкурентную компанию с передачей инсайдерской информации.

Для того чтобы снизить подобные риски, можно использовать следующие меры:

– подписание при приеме на работу соглашения о невозможности работы на прямого конкурента при увольнении на протяжении определенного периода времени;

– подписание договора о неразглашении коммерческой информации с четким определением границ коммерческой тайны и суммами ответственности за ее разглашение (в случае нарушения договора компенсация может быть взыскана и в судебном порядке);

– перед этапом высвобождения работника из компании осуществить его перевод на работу без доступа к информации, носящей коммерческую тайну;

– изучение причин увольнения и его отношения к компании (последнее в случае отрицательного отношения к организации может привести к распространению негативного имиджа).

В любом случае увольнение сотрудника должно сопровождаться четким объяснением причин увольнения, подкрепленным примерами-фактами либо плохой работы сотрудника, либо наличием проблем в компании.

В настоящее время в крупных корпорациях служба безопасности формируется как отдел, в котором работают профессионалы. В малых компаниях обеспечение безопасности часто становится дополнительной функцией юридического и *HR*-отделов. Практика показывает, что достаточно часто современные компании различных масштабов приглашают для обеспечения безопасности внешние специализированные агентства. В

любом случае необходимо комплектование службы управления персоналом высококвалифицированными специалистами, компетентными в решении всего комплекса вопросов управления персоналом, способными исключить ситуации риска в процессе работы с персоналом.

7.5. Информационная безопасность предприятия

Основные положения и вводные понятия

В современных условиях перед предприятиями и организациями остро встает задача сохранения как материальных ценностей, так и информации, в том числе сведений, составляющих коммерческую или государственную тайну.

Успех производственной и предпринимательской деятельности в немалой степени зависит от умения распоряжаться таким ценнейшим товаром, как информация, но выгодно использовать можно лишь ту информацию, которая требуется рынку, но неизвестна ему. Поэтому в условиях ужесточения конкуренции успех предпринимательства, гарантия получения прибыли все в большей мере зависят от сохранения в тайне секретов производства, опирающихся на определенный интеллектуальный потенциал и конкретную технологию.

Предпринимательская (коммерческая) деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Однако защите подлежит не вся информация, а только та, которая представляет ценность для предпринимателя. При определении ценности предпринимательской информации необходимо руководствоваться такими критериями (свойствами), как полезность, своевременность и достоверность поступивших сведений.

Разработку мероприятий по сохранению коммерческой тайны предприятия следует осуществлять, соблюдая принцип комплексного перекрытия возможных каналов утечки информации и обеспечения равнозначной надежности защиты всех ее носителей. Угрозы сохранности коммерческой тайны могут быть внешними и внутренними.

Действия извне могут быть направлены на пассивные носители информации и выражаться, например, в следующем: попытки похищения документов или снятия копий с документов, съемных носителей (флеш-карты), снятие информации, возникающей в тракте передачи в процессе коммуникаций; уничтожение информации или повреждение ее носителей; случайное или преднамеренное доведение до сведения конкурентов документов или материалов, содержащих коммерческую тайну.

Действия извне могут быть также направлены на персонал компании и выражаться в форме подкупа, угроз, шантажа, выведывания информации, составляющей коммерческую

тайну, или предполагать переманивание ведущих специалистов на конкурирующую фирму и т.п.

Внутренние угрозы представляют наибольшую опасность для вновь сформированных и не устоявшихся коллективов, где не успели сложиться традиции поддержания высокой репутации предприятия, однако внимание своевременному вскрытию этих угроз должно уделяться повсеместно. Не исключена вероятность того, что отдельные сотрудники с высоким уровнем самооценки из-за неудовлетворенности своих амбиций (недовольство уровнем заработной платы, отношениями с руководством, коллегами и пр.) могут предпринимать меры по инициативной выдаче коммерческой информации конкурентам, а также попытаться уничтожить важную информацию или пассивные носители (например, внести компьютерный вирус). По оценкам психологов, до 25% всех служащих фирм, стремясь заработать денежные средства любыми способами и любой ценой, зачастую в ущерб интересам своей фирмы ожидают удобного случая для разглашения коммерческих секретов, их продажи.

Весьма принципиальным представляется также отражение вопросов защиты коммерческой тайны в контракте, заключаемом с руководителем предприятия при его назначении на должность.

Угрозы и основные направления обеспечения информационной безопасности предприятия

При оценке угроз безопасности информации и выборе приоритетов в системе защиты предприятия проанализируем практику защиты информации и обеспечения безопасности деятельности различных организаций – государственных и коммерческих банков, крупных фирм, промышленных предприятий, а также существующий международный опыт в решении данной проблемы.

Классификация угроз безопасности информации. Основным объектом воздействия угроз безопасности является информация, обрабатываемая в автоматизированных системах учреждения (АС). Базисом АС являются: общесистемное программное обеспечение (ПО), программные оболочки, программы общего назначения, текстовые процессоры, редакторы и интегрированные пакеты программ. Особое место в общесистемном ПО занимают системы управления базами данных.

Информация в АС может поступать с автоматизированного рабочего места (далее – АРМ) локальной сети по внутренним и по внешним каналам связи, при этом информация может вводиться как с клавиатуры, так и с внешних носителей информации. Кроме того, АС может использовать информационные ресурсы других учреждений и организаций и ресурсы глобальных телекоммуникационных сетей.

К пользователям АС относятся все зарегистрированные в ней лица (организации), наделенные определенными полномочиями доступа. В рамках своих полномочий пользователь может осуществлять только разрешенные ему действия с использованием общесистемного и прикладного ПО.

Процесс обработки информации в АС осуществляется под контролем администраторов системы, а ее защиты – администраторов безопасности.

Источники угроз безопасности информации предприятия можно разделить на три группы: антропогенные, техногенные и стихийные.

В группу ***антропогенных источников*** угроз безопасности информации входят:

• криминальные структуры, рецидивисты и потенциальные преступники;

• недобросовестные партнеры и конкуренты;

• персонал учреждения (банка, его филиалов).

С учетом анализа международного опыта защиты информации и опыта проведения аналогичных работ в отечественных организациях злоумышленные действия персонала, работающего в учреждении, можно разделить с учетом социальных предпосылок, характерных для России, на четыре основные категории:

1) прерывание – прекращение нормальной обработки информации, например вследствие разрушения вычислительных средств. Такие действия могут вызвать весьма серьезные последствия, если даже информация при этом не подвергается никаким воздействиям;

2) кража – чтение или копирование информации, хищение носителей информации с целью получения данных, которые могут быть использованы против интересов владельца (собственника) информации;

3) модификация информации – внесение в данные несанкционированных изменений, направленных на причинение ущерба владельцу (собственнику) информации;

4) разрушение данных – необратимое изменение информации, приводящее к невозможности ее использования.

К ***техногенным источникам*** угроз относятся:

• некачественные технические средства обработки информации;

• некачественные программные средства обработки информации;

• средства связи, охраны, сигнализации;

• другие технические средства, применяемые в учреждении;

• глобальные техногенные угрозы (опасные производства, сети энерго-, водоснабжения, канализации, транспорт и т.п.).

К ***стихийным источникам*** угроз относятся пожары, землетрясения, наводнения, ураганы и другие форс-мажорные

обстоятельства. Сюда же входят и различные непредвиденные обстоятельства и необъяснимые явления.

нформация, подлежащая защите

Определение степени конфиденциальности, а следовательно, и класса защиты информации является прерогативой собственника информации, а владелец информационных систем, на которых обрабатывается эта информация, обязан обеспечить выполнение комплекса организационных, организационно-технических и технических мер защиты, соответствующих выбранной степени конфиденциальности. Защите подлежит только документированная информация, т.е. зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Физические принципы защиты информации неизменны независимо от степени конфиденциальности. Поэтому методы и способы защиты сведений, составляющих государственную тайну, распространяются и на защиту конфиденциальной информации.

Банковская информация и банковская тайна. Под банковской информацией понимается совокупность информационных ресурсов банка, содержащих сведения об операциях и сделках, осуществляемых банком по всем направлениям его деятельности. Это могут быть сведения:

– о привлекаемых вкладах (депозитах) и предоставляемых кредитах;

– расчетах по поручению клиентов и банков-корреспондентов и об их кассовом обслуживании;

– об открытии и о ведении счетов клиентов и банков-корреспондентов;

– о финансировании капитальных вложений по поручению владельцев или распорядителей инвестируемых средств, а также за счет собственных средств банка;

– покупке у российских и иностранных юридических и физических лиц и продаже им наличной иностранной валюты и валюте, находящейся на счетах и во вкладах;

– покупке и продаже в Российской Федерации и за ее пределами драгоценных металлов, камней, а также изделий из них;

– привлечении и размещении драгоценных металлов во вклады, об осуществлении иных операций с этими ценностями в соответствии с международной банковской практикой;

– привлечении и размещении средств и управлении ценными бумагами по поручению клиентов;

– об оказании брокерских и консультативных услуг, осуществлении лизинговых операций и др.

Банковская тайна – это часть банковской информации, не содержащая сведений, составляющих государственную тайну, разглашение которой может нанести ущерб как самому банку, так и его клиентам и корреспондентам.

К банковской тайне ***не могут быть отнесены*** следующие сведения:

– учредительные документы (договор учредителей) и Устав;

– документы, дающие право заниматься банковской деятельностью (регистрационное удостоверение, лицензии, патенты);

– сведения по установленным формам отчетности о финансово-хозяйственной де

деятельности и иные сведения, необходимые для проверки правильности исчисления налогов и других обязательных платежей в государственную бюджетную систему РФ;

– документы о платежеспособности;

– сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

– документы об уплате налогов и обязательных платежей;

– сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, а также других нарушениях законодательства РФ и размерах причиненного ущерба.

Конкретный состав и объем сведений, составляющих банковскую тайну, определяются перечнями сведений, составляющих банковскую тайну, формируемых в банках.

По степени конфиденциальности информация, составляющая банковскую тайну, может подразделяться на конфиденциальную и строго конфиденциальную.

К ***конфиденциальной информации предприятия*** относятся сведения, содержащие планово-аналитические материалы и отчеты за текущий период времени, и другая информация о деятельности учреждения, разглашение которых может привести к снижению эффективности функционирования одной из систем, обеспечивающих жизнедеятельность и развитие учреждения. К такой информации можно отнести:

– результаты изучения и формирования новых направлений в инвестиционной политике предприятия;

– формы и методы работы с активами, структуру инвестиционного портфеля;

– информацию о поиске новых путей в деятельности учреждения, повышающих ее эффективность;

– материалы контроля организаций, работающих с участием банковского капитала;

– операции с акциями клиентов;

– дополнительные соглашения, протоколы и прочие документы, оформляемые в депозитарии к договорам;

– направления разработок в депозитарной и банковской технологиях;

– другие сведения.

К ***строго конфиденциальной информации*** относятся сведения стратегического характера, разглашение которых может привести к срыву выполнения функций одной или нескольких систем предприятия, прямо влияющих или способных повлиять на его жизнедеятельность и развитие. К таким сведениям можно отнести:

– главные цели, задачи учреждения, программы и пути их реализации;

– сведения об ошибках и просчетах в деятельности подразделений учреждения;

– информацию о причинах, сдерживающих динамику развития учреждения, обусловленных действиями государственных органов, конкурентов, внутренними причинами и др., главных проблемах и трудностях, возможностях их преодоления;

– информацию о негативном характере взаимодействия с органами государственного регулирования и управления, эмитентами и партнерами учреждения;

– предмет и результаты совещаний и заседаний высшего руководства учреждения.

Выделение документов и других носителей информации, содержащих конфиденциальные сведения, из общего потока информации осуществляется присвоением им грифов "Конфиденциально" и "Строго конфиденциально".

Примерный перечень сведений, подлежащих защите. С учетом принятого деления предлагается следующий примерный перечень конфиденциальных сведений, подлежащих защите.

Сведения об организации работы учреждения:

– концепция, планы и перспективы развития учреждения, включая его автоматизированную систему;

– штатное расписание и функциональные обязанности сотрудников;

– схемы, планы размещения оборудования, служебных помещений и их закрепление за должностными лицами учреждения;

– служебная и деловая переписка, информация частного характера;

– персональные данные сотрудников учреждения и его филиалов.

Сведения о функционировании систем обеспечения безопасности:

– планы размещения и технические характеристики систем и средств обеспечения безопасности;

– сведения о разграничении доступа персонала учреждения к конфиденциальной информации и полномочиях пользователей;

– закрепление служебных автомобилей за должностными лицами учреждения, маршруты их движения, места стоянки, пункты технического обслуживания;

– сведения о размещении хранилищ материальных ценностей и информации, оборудовании их средствами безопасности и порядке доступа к ним.

Сведения о возможностях и организации функционирования АС:

– сведения о разработчиках АС учреждения и средствах ее защиты, применяемых технических решениях защиты информации;

– сведения о мерах, принятых для обеспечения безопасности информации и персонала учреждения;

– исходные тексты уникального программного обеспечения, персональные данные о его разработчиках;

– сведения о технических возможностях АС по обработке информации, поступающей о от клиентов и партнеров.

Порядок отнесения сведений к конфиденциальным. Полномочия должностных лиц по отнесению информации к различным степеням конфиденциальности определяются Уставом организации, решением его руководства (правления) о разработке Перечня сведений, составляющих конфиденциальную тайну, решением руководства (правления) об утверждении Перечня и должностными обязанностями руководителей и сотрудников учреждения.

Руководитель предприятия в пределах своей компетенции определяет:

– порядок формирования и введения в действие Перечня сведений, составляющих конфиденциальную информацию;

– категорию должностных лиц, уполномоченных относить информацию к категории конфиденциальной информации;

– порядок передачи конфиденциальной информации другим учреждениям, органам и организациям;

– порядок выведения информации из категории конфиденциальной;

– организацию защиты информации, составляющей конфиденциальную тайну.

Он имеет право:

– дать разрешение на доступ к конфиденциальным сведениям;

– применять меры к сотрудникам учреждения, допустившим разглашение сведений, составляющих банковскую и коммерческую тайну;

– поощрять сотрудников, предотвративших разглашение конфиденциальных сведений.

Для придания сведениям, отнесенным к категории конфиденциальной информации, законной силы, они должны быть в обязательном порядке оформлены в виде специального перечня, утвержденного руководителем учреждения.

Прерогатива разработки такого перечня должна принадлежать ограниченному кругу лиц администрации учреждения. С перечнем должны быть ознакомлены все сотрудники учреждения, но только в части, их касающейся.

Полный Перечень сведений учреждения, отнесенных к категории конфиденциальных, должен иметь высший гриф конфиденциальности.

Защита от воздействия программ-вирусов

В современных условиях противодействие компьютерным вирусам стало одной из самых распространенных проблем при эксплуатации АС.

Защита АС от программ-вирусов является очень важной задачей, поскольку ущерб от их деструктивных воздействий может оказаться весьма существенным, а ликвидация как самих программ-вирусов, так и последствий их воздействия – чрезвычайно длительным.

Проблема компьютерных вирусов возникла давно и сразу же получила широкое распространение. В 1988 г. с появлением в сети "вируса Морриса" фактически началось более-менее целенаправленное развитие антивирусных средств.

Термин "вирус" в применении к компьютерам был придуман Фредом Когеном из Университета Южной Каролины. Слово "вирус" латинского происхождения и означает "яд". Компьютерный вирус – это программа, которая пытается тайно записать себя на компьютерные диски. Каждый раз, когда компьютер загружается с инфицированного диска, происходит скрытое инфицирование.

Вирусы представляют собой достаточно сложные и своеобразные программы, выполняющие несанкционированные пользователем действия.

Программой-вирусом принято называть программу, способную, саморазмножаясь, внедряться в другие программы. Единственным и возможным каналом проникновения вирусов в АС являются накопители на съемных носителях информации и средства межкомпьютерной коммуникации.

В жизненном цикле вируса выделяется три периода:

1) латентный период – вирус находится в зараженной программе, не предпринимая никаких действий;

2) инкубационный период – вирус размножается, заражая другие программы;

3) период деструктивных действий – вирус выполняет заложенный в него разработчиком алгоритм действий, продолжая при этом заражать другие программы.

Первые два периода предназначены для целей:

– сокрытия канала проникновения вируса в вычислительную систему;

– сокрытия факта существования вируса в программном обеспечении системы;

– заражения возможно большего числа программ вирусом.

Вирусы, как правило, могут содержаться в программных файлах и в ряде компонентов системной области диска, участвующих в процессе загрузки операционной системы.

К вирусам также относят вредоносные программы, не способные заражать другие программы, но разрушающие информацию на магнитных носителях информации или срывающие нормальное течение вычислительного процесса.

Способ функционирования большинства вирусов – это такое изменение системных файлов компьютера пользователя, чтобы вирус начинал свою деятельность либо при каждой загрузке, либо в один прекрасный момент, когда происходит некоторое "событие вызова".

При разработке современных компьютерных вирусов используется много технических новшеств, однако большая часть вирусов является имитацией и модификацией нескольких классических схем.

Вирусы можно классифицировать по типу поведения следующим образом.

1. Вирусы, поражающие загрузочный сектор, пытаются заменить или инфицировать часть съемного (или жесткого) диска, зарезервированную только для операционной системы и хранения файлов запуска. Они особенно коварны, так как загружаются в память при каждом включении компьютера. Тем самым вирусу дается полная возможность контролировать любой выполняемый компьютером процесс. Эти вирусы обладают наибольшей способностью к размножению и могут постоянно распространяться на новые диски.

2. Вирусы, инфицирующие файлы. Чтобы остаться необнаруженными, множество вирусов пытается инфицировать исполняемые файлы. Обычно вирусы отдают предпочтение ***EXE-*** и ***COM***-файлам, однако в связи с растущей популярностью ***Windows*** некоторые авторы вирусов стараются инфицировать файлы библиотек динамической связи ***(DLL).***

Файловые вирусы распространяются более медленно, чем вирусы, поражающие загрузочный сектор, вирус активизируется и начинает размножаться, только когда инфицированный файл запущен на выполнение. Единственное условие распространения вируса – это выполнение инфицированного программного файла. При этом он будет загружаться в память и сможет приступать к работе.

3. Многофункциональные вирусы. Некоторые вирусы используют для инфицирования компьютерной системы как загрузочный сектор, так и метод заражения файлов. Это несколько затрудняет выявление и идентификацию вируса специальными программами и ведет к быстрому его распространению.

4. Вирусы-невидимки. Один из способов выявления и идентификации вируса антивирусными программами – проверка контрольных сумм. Контрольная сумма – это результат выполнения математического алгоритма, проверяющего соответствие длины полученного файла длине его первоначальной копии. Ряд антивирусных программ создает списки контрольных сумм файлов, находящихся на вашем диске. Вирусы-невидимки используют ряд методов для маскировки своего присутствия – они фальсифицируют фактические значения контрольных сумм, что затрудняет их обнаружение.

5. Системные вирусы. Пытаясь остаться незамеченными, системные вирусы поражают не загрузочный сектор, а операционные системы. Основные жертвы этих вирусов – таблица размещения файлов (оглавление диска), таблицы разделов, драйверы устройств и системные файлы.

Наилучший способ защитить свою систему от вирусов – регулярно использовать антивирусные программы, предназначенные для проверки памяти и файлов системы, а также поиска сигнатур вирусов. Вирусная сигнатура – это некоторая уникальная характеристика вирусной программы, которая выдает присутствие вируса в компьютерной системе. Обычно в антивирусные программы входит периодически обновляемая база данных сигнатур вирусов.

При выполнении антивирусная программа просматривает компьютерную систему на предмет наличия в ней сигнатур, подобных имеющимся в базе данных.

В самом хорошем антивирусном программном обеспечении не только ищется соответствие с сигнатурами в базе данных, но используются и другие методы. Такие антивирусные программы могут выявить новый вирус даже тогда, когда он еще не был специально идентифицирован.

Однако большинство вирусов обезвреживается все же путем поиска соответствия с базой данных. Когда программа находит такое соответствие, она будет пытаться вычистить обнаруженный вирус. Важно постоянно пополнять имеющуюся базу вирусных сигнатур. Большинство поставщиков антивирусного программного обеспечения распространяет файлы обновлений через Интернет.

Однако следует иметь в виду, что иногда встречаются вирусы, идентификация которых затруднена либо из-за их новизны, либо из-за большого промежутка времени перед их активизацией (у вирусов имеется некоторый инкубационный период, и они некоторое время скрываются, прежде чем активизироваться и распространиться на другие диски и системы).

Поэтому следует обращать внимание на следующее:

1) изменения размера файла. Файловые вирусы почти всегда изменяют размер зараженных файлов, поэтому если вы заметите, что объем какого-либо файла, особенно ***COM*** или ***EXE,*** вырос на несколько килобайт, необходимо немедленно обследовать жесткие диски антивирусной программой;

2) необъяснимые изменения в доступной памяти. Для эффективного распространения вирус должен находиться в памяти, что неизбежно уменьшает количество оперативной памяти ***(RAM),*** остающейся для выполнения программ. Поэтому если вы не сделали ничего, что изменило бы объем доступной памяти, однако обнаружили ее уменьшение, необходимо также запустить антивирусную программу;

3) необычное поведение. При загрузке вируса, как и любой новой программы, в компьютерную систему происходит некоторое изменение в ее поведении. Может быть, это будет либо неожиданным изменением времени перезагрузки, либо изменением в самом процессе перезагрузки, либо появлением на экране необычных сообщений. Все эти симптомы говорят о том, что следует незамедлительно запустить антивирусную программу.

Если вы обнаружили в компьютере какой-либо из указанных выше симптомов, а антивирусная программа не в состоянии обнаружить вирусную инфекцию, следует обратить внимание на саму антивирусную программу – она может быть устаревшей (не содержать новых вирусных сигнатур) или же сама может быть заражена. Поэтому надо запустить надежную антивирусную программу.

В заключение приведем девять правил компьютерной безопасности (защиты от вирусов) от "Лаборатории Касперского".

1. Периодически обновляйте вашу антивирусную программу. Антивирусные сканеры способны защищать только от тех компьютерных вирусов, данные о которых содержатся в антивирусной базе. В связи с этим необходимо регулярно обновлять антивирусные базы. Чем чаще выполняется эта несложная операция, тем более защищенным будет компьютер. Рекомендуется настроить внутренний планировщик, присутствующий в большинстве современных антивирусных программ, на автоматическую загрузку обновлений.

2. Будьте осторожны с файлами в письмах электронной почты. Нельзя запускать программы, присланные неизвестным лицом. Файлы, полученные от "надежных" корреспондентов, также могут быть инфицированы.

Не менее важным моментом является кажущаяся безопасность вложенных файлов определенного формата. Если вы думаете, что файлы с расширением ***PIF, GIP, TXT*** не могут содержать вредоносных программ, то глубоко заблуждаетесь. Даже в таких "безобидных" программах могут быть замаскированы вирусы. Следовательно, второе

правило можно сформулировать так: не запускайте полученные файлы, пока не убедитесь, что они присланы известным вам лицом, и не проверите их антивирусной программой с самыми последними обновлениями,

3. Ограничьте круг лиц, пользующихся вашим компьютером. Идеальным вариантом является ситуация, когда никто, кроме вас, не имеет доступа к вашему компьютеру. Если это невозможно, то необходимо четко разграничить права доступа и определить круг разрешенных действий для других лиц. В первую очередь это касается работы с мобильными носителями информации (ленты, диски), Интернетом и электронной почтой.

4. Своевременно устанавливайте "заплатки" к программному обеспечению. Многие вирусы используют "дыры" в системах защиты операционных систем и приложений. Антивирусные программы способны защищать от такого типа вредоносных воздействий, даже если на компьютере не установлена соответствующая "заплатка", закрывающая "дыру". Тем не менее рекомендуется регулярно проверять ***Web***-сайты производителей установленного программного обеспечения и следить за выпуском новых "заплаток". В первую очередь это относится к операционной системе ***Windows*** и другим программам корпорации ***Microsoft,*** которые наиболее распространены и привлекают наибольшее внимание создателей вирусов.

5. Обязательно проверяйте мобильные носители информации. Несмотря на то что около 85% всех зарегистрированных случаев заражения компьютерными вирусами приходится на электронную почту и Интернет, не стоит забывать о таком традиционном способе транспортировки вредоносных кодов, как мобильные носители информации. Следует тщательно проверять их антивирусной программой, прежде чем использовать на своем компьютере. Исключением, пожалуй, являются диски, предназначенные для форматирования.

Большую опасность представляют собой и столь широко распространенные в России пиратские компакт-диски. К примеру, проверка, проведенная "Лабораторией Касперского" в 1999 г., выявила факт присутствия вирусов на 23% закупленных носителей. Вывод и здесь достаточно прост: тщательно проверяйте даже вновь приобретенные компакт-диски.

6. Будьте осторожны и с источниками, заслуживающими доверия. Никто не застрахован от компьютерных вирусов. Это относится и к крупным компаниям-производителям программного и аппаратного обеспечения. Посетителям их сайтов нередко предлагаются зараженные программы. Показателен факт, когда в течение нескольких недель на сайте ***Microsoft*** находился документ ***Word,*** зараженный макровирусом ***Wazzu.***

Нередки случаи присутствия вирусов на дисках с драйверами к аппаратному обеспечению, в лицензионном программном обеспечении и т.п.

Бывает также, что компьютер, переданный на техническое обслуживание в ремонтную мастерскую, возвращается не совсем "чистым". Как правило, это происходит из-за того, что ремонтники пользуются одними и теми же дисками и флеш-картами для загрузки программ для тестирования различных узлов компьютера. Таким образом, они очень быстро переносят компьютерную "заразу" с одних компьютеров на другие.

Вывод: получив компьютер из ремонта, не забудьте тщательно проверить его на наличие вирусов.

Настоятельно рекомендуется проверять даже данные, полученные из источников, заслуживающих доверия. Не стоит думать, что производители умышленно заражают ваш компьютер, в каждой работе бывают осечки. Иногда они касаются и антивирусной безопасности.

7. Сочетайте разные антивирусные технологии. Не следует ограничиваться классическим антивирусным сканером, запускаемым по требованию пользователя или при помощи встроенного планировщика событий. Существует ряд других, нередко более эффективных технологий, комбинированное использование которых способно гарантировать безопасную работу компьютера. К числу таких технологий относятся:

– антивирусный монитор, постоянно присутствующий в памяти компьютера и проверяющий все используемые файлы в масштабе реального времени (в момент доступа к ним);

– ревизор изменений, который отслеживает все изменения на диске и немедленно сообщает, если в каком-либо из файлов "поселился" вирус;

– поведенческий блокиратор, обнаруживающий вирусы не по их уникальному коду, а по последовательности их действий.

Сочетание описанных способов борьбы с вирусами является залогом успешной защиты от вредоносных программ.

8. Регулярное резервное копирование. Выполнение этого правила позволит сохранить данные не только при поражении компьютера каким-либо вирусом, но и в случае серьезной поломки в аппаратной части компьютера.

Вряд ли кому захочется потерять результаты многолетних наработок вследствие произошедшего сбоя в системе вне зависимости от того, вызвано это вирусами или нет. Именно поэтому рекомендуется регулярно копировать наиболее ценную информацию на независимые носители – флеш-карты, внешние жесткие диски и т.д.

9. Не паникуйте! Не следует думать, что вирусы – это неисправимая катастрофа. Они являются такими же программами, как, скажем, калькулятор или записная книжка ***Windows.*** Отличительная их черта в том, что вирусы способны размножаться (т.е. создавать свои копии), интегрироваться в другие файлы или загрузочные секторы, а также производить другие несанкционированные действия. И гораздо больший вред способны нанести необдуманные действия, направленные на нейтрализацию вируса. При работе в корпоративной сети следует немедленно обратиться к системному администратору. Если же вы просто автономный пользователь, свяжитесь с компанией, у которой приобрели антивирусную программу. Предоставьте возможность профессионалам позаботиться о безопасности вашего компьютера.

Как показывает практика, небольшая доля подозрительности является обязательной для успешного проведения политики компьютерной безопасности.

7.6. Финансовая безопасность предприятия

Состояние финансовой безопасности предприятия характеризуют многие показатели, которые можно исходя из их назначения объединить в следующие группы.

1. Показатели платежеспособности: коэффициент обеспеченности собственными средствами; коэффициент восстановления платежеспособности; коэффициент утраты платежеспособности; коэффициент автономии, коэффициент маневренности собственного капитала.

2. Показатели финансовой устойчивости: коэффициент собственности (независимости); доля заемных средств; соотношение заемных и собственных средств.

3. Показатели деловой активности: общий коэффициент оборачиваемости; скорость оборота; оборачиваемость собственных средств.

4. Показатели рентабельности: имущество предприятия; собственные средства; производственные фонды; долгосрочные и краткосрочные финансовые вложения; собственные и долгосрочные заемные средства; норма балансовой прибыли; чистая норма прибыли.

Первичный анализ финансовой составляющей экономической безопасности предприятия производится по данным бухгалтерского баланса предприятия и формы № 2. Он необходим не только для того, чтобы знать, в каком положении находится предприятие на тот или иной отрезок времени, но и для эффективного управления с целью обеспечения финансово-хозяйственной устойчивости предприятия.

Показатели платежеспособности. Показатели платежеспособности характеризуют возможность предприятия в течение финансового года погашать все краткосрочные обязательства. Устойчивое финансовое развитие предприятия является одним из

показателей его кредитоспособности. Коэффициенты платежеспособности предприятия и их динамика позволяют выявить наличие собственных средств предприятия и источников их формирования для покрытия кредитных обязательств в будущем периоде.

Коэффициенты платежеспособности:

1) коэффициент обеспеченности собственными средствами (Коск) – характеризует наличие собственных оборотных средств у предприятия, необходимых для его финансовой устойчивости. Рекомендуемое значение – больше 1.

Коск = СК – ВА / ОА,

где СК – собственный капитал (стр. 1300); ВА – внеоборотные активы (итого по разд. I (стр. 1100)); ОА – оборотные активы (итого по разд. II (стр. 1200));

2) коэффициент восстановления платежеспособности (Квпл) – отражает наличие/отсутствие у предприятия реальной возможности восстановить свою платежеспособность в течение установленного срока:

Квпл = (Ктл + 6/ ***Т(***Ктл – 2)) / 2,

где Ктл – коэффициент текущей ликвидности; ***Т*** – период (в данном случае 12 месяцев);

3) коэффициент утраты платежеспособности (Кут) – отражает наличие/отсутствие у предприятия реальной возможности утратить свою платежеспособность в течение установленного срока:

Кут = (Ктл + 3 / ***Т*** (Ктл – 2)) / 2;

4) коэффициент автономии, или коэффициент концентрации собственного капитала (Ккск) – характеризует долю владельцев (собственников) предприятия в общей сумме средств, используемых в финансово-хозяйственной деятельности. Чем выше коэффициент, тем предприятие более устойчиво и независимо от внешних кредиторов:

Ккск= СК / ВБ,

где СК– собственный капитал (стр. 1300); ВБ – валюта баланса (стр. 1700);

5) коэффициент маневренности собственного капитала (Кмск) – показывает, какая часть капитала используется для финансирования текущей деятельности (т.е. вложена в оборотные средства), а какая – капитализирована:

Кмск = СОС / СК,

где СОС – собственные оборотные средства (стр. 1200 – стр. 1500); СК – собственный капитал (стр. 1300).

Показатели финансовой устойчивости характеризуют степень защищенности привлеченного капитала. Они состоят из коэффициента собственности (независимости) (***F***р); коэффициента заемных средств (***F***т***I***); коэффициента заемных и собственных средств (***F***т***I***р***).***

Fp= ***R***P/ ***R***f**,**

где ***R***p **–** собственные средства; ***R***f **–** основные средства собственности.

Коэффициент заемных средств и коэффициент заемных и собственных средств рассчитываются по аналогии, в знаменателе – основные средства, в числителе соответственно заемные средства и сумма заемных и собственных средств

В странах с развитой рыночной экономикой установлены предельные значения этих показателей: ***F***p > 0,7; ***F***r***I***<0,3; ***F***r***I***p < 1.

Показатели деловой активности: общий коэффициент оборачиваемости ***(F***tkq***);*** скорость оборота; оборачиваемость собственных средств.

$$F_{tkq} = G_{rp} / C_{p}$$

где ***G***rp – выручка от реализации продукции; ***C***p – стоимость имущества (итог баланса).

Для характеристики деловой активности предприятия применяется и ряд других показателей. В странах с развитой рыночной экономикой по наиболее важным показателям деловой активности устанавливаются нормативы в целом и по отраслям. Как правило, такие нормативы отражают средние фактические значения этих коэффициентов. Так, в большинстве стран существуют следующие нормативы:

– нормативом оборачиваемости запасов являются три оборота, т.е. 120 ***F***tkq – 122 дня;

– нормативом оборачиваемости дебиторской задолженности – 4,9, или примерно 74 дня.

Среднюю стоимость активов и пассивов за определенный период рассчитывают как среднюю хронологическую по месячным данным; если в распоряжении финансового аналитика имеется лишь годовой баланс, то применяется упрощенный прием: средняя из сумм данных на начало и конец периода.

Показатели оценки рентабельности: имущество предприятия; собственные средства; производственные фонды; долгосрочные и краткосрочные финансовые вложения; собственные и долгосрочные заемные средства; норма балансовой прибыли.

$$R_p = P_c / A \cdot 100\%,$$

где ***R***p – рентабельность имущества; ***P***c – чистая прибыль; ***A*** – средняя стоимость имущества (активов).

Для того чтобы постоянно следить за экономической безопасностью предприятия, руководству необходимы индикаторы, позволяющие быстро определить изменения. В практической деятельности наиболее содержательными представляются квартальные, ежемесячные или даже ежедневные промежуточные отчеты, оцениваемые по тем же методикам, что и ежегодные. При надлежащей плотности и взаимосвязанности именно краткосрочные анализы могут быстро обнаружить слабые и сильные стороны положения

предприятия и дать необходимые отправные точки для корректирующих мероприятий. Из открытых годовых и итоговых отчетов следует брать следующую информацию:

– параметры деятельности предприятия, предшествовавшие банкротству или обеспечивающие интенсивное развитие предприятия;

– наличие реальной возможности восстановить (либо утратить) свою платежеспособность в течение определенного периода;

– причины финансовой неустойчивости предприятия, приведшие к его неплатежеспособности;

– состояние ликвидности активов и их структуры.

Финансовое равновесие предполагает своевременное выполнение своих платежных обязательств перед бюджетом, работниками и поставщиками материальных ресурсов, сдерживание факторов, способных дестабилизировать ситуацию.

Способность к дальнейшему развитию и совершенствованию, что особенно важно в современном, динамично развивающемся мире, предполагает модернизацию производства, повышение профессионального, образовательного и общекультурного уровня работников, расширение производства, диверсификацию направлений деятельности, внутренние инвестиции, что становится необходимым и обязательным условием устойчивости и стабильности функционирования предприятия.

С целью получения более достоверной картины проводится расчет коэффициентов ликвидности. Основными из них являются следующие.

1. Коэффициент быстрой (промежуточной) ликвидности (Кбл) – характеризует возможность компании погашать краткосрочные обязательства за счет оборотных активов.

Кбл = ОА – З / КО,

где ОА – оборотные активы – это итог разд. II баланса (стр. 1200) за вычетом дебиторской задолженности, поступления по которой ожидаются более чем через 12 месяцев; З – запасы (стр. 1210); КО – краткосрочные обязательства (сгр. 1510 + стр. 1520 + стр. 1550).

Рекомендуемое значение коэффициента быстрой (промежуточной) ликвидности – 0,7-1,5.

2. Коэффициент текущей ликвидности (Ктл) отражает достаточность средств предприятия, необходимых для покрытия краткосрочных обязательств в течение года, и имеет вид

$$К_{тл} = ОА / КО.$$

Рекомендуемое значение коэффициента текущей ликвидности – 1–2.

3. Коэффициент абсолютной ликвидности (Каб1) – показывает, какую часть кредиторской задолженности предприятие может погасить немедленно.

$$К_{абл} = (ДС + КФВ) / КО,$$

где ДС – денежные средства (стр. 1250); КФВ – краткосрочные финансовые вложения (стр. 1240).

Рекомендуемое значение коэффициента абсолютной ликвидности – более 0,2.

Оценку уровня экономической безопасности предприятия можно определить с помощью оценки уровня потенциального банкротства. Одним из наиболее популярных методов является метод Альтмана.

Этот метод предложен в 1968 г. известным западным экономистом Альтманом ***(Edward I. Altman).***

Индекс кредитоспособности построен с помощью аппарата мультипликативного дискриминантного анализа (***Multiple-discriminant, analysis – MDA)*** и позволяет в первом приближении разделить хозяйствующие субъекты на потенциальных банкротов и небанкротов. Данный подход был разработан с учетом мирового опыта антикризисного управления.

При построении индекса Альтман обследовал 66 предприятий, половина которых обанкротилась в период между 1946 и 1965 гг., а половина работала успешно, и исследовал 22 аналитических коэффициента, которые могли быть полезны для прогнозирования возможного банкротства. Из этих показателей он отобрал пять наиболее значимых и построил многофакторное регрессионное уравнение. Таким образом, индекс Альтмана представляет собой функцию от некоторых показателей, характеризующих экономический потенциал предприятия и результаты его работы за истекший период. В общем виде индекс кредитоспособности (Z-коэффициент) имеет вид:

$$Z = 1{,}2X1 + 1{,}42X2 + 3{,}3X3 + 0{,}6X4 + 0{,}99X5,$$

где $X1$ – оборотные активы/сумма активов; $X2$ – нераспределенная прибыль/сумма активов; $X3$ – операционная прибыль (прибыль до налогообложения)/сумма активов; X4 – рыночная стоимость компании (стоимость собственного капитала)/суммарная задолженность (долгосрочные + краткосрочные обязательства); $X5$ – выручка/сумма активов.

Результаты многочисленных расчетов по модели Альтмана показали, что обобщающий показатель Z может принимать значения в пределах [-14, +22], при этом предприятия, для которых $Z > 2{,}99$, попадают в число финансово устойчивых, предприятия, для которых $Z < 1{,}81$, являются безусловно-несостоятельными, а интервал [1,81–2,99] составляет зону неопределенности.

Критическое значение показателя Z = 2,675, сравнение этого критического показателя со значениями для каждой конкретной фирмы позволит судить о возможном банкротстве за два-три года до его наступления (если Z < 2,675). Если показатель предприятия Z > 2,675, это говорит о его финансовой устойчивости.