К. С. Кривякин, Н. Н. Макаров, Д. М. Шотыло

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ НА РЕЖИМНЫХ ОБЪЕКТАХ

Учебно-методическое пособие

Воронеж
Издательско-полиграфический центр
«Научная книга»
2020

УДК 658.11
ББК 65.292.9-983
К82

Рецензенты:
д-р. экон. наук. *А. С. Свиридов*
(кафедра экономики и менеджмента Воронежского филиала
ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»);
канд. экон. наук, доц. *О. М. Фокина*
(кафедра экономики, финансов и менеджмента РАНХиГС
при Президенте Российской Федерации, Воронежский филиал)

Кривякин, К. С.

К82 Экономическая безопасность на режимных объектах : учебно-методическое пособие / К. С. Кривякин, Н. Н. Макаров, Д. М. Шотыло. – Воронеж : Издательско-полиграфический центр «Научная книга», 2020. – 102 с. – ISBN 978-5-4446-1479-2. – Текст : непосредственный.

В учебно-методическом пособии представлен конспект лекций, комплекс практических занятий и лабораторных работ, позволяющие студентам приобрести теоретические знания и практические навыки по дисциплине «Экономическая безопасность на режимных объектах»

Издание соответствует требованиям Федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 «Экономическая безопасность», дисциплине «Экономическая безопасность на режимных объектах»

Предназначено для студентов, аспирантов и преподавателей вузов, изучающих дисциплины организационно-экономического цикла.

УДК 658.11
ББК 65.292.9-983

ISBN 978-5-4446-1479-2

ВВЕДЕНИЕ

В условиях активизации глобальных вызовов и возрастания неопределенности внешней среды повышается значимость задач обеспечения экономической безопасности на режимных объектах.

Режимными объектами являются военные и специальные объекты, воинские части, предприятия, организации, учреждения, для функционирования которых установлены дополнительные меры безопасности [27].

Экономическую безопасность можно рассматривать как состояние, обеспечивающее эффективное использования конкурентных преимуществ и различного вида ресурсов, для реализации экономических интересов предприятия и с учетом необходимости защиты от внешних и внутренних угроз, включая экономические преступления.

Экономическая безопасность режимного предприятия - это, скорее, состояние предприятия, либо его определенное свойство, характеристика, а не процесс. В свою очередь, обеспечение безопасности режимного предприятия - это процесс, который должен быть непрерывным и комплексным, работа должна вестись по всем без исключения составляющим экономической безопасности.

В качестве объекта исследования в данном курсе будут выступать режимные предприятия. Предметом исследования является процесс обеспечения экономической безопасности режимного предприятия.

Цель изучения дисциплины «Экономическая безопасность на режимных объектах» состоит в освоении студентами структуры и основных направлений обеспечения экономической безопасности режимного предприятия.

К задачам освоения дисциплины «Экономическая безопасность на режимных объектах» относится:

- формирование системных знаний об основах обеспечения экономической безопасности режимного предприятия;
- изучение форм и методов оценки уровня и анализа отдельных составляющих экономической безопасности режимного предприятия;
- овладение навыками оценки рисков и угроз экономической безопасности на режимном предприятии;
- приобретение практических навыков в области разработки системы экономической безопасности режимного предприятия.

РАЗДЕЛ 1. КОНСПЕКТ ЛЕКЦИЙ
ТЕМА №1.Теоретические основы экономической безопасности предприятия

1.1 Сущность экономической безопасности предприятия

Одним из условий эффективного функционирования предприятия в современных условиях рыночной экономики, является его экономическая безопасность. Экономическая безопасность отдельных предприятий является основой экономической безопасности регионов, в которых они находятся и государства в целом.

Отечественные предприятия подвержены воздействию большого количества внутренних и внешних угроз, зачастую криминального характера, что приводит к негативным последствиям для всего народного хозяйства. Поэтому обеспечение экономической безопасности предприятий является одним из приоритетных направлений в системе национальной безопасности государства.

В научной литературе отсутствует единое мнение относительно трактовки понятия «экономическая безопасность предприятия». В дискуссии о сущностной характеристики экономической безопасности предприятия, можно выделить несколько подходов, представленных на рис. 1.1.1

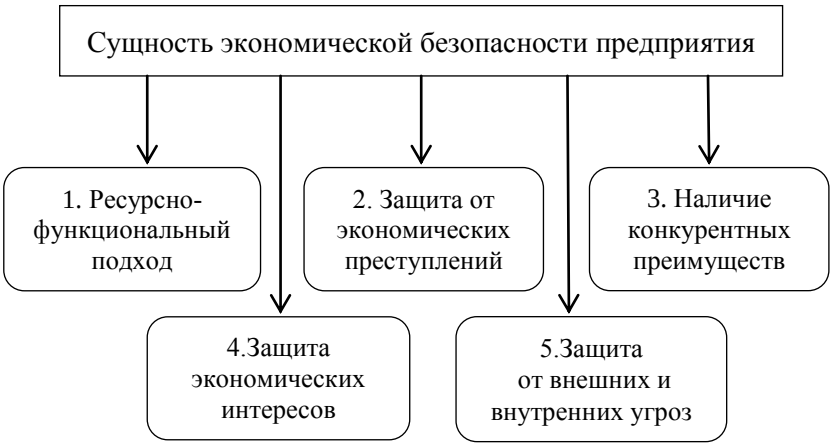

Рис. 1.1.1 Основные подходы к определению сущности экономической безопасности предприятия

Представленные подходы к определению сущности экономической безопасности предприятия, разделяют различные авторы.

Первая группа авторов трактует экономическую безопасность предприятия как состояние, обеспечивающее эффективное применение ресурсов или потенциала предприятия. Сторонники данного подхода, пытаются избежать употребления понятия угрозы в определении экономической безопасности предприятия, фокусируясь на экономических понятиях достижения цели, функционирование предприятия. Ресурсно-функционального подхода придерживаются такие ученые, как А.А. Одинцов [25], А.Ю. Евсеева, С.В. Котик [11], Е.А. Олейников [33], Н.В. Матвеев [21], А.А. Беспалько [4], В. А. Богомолов [6].

Вторая группа авторов, таких как М.И. Королев[17], А.Г. Шаваев [30], В.И. Ярочкин [35] определяет экономическую безопасность предприятия, как защиту против экономических преступлений. Очень часто, обеспечение экономической безопасности предприятия сводят к противостоянию, защите от разного рода экономических преступлений (кражи, мошенничество, фальсификации, промышленный шпионаж и т.д.). Несомненно, эти угрозы очень важны и должны постоянно анализироваться и учитываться, но сводить экономическую безопасность предприятия только к этому нельзя.

А.В. Козаченко, В.П. Пономарев, А.Н. Ляшенко [15], определяет экономическую безопасность предприятия, как наличие конкурентных преимуществ. Сторонники данного подхода считают, что наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и организационной структуры предприятия его стратегическим целям и задачам обеспечат ему определенный уровень экономической безопасности. Но сам факт наличия преимуществ и потенциала, без их использования и реализации, не гарантирует предприятию экономической безопасности.

Самым популярным подходом является определение экономической безопасности предприятия, как состояние защищенности от внутренних и внешних угроз. Предприятие - это в первую очередь - объект экономических отношений. Владелец предприятия в первую очередь ставит результатом деятельности предприятия - достижение поставленной им цели, которая, как правило, носит экономический характер. Борьба с угрозами, как таковая, зачастую не является целью создания и функционирования предприятия. Впрочем, рассуждения об экономической целесообразности ведения борьбы с угрозами наверняка вызовет интерес собственника, поскольку это непосредственно затрагивает его материальные интересы, однако ведение этой борьбы требует осуществления расходов, а резуль-

тат в данном случае не является очевидным. Такого подхода придерживаются такие ученые, как В.В. Шлыков [32], А.В. Кашин [13], С.Л. Маламедов [22], О.А Грунин, С.О. Грунин [9], С.А. Арбузов [2] и др.

Относительно новый подход, основанный на реализации и защите экономических интересов предприятия, определяет экономическую безопасность, как защищенность его жизненно важных интересов от внутренних и внешних угроз, то есть защиту предприятия, его кадрового и интеллектуального потенциала, информации, технологий, капитала и прибыли, которая обеспечивается системой мер специального правового, экономического, организационного, информационно-технического и социального характера. Данного подхода придерживаются У.Т. Хайитматов, О.Х. Азаматов, Р.Р. Мажидов, А.Ф. Хакимов [29], Н. К. Муратова [23], И. А. Коноплева, И. А. Богданов [16].

Наиболее полное определение экономической безопасности предприятия, можно сформулировать на основе комплексного подхода, опирающегося на комбинацию существующих. В этом контексте, понятие экономическая безопасность предприятия, можно рассматривать, как состояние, обеспечивающее эффективное использования конкурентных преимуществ и различного вида ресурсов, для реализации экономических интересов предприятия, с учетом защищенности от внешних и внутренних угроз, включая экономические преступления.

1.2 Основные компоненты экономической безопасности предприятия

Уровень экономической безопасности предприятия, напрямую зависит от уровня функциональных составляющих экономической безопасности предприятия [20].

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

По мнению И.А. Бланка, финансовая безопасность – это количественно и качественно детерминированный уровень финансового состояния предприятия, обеспечивающий стабильную защищенность его приоритетных сбалансированных финансовых интересов от реальных и потенциальных угроз внешнего и внутреннего характера, параметры которого определяются на основе его финансовой философии и создают необходимые предпосылки финансовой поддержки его устойчивого роста в текущем и перспективном периоде [5].

Основные функциональные составляющие экономической безопасности предприятия представлены на рис.1.1.2.

Рис.1.1.2 Основные функциональные составляющие экономической безопасности предприятия

Процесс обеспечения финансовой составляющей экономической безопасности предприятия может быть определен, как совокупность работ по обеспечению максимально высокого уровня платежеспособности предприятия и ликвидности его оборотных средств, наиболее эффективной структуры капитала предприятия, повышению качества планирования и осуществления финансово-хозяйственной деятельности

предприятия по всем направлениям стратегического и оперативного управления технологическим, интеллектуальным и кадровым потенциалом предприятия, его основными и оборотными активами с целью максимизации прибыли и повышения уровня рентабельности бизнеса, а также роста курсовой стоимости ценных бумаг предприятия.

Данная составляющая экономической безопасности находится в зоне ответственности финансовых и экономических служб предприятия.

Под кадровой безопасностью предприятия понимают процесс предотвращения негативных воздействий (ущербов) на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом [12].

Обеспечение интеллектуально-кадровой составляющей экономической безопасности предприятия включает в себя тесно связанные между собой, но в тоже время различные направления деятельности. Первое направление ориентировано на работу с персоналом предприятия, на повышение эффективности работы его сотрудников. Втрое направление нацелено на сохранение и развитие интеллектуального потенциала предприятия.

Интеллектуально-кадровая безопасность обеспечивается в процессе предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным и трудовым потенциалом.

Основная сущность технико-технологической составляющей экономической безопасности предприятия, будь то предприятие производственной или непроизводственной сферы, заключается в том, насколько уровень используемых на данном предприятии технологий соответствует лучшим мировым аналогам. Принципиально важным моментом является проблема наличия у этих технологий потенциала развития их будущей конкурентоспособности с технологиями-заместителями, чье влияние на технологическое развитие в современной мировой экономики возрастает с каждым днем [10].

Технико-технологическая составляющая экономической безопасности предполагает создание и использование такой материально-технической базы и технологических процессов, которые позволят повысить уровень конкурентоспособности предприятия.

Информационную безопасность – это состояние защищенности информационной среды предприятия, способное обеспечить его функционирование и устойчивое развитие [31]. Информационная составляющая предполагает защищенность информации, ресурсов и поддерживающей

инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений - производителям, владельцам и пользователям информации.

Существующую на предприятии систему обеспечения информационной безопасности следует оценивать с позиций реализации комплекса мероприятий и технических решений по защите от преступлений в сфере информационных технологий, к которым относятся:

- нарушения функционирования информационного пространства путем исключения воздействия на информационные каналы и ресурсы;

- несанкционированный доступ к информации путем обнаружения и ликвидации попыток по использованию ресурсов информационного пространства, приводящих к нарушению его целостности;

- разрушение встраиваемых средств защиты с возможностью выявления неправомочности действий пользователей и обслуживающего персонала;

- внедрения программных «вирусов» и «закладок» в программные продукты и технические средства.

Рассматривая содержание процесса обеспечения экономической безопасности предприятия, можно выделить основные функции информационно-аналитического подразделения предприятия, надлежащие выполнение, которых обязательно необходимо для достижения необходимого приемлемого уровня обеспечения информационной безопасности предприятия. К числу таких основных функций относятся:

-сбор всех видов информации, имеющей отношение к деятельности конкретного предприятия;

-анализ получаемой информации;

-прогнозирование тенденций научного и технологического прогресса в сфере деятельности предприятия, экономических и политических процессов в стране и в мире, имеющих отношение к данному бизнесу, а также показателей, которых необходимо достичь предприятию во всех областях своей деятельности;

-оценка уровня экономической безопасности предприятия по всем ее составляющим, и в целом, выработка рекомендаций по повышению уровня обеспечения экономической безопасности предприятия.

Силовая составляющая экономической безопасности ориентирована на организацию режима, физической охраны объектов и личной охраны руководства, противодействием криминалу, взаимодействием с правоохранительными и другими государственными органами.

Под силовой составляющей экономической безопасности предприятия можно понимать совокупность следующих состояний:

- физическая безопасность сотрудников предприятия, особенно представителей руководства предприятия;
- сохранность имущества от негативных воздействий, угрожающих потерей этого имущества или снижением его стоимости;
- силовые аспекты информационной безопасности предприятия.

Правовая составляющая экономической безопасности подразумевает всестороннее юридическое обеспечение деятельности предприятия, грамотную правовую работу с контрагентами и властью, а также решение других правовых вопросов.

Сущность правовой составляющей экономической безопасности предприятия состоит в эффективном и всестороннем правовом обеспечении деятельности данного предприятия, четком соблюдением предприятием и его сотрудниками всех аспектов действующего законодательства при оптимизации затрат кооперативных ресурсов на достижение этих целей при активной работе соответствующих служб предприятия по благоприятному изменению внешней правовой среды.

Возможными причинами низкого уровня правовой составляющей экономической безопасности чаще всего являются:

- низкая квалификация сотрудников юридической службы, слабая проработка договорных отношений предприятия с контрагентами по бизнесу, с персоналом по трудовым договорам;
- неэффективное юридическое отстаивание интересов предприятия в конфликтных ситуациях и слабое юридическое планирование обеспечения поддержки бизнеса.

Под экологической безопасностью предприятия понимают обеспечение соответствия его природоохранной деятельности нормативным требованиям. В свете повышения уровня экологической ответственности предприятия его экологическая безопасность для окружающей среды и населения в значительной степени определяет его конкурентоспособность [1].

Экологическая составляющая экономической безопасности предприятия представляет собой комплекс организационно-технических мер, которые направлены на обеспечение соответствия природоохранной деятельности предприятия нормативным требованиям.

Сущность экологической составляющей экономической безопасности с точки зрения предприятия, состоит в стремлении оптимизировать свои финансовые затраты таким образом, чтобы при минимальных затратах на соблюдение экологических норм по технологическим процессам

на предприятии и выпускаемой им продукции, минимизировать свои потери от административных санкций за загрязнение окружающей среды и потери рынков стран с более жесткими нормами экологического законодательства [10].

Таким образом, безопасность предприятия - это скорее состояние предприятия, либо его определенное свойство, характеристика, а не процесс. В свою очередь обеспечение безопасности предприятия – это процесс, который должен быть непрерывным и комплексным, работа должна вестись по всем без исключения выделенным составляющим экономической безопасности [18].

Описанные цели, проблемы и содержание выделенных функциональных составляющих экономической безопасности, должны быть положены в основу разработки системы обеспечения экономической безопасностью предприятия. Организация эффективного функционирования системы обеспечения экономической безопасности предприятия, позволит прогнозировать угрозы экономической безопасности и оперативно регулировать объемы и структуру издержек на обеспечение безопасности выделенных функциональных составляющих экономической безопасности. Кроме того, работа по обеспечению безопасности окажет качественное воздействие на общее финансовое состояние предприятия, что в конечном итоге, положительным образом отразится не только на деятельности предприятия, но и на экономике региона, в котором оно находится.

Контрольные вопросы:

1.Перечислите основные походы к определению понятия «экономическая безопасность предприятия».

2. Какое определение понятия «экономическая безопасность предприятия», представляется наиболее приемлемым для вас, аргументируйте свой выбор.

3. Назовите и охарактеризуйте основные составляющие компоненты экономической безопасности предприятия.

ТЕМА №2. Организация режима и охраны на предприятии

2.1 Задачи организации режима и охраны на предприятии

Цель создания режима и охраны определяет его задачи, выбор способов, а также сил и средств для охраны.

Режим и охрана - это сочетание организационных, регламентационных и контрольных мер, направленных на обеспечение полной (круглосуточной, в течение длительного времени), частичной (только ночное или

дневное время) или выборочной (при завозе ценных грузов, на определенный отрезок времени и т.п.) сохранности физических лиц, материальных и финансовых ценностей, зданий и помещений предприятия, а также любых сведений о деятельности предприятия, не подлежащих разглашению. Соблюдение этих мер обязательно для всех сотрудников, посетителей и клиентов.

Основные задачи службы безопасности по организации режима и охраны на предприятии:

- обеспечение сохранности зданий и помещений предприятия;
- сохранность и контроль за перемещением материальных ценностей;
- обеспечение пропускного режима (или контроль за допуском граждан в здания и помещения);
- сохранность собственной информации о деятельности предприятия;
- поддержание противопожарной безопасности.

В число обеспечивающих задач входят:

- подбор, подготовка и расстановка сил и средств;
- контроль функционирования системы режима и охраны;
- материально-техническое обеспечение режима и охраны;
- сбор и анализ информации о состоянии режима.

Принципами режима и охраны являются: целесообразность, активность, рациональное использование сил и средств, скрытность, выбор ключевого звена, стремление к максимальной информированности [26].

2.2 Организация пропускного режима

Обычно устанавливаются следующие виды пропускных документов, дающих право прохода сотрудников и посетителей на предприятие, вноса (выноса), ввоза (вывоза) материальных ценностей:

- удостоверение личности;
- пропуск.

Пропуска могут быть постоянными, временными и разовыми для сотрудников и посетителей, а также материальными для ввоза (вывоза) материальных ценностей.

На удостоверениях и пропусках проставляются печати, предусмотренные правилами режима, и цифровые знаки, определяющие зону доступности, период их действия, право проноса портфелей (кейсов, папок и др.). Период пребывания сотрудников на предприятии в рабочее и нерабочее время определяет руководство, проставляя цифровой знак на удостоверении или пропуске. Образцы удостоверений и пропусков разрабатывает служба безопасности и утверждает руководство предприятия.

Утвержденные образцы удостоверений личности, пропусков, оттисков цифровых знаков, печатей (штампов), проставляемых на удостоверениях и пропусках, списки с образцами подписей руководителей или уполномоченных лиц, имеющих право подписывать удостоверения и пропуска, передаются начальнику отдела режима и охраны под расписку.

Удостоверения и постоянные пропуска могут выдаваться лицам, не работающим на данном предприятии, по отдельному, утвержденному руководством, списку с указанием учреждения, должности, фамилии, имени, отчества и сопроводительных помет. Эти документы должны постоянно храниться в бюро пропусков (или у уполномоченного лица) и выдаваться посетителю в момент его прибытия. После завершения работы эти лица сдают документы в бюро пропусков.

Удостоверения и постоянные пропуска выдаются указанным лицам на основании письменных ходатайств руководителей учреждений, где они состоят в штате.

Временные пропуска с фотографиями на срок до трех месяцев выдаются лицам, работающим временно или прикомандированным. Временные пропуска без фотографии на срок до одного месяца действуют при предъявлении паспорта (удостоверения личности) предъявителя. Продление действия временных пропусков допускается на срок не более двух месяцев.

Удостоверения или постоянные пропуска выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат.

Разовый пропуск действителен в течение 30 минут с момента выдачи до входа в здание, а также в течение 15 минут после отметки на пропуске о времени ухода посетителя из предприятия. Руководитель подразделения, в котором находится посетитель, обязан на обороте разового пропуска сделать отметку о времени ухода посетителя и расписаться с указанием своей фамилий полностью.

Материальные пропуска выдаются лицом, ответственным за сохранность материальных средств.

Учет бланков удостоверений и пропусков, их оформление и выдача осуществляет бюро пропусков в соответствующих учетно-контрольных документах.

Для оформления всех видов пропусков в бюро пропусков должны быть следующие печати и штампы:

- круглая (диаметр 25 мм) или треугольная каучуковая печать для разовых и материальных пропусков;

- круглая рельефная металлическая или каучуковая печать для удостоверений и постоянных пропусков (диаметр 20 мм);

- штампы цифровых знаков.

В журнале учета печатей и штампов предприятия против оттиска каждого штампа или печати делается описание его содержания и назначения [26].

2.3 Обеспечение охраны объектов предприятия

Обеспечение безопасности стационарных объектов представляет собой многогранный процесс реализации охранных мероприятий по большей части предупреждающего характера.

В основе разработки системы защиты объекта и организации ее функционирования лежит принцип создания последовательных рубежей безопасности, в которых угрозы должны быть своевременно обнаружены, а их распространению будут препятствовать надежные преграды. Такие рубежи должны располагаться последовательно, от забора вокруг территории объекта до главного, особо важного помещения, такого, как хранилище материальных ценностей и коммерческой тайны.

Эффективность системы защиты оценивается в зависимости от времени, прошедшего с момента возникновения угрозы до начала ее ликвидации. Чем более сложна и разветвлена система защиты, тем больше времени требуется на ее преодоление и тем больше вероятность того, что угроза будет обнаружена, определена, отражена и ликвидирована.

Режим охраны объекта по времени может иметь круглосуточный, частичный (определенные часы суток) или выборочный характер. В зависимости от количества используемых сил и средств, плотности контроля территории и объекта режим охраны может быть простым или усиленным.

На значительной части охраняемых объектов охранники присутствуют круглосуточно. В дневное время контролируют посетителей, прибывающих на объект, осуществляют контрольно-пропускной режим, а в ночное время осуществляют закрытую охрану объекта, принимая на себя полную ответственность за его сохранность. Некоторые объекты охраняются лишь эпизодически, т.е. выборочно по времени. К таким объектам относятся квартиры, охраняемые в период отсутствия хозяина, временные хранилища или территории на период завоза товарно-материальных ценностей и др.

Существует несколько видов охраны:

- охрана с помощью технических средств с подключением на пульт централизованного наблюдения с установкой автоматической сигнализации;

- охрана путем выставления постов (силами отдела охраны или силами милиции);

- комбинированная охрана.

Эффективный режим охраны призван обеспечить сохранность зданий и помещений на объекте, сохранность и контроль за перемещением материальных ценностей и людей, предупредить утечку информации о деятельности объекта, поддерживать противопожарную безопасность.

Основные принципы режима охраны:

- активность и предупредительный характер охраны, что заключается в опережающем выявлении признаков готовящейся атаки объекта и своевременном принятии мер по ее предупреждению или пресечению (отражению);

- целесообразность и обоснованность организации режима охраны объекта, своевременность его усиления, рациональное использование сил и средств охраны;

- разумное сочетание собственных возможностей и возможностей сил правоохранительных органов для обеспечения безопасности объекта;

- осуществление охраны по единому плану;

- скрытность или демонстративность охраны в зависимости от ситуации, складывающейся вокруг охраняемого объекта;

- максимальная информированность охраны обо всех событиях, происходящих на объекте, условиях коммерческих сделок фирмы и т.п. для правильного определения ключевого звена, воздействие на которое позволяет обеспечить безопасность объекта охраны.

В деятельности подразделений охраны по обеспечению безопасности выделяются две группы задач режима охраны объекта:

- аналитические и предупредительные;

- процедурно-отражательные.

Аналитические задачи решаются путем систематического сбора информации о субъектах преступной деятельности и состояний собственного режима охраны. Главным здесь является соблюдение принципов непрерывности и постоянства сбора информации.

Решение предупредительных задач связано в первую очередь с созданием имиджа сильного и надежного режима охраны. Подобный имидж может быть создан серией имитационных мероприятий, демонстрирующих «неудачные» попытки посягательства на объект, и мощное противодействие охраны преступникам. Все это может быть дополнено впечатляющей демонстрацией элементов режима охраны (внушительного вида охранники, современная охранная сигнализация, присутствие милиции на объекте и т.д.). Предупредить покушение на охраняемый объект можно

также путем его маскировки, перекрытия информационных каналов о его деятельности и дезинформацией конкурентов и криминальных элементов о характере деятельности, форме собственности, состоянии режима охраны, объеме имеющихся на объекте товарно-материальных ценностей и т.д.

Процедурно-отражательные задачи режима охраны объекта решаются путем своевременного обнаружения признаков готовящегося посягательства с последующим его отражением предварительно подготовленными силами и средствами. Как правило, подобное мероприятие (операцию) следует проводить во взаимодействии с сотрудниками органов внутренних дел, которые будут иметь возможность своевременно зафиксировать следы преступной деятельности. В тех случаях, когда время начала посягательства трудно предугадать, имеет смысл иногда «подтолкнуть» преступников к началу посягательства. Это может быть достигнуто путем дезинформирования криминальных элементов о времени и месте ввоза ценных грузов, крупной суммы денег и т.п.

При организации охраны объекта служба безопасности должна предусмотреть в перечне служебных обязанностей охранников варианты их действий на случай возникновения на объекте или поблизости от него различного рода критических ситуаций [26].

Контрольные вопросы:

1. Назовите основные задачи службы безопасности по организации режима и охраны на предприятии.
2. Назовите принципы режима охраны предприятия.
3. Перечислите пропускные документы, использующиеся на режимном предприятии.

ТЕМА №3. Организация службы экономической безопасности на предприятии

3.1 Цель, задачи и функции службы экономической безопасности

Под службой экономической безопасности предприятия понимается структурное подразделение, которое организует администрация режимного объекта для обеспечения должного уровня безопасности экономических, технико-технологических, правовых, коммерческих, физических и режимных компонентов предприятия.

Служба экономической безопасности является структурной единицей, которая непосредственно участвует в работе предприятия. Служба экономической безопасности является важнейшим элементом ком-

плексной системы экономической безопасности субъекта предпринимательства [26].

Формирование службы экономической безопасности предприятия производится на основе разработанных документов (устава и инструкций), в которых сформулированы цели, задачи и обязанности службы.

Структуру и штаты службы экономической безопасности определяет руководитель предприятия в зависимости от объема работ и особенностей деятельности. Назначение на должность начальника службы экономической безопасности предприятия, а также его освобождение производит руководитель предприятия.

Целью деятельности службы экономической безопасности является своевременное выявление и нейтрализация причин и условий, способствующих утечке коммерческой тайны, нанесению материального, морального ущерба предприятию (организации) и препятствующих его развитию в рыночных условиях [26].

Основные задачи службы безопасности определяются необходимостью достижения этой цели и представляют собой требования к осуществлению мер по следующим направлениям:

- обеспечение защиты имущественной собственности предприятия;
- обеспечение безопасности персонала предприятия;
- обеспечение защиты коммерческой тайны на предприятии;
- обеспечение безопасности коммерческой деятельности предприятия.

К числу основных задач службы экономической безопасности можно также отнести [24]:

- разработку и осуществление профилактических мероприятий по защите финансовых и других операций;
- сбор, обработку, хранение и анализ официальной и конфиденциальной информации в отношении контрагентов и деловых интересов предприятия, с целью предупреждения сделок с недобросовестными контрагентами;
- организацию и проведение мероприятий по обеспечению безопасности персонала предприятия, основных фондов и финансовых активов в различных условиях повседневной деятельности и в экстремальных ситуациях;
- проведение работ по защите информации на предприятии;

- внедрение нормативных актов по организации охраны помещений предприятия, взаимодействию с охранной фирмой, представителями МВД;

- проведение единой технической политики в вопросах охраны;

- контроль, выполнение требований подразделениями предприятия по вопросам, входящим в компетенцию службы;

- проведение инструктажа и обучения работников предприятия правилам работы с конфиденциальной информацией.

К основным функциям службы экономической безопасности на предприятия относятся следующие:

- организационно-управленческая - заключается в участии службы в создании и поддержании эффективного функционирования структуры, управляющей процессом обеспечения безопасности, а также гибких временных структур по отдельным направлениям работы, в организации взаимодействия и координации между отдельными звеньями системы для достижения поставленных целей;

- административно-распорядительная - реализуется путем подготовки решений по установлению и поддержанию системы безопасности, определению полномочий, прав, обязанностей и ответственности должностных лиц по вопросам обеспечения безопасности объекта;

- планово-производственная - реализуется в разработке комплексной программы и отдельных подсистемных целевых планов обеспечения безопасности объекта, подготовке и проведению мероприятий по их осуществлению, установлению и поддержке режимов безопасности;

- социально-кадровая - подразумевает участие службы в подборе и расстановке персонала, изучении причин и локализации возможных конфликтов, выявлении предпосылок социальной напряженности, инструктаже сотрудников по вопросам своей компетенции, контроле за соблюдением правил режима и безопасности;

- организационно-техническая - осуществляется путем материально-технического и финансового обеспечения системы безопасности объекта, освоением специальной техники и достижений соответствующего потребностям обеспечения безопасности уровня, содействием в освоении новых видов техники для специальной деятельности;

- учетно-контрольная - реализуется выделением наиболее важных направлений финансово-коммерческой деятельности и работой по организации своевременного обнаружения внешних и внутренних угроз финансовой стабильности и устойчивости объекта, оценкой их источников, налаживанием контроля за критическими ситуациями, ведением учета негативных факторов, влияющих на безопасность объекта, а также

накоплением информации о недобросовестных конкурентах, ненадежных партнерах, лицах и организациях, посягающих на жизненно важные интересы объекта;

- хозяйственно-распорядительная - реализуется путем участия службы безопасности в определении ресурсов, необходимых для решения задач безопасности объекта, в подготовке и проведении мероприятий по обеспечению сохранности имущества, финансовой, интеллектуальной и иной собственности.

- научно-методическая - реализуется накоплением и освоением опыта обеспечения безопасности, организацией обучения штатного контингента объекта, научной разработки возникающих проблем обеспечения безопасности и методического сопровождения деятельности в этой сфере.

- информационно-аналитическая заключается в целенаправленном сборе, накоплении и обработке информации, относящейся к сфере безопасности, создании и использовании необходимых для этого технических и методических средств аналитической обработки информации, организации информационного обеспечения заинтересованных подразделений и отдельных лиц в сведениях, имеющихся в службе безопасности.

3.2 Роль и особенности построения службы экономической безопасности на предприятии

Структура службы экономической безопасности и ее штаты определяются в соответствии с целями, функциями и задачами обеспечения безопасности предприятия. Ее деятельность должна быть направлена на комплексное решение поставленных задач на основе разработанной стратегии и применения взаимосвязанных тактических приемов подготовки и проведения мероприятий по обеспечению безопасности.

Предлагаемые структурные единицы должны осуществлять разработку режимов безопасности, установление и поддержание этих режимов, а также контроль за их соблюдением. Они могут включать подструктуры экономической разведки, внутренней безопасности, физической защиты для действий в критических ситуациях и т.п.

В составе службы экономической безопасности могут быть образованы информационно-аналитические и вспомогательные подразделения, а также другие организационные звенья по направлениям обеспечения безопасности, созданы временные структуры с привлечением компетентных специалистов фирмы для решения сложных комплексных задач обеспечения безопасности, определяемых конкретными целями и складывающейся обстановкой.

Для крупных предприятий, которые имеют многочисленный персонал, высокорентабельное производство, применяют высокие технологии, необходимо формирование собственной службы экономической безопасности, включающей в себя несколько подразделений. Возможный вариант построения организационной структуры службы экономической безопасности на крупном предприятии представлен на рис. 1.3.1

Рис. 1.3.1 Пример построения организационной структуры службы экономической безопасности на крупном предприятии [24].

Представленные на рисунке подразделения предприятия в совокупности обеспечивают решение задач по различным направлениям, таким как:

- охрана материальных ценностей;
- защита коммерческой тайны;
- работа с персоналом;
- обеспечение безопасности коммерческой деятельности.

В том случае, если предприятие небольшое, то целесообразно либо использовать услуги соответствующих охранных фирм, либо формировать собственную службу экономической безопасности, но с более простой структурой.

Структура службы экономической безопасности предприятия может состоять из двух подразделений - информационно аналитического и оперативного отдела.

В задачи информационно-аналитического отдела могут быть включены следующие:

- сбор информации из открытых источников, создание собственных информационных массивов и баз данных;
- разработка рекомендаций по совершенствованию системы экономической безопасности;
- организация информационного взаимодействия СЭБ с единой информационной службой предприятия;
- поддержание деловых контактов с сотрудниками министерств и ведомств, представителями деловых и научных кругов;
- выполнение сотрудниками требований к конфиденциальности информации.

К задачам оперативного отдела могут относиться следующие:

- сбор информации из нетрадиционных источников (охранные агентства, охранные бюро и др.) и ее первичную обработку;
- разработка рекомендаций по совершенствованию системы экономической безопасности с использованием информационных возможностей службы экономической безопасности;
- проведение мероприятий по компрометации наиболее агрессивных конкурентов, использующих «грязные» и криминальные методы против предприятия;
- работа с должниками по погашению задолженностей в случае невозврата долгов.

Служба экономической безопасности предприятия может также состоять из нескольких групп и отделений. Подобная структура службы экономической безопасности предприятия представлена на рис. 1.3.2. При этом выделенные блоки непосредственно входят в службу экономической безопасности, а остальные - только в пределах вопросов, находящихся в компетенции службы.

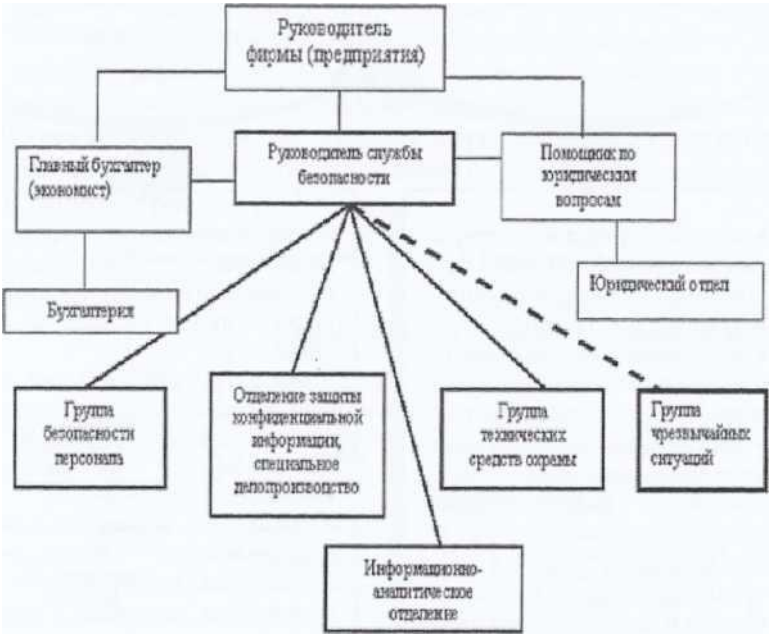

Рис. 1.3.2 - Пример организационной структуры службы экономической безопасности, включающей нескольких групп и отделений [24]

Взаимоотношения службы экономической безопасности со службами и подразделениями предприятия определяются специальным уставом и организационно-распорядительными документами по вопросам этих отношений, которые оформляются соответствующими приказами и распоряжениями руководства предприятия.

Ответственность службы экономической безопасности перед руководством предприятия, его подразделениями и трудовыми коллективами определяется в соответствии с функциями. За результаты своей работы она и ее сотрудники несут юридическую, материальную и дисциплинарную ответственность.

Создание правовых условий заключается в разработке, толковании и реализации норм права, установлении пределов их действия, в формировании необходимых правоотношений, определении и обеспечении правомерного поведения персонала предприятия по отношению к его криминологической безопасности.

Организационные условия формируются путем разработки, построения и поддержания высокой работоспособности общей организационной структуры управления процессом выявления и подавления криминальных угроз деятельности предприятия, использования эффективного механизма стимулирования ее оптимального функционирования, соответствующей подготовки кадров.

Материальные условия формируются за счет выделения и использования финансовых, технических, кадровых, интеллектуальных, информационных и иных ресурсов, обеспечивающих своевременное выявление, ослабление и подавление внешних и внутренних источников угрозы, предотвращение и локализацию возможного ущерба и создание благоприятных возможностей и условий деятельности предприятия.

Служба безопасности осуществляет свою деятельность на основании собственного комплексного плана обеспечения и поддержания высокого уровня безопасности объекта, который может включать целевые программы:

- обеспечения и поддержания внутренней и внешней экономической безопасности;
- организации защиты коммерческой тайны;
- деятельности по предупреждению негативных процессов в коллективах;
- обеспечения физической безопасности персонала объекта.

Главная форма планирования деятельности службы экономической безопасности - годовой план, включаемый в общий план развития предприятия и сбалансированный с ним, с последующей конкретизацией этого плана по месяцам.

Концепция перспективного развития и планы деятельности службы безопасности рассматриваются, обсуждаются, утверждаются и контролируются руководством предприятия.

Важной частью работы службы экономической безопасности и ее подразделений является организация системы внутренней безопасности предприятия, которая включает в себя четко действующий механизм выявления источников информации структур организованной преступности, промышленного шпионажа среди сотрудников объекта.

Мероприятия по организации защиты коммерческой тайны обеспечиваются имеющимися на предприятии финансовыми, кадровыми и материально-техническими ресурсами спецотдела службы экономической безопасности по защите коммерческой тайны. На него возлагаются обязанность разработки и совершенствования нормативной базы, определе-

ние и организация защиты коммерческой тайны, создание методик и определение стратегии применения соответствующих режимных мер.

Важным подразделением службы экономической безопасности в условиях развития современных информационных технологий может быть группа инженерно- технической защиты конфиденциальной информации предприятия.

Кадровый состав службы экономической безопасности целесообразно формировать из лиц, ранее служивших в органах государственной безопасности, органах внутренних дел, вооруженных силах, которые по своим деловым и физическим данным могут осуществлять интеллектуальную, техническую и физическую защиту экономической безопасности предприятия.

Функциональные обязанности сотрудников службы обусловлены кругом задач, которые определяет руководство предприятия. Основным принципом наделения тех или иных работников службы специальными функциями является их компетентность.

Каждый сотрудник службы экономической безопасности должен иметь перечень своих задач и знать способы их решения, отвечать за то, что непосредственно вменено ему в обязанность.

Управление системой обеспечения экономической безопасности предприятия осуществляет первый руководитель через специально создаваемую в этих целях службу экономической безопасности, которая, являясь исполнительно-распорядительным органом, обеспечивает функциональное управление структурными звеньями объекта в интересах комплексного решения задач в сфере безопасности.

Работа службы экономической безопасности не ограничивается одними лишь функциями обеспечения всех видов безопасности. Для повышения эффективности системы корпоративной безопасности необходима оценка взаимозависимости между портфелем возможных рисков предприятия и продвижением бизнеса. Сотрудники службы экономической безопасности так же должны всегда находится на передовом крае бизнеса, реагируя на новые тенденции в нем. Как следствие, их круг обязанностей будет постоянно меняться.

В современных условиях сотрудники службы экономической безопасности должны уметь хорошо ориентироваться в делах предприятия, владеть финансовым и экономическим анализом, методами программно-целевого планирования и проектного управления, выполнять информационно-аналитическую работу, анализировать риски, обеспечивать защиту информационных ресурсов, организовывать создание и эксплуатацию сложных комплексов инженерной защиты объектов предприятий.

Таким образом, при осуществлении комплекса мероприятий по обеспечению экономической безопасности на предприятии важное внимание необходимо уделять вопросам построения и совершенствования организационной структуры службы экономической безопасности.

Контрольные вопросы:

1. Назовите основные цель и задачи службы экономической безопасности на предприятии.
2. Перечислите основные функции службы экономической безопасности на предприятии.
3. Из каких подразделений может состоять служба экономической безопасности крупного предприятия? Обоснуйте ответ.
4. Какие задачи могут решать работники информационно-аналитического отдела службы экономической безопасности?
5. Какие условия формируются на предприятии по результатам деятельности службы экономической безопасности?

ТЕМА №4 Финансовая безопасность предприятия

4.1 Сущность финансовой безопасности предприятия

Процессы глобализации, структурные изменения в экономике, усиливающаяся конкуренция, высокий уровень неопределенности макросреды обуславливают возрастающую актуальность обеспечения экономической безопасности как государства в целом, так и отдельных предприятий.

Одной из ключевых функциональных составляющих экономической безопасности является финансовая безопасность. Проблема ее обеспечения на сегодняшний день актуальна в теории и практике современного финансового менеджмента, как на микро, так и на макроуровне.

Финансовая безопасность является одной из важнейших составляющих экономической безопасности предприятия, в силу того, что финансовые ресурсы занимают ведущее звено в процессе деятельности предприятия.

Первоначальное понятие финансовой безопасности, которое рассматривалось, как обеспечение условий сохранения коммерческой тайны и других секретов предприятия в начале 90-х годов прошлого века, с развитием рыночных отношений постепенно сменилось другим подходом к определению понятия «финансовой безопасности предприятия».

Под «финансовой безопасностью» стали понимать такое состояние предприятия, которое обеспечивает способность противостоять неблагоприятным внешним воздействиям. В связи с этим финансовая безопас-

ность предприятия стала рассматриваться намного шире - как возможность обеспечения его устойчивости в разнообразных, в том числе и в неблагоприятных условиях, которые складываются во внешней среде, независимо от характера ее влияния на деятельность предприятия, масштаба и характера внутренних изменений. Так, финансовая безопасность предприятия определена как «защищенность его деятельности от негативных воздействий внешней среды, а также как способность быстро устранить различные вариантные угрозы или приспособиться к существующим условиям, которые не сказываются негативно на его деятельности» [3].

На сегодня среди ученых нет единого мнения относительно определения категории «финансовая безопасность» предприятия. Достаточно часто финансовую безопасность рассматривают как систему защиты от возможных финансовых потерь и предупреждения банкротства предприятия, направленную на достижение наиболее эффективного использования корпоративных ресурсов. Сущность финансовой безопасности предприятия заключается в способности самостоятельно разрабатывать и проводить финансовую стратегию, в условиях неопределенности и конкуренции.

С.Г. Килинкарова, С.О. Кибизова отмечают, что нередко ставиться знак равенства между понятием «финансовой безопасности» и «финансовой устойчивости [14]. Так, Е.А. Филимонова финансовую устойчивость применяет к фиксации финансовых отношений, рассматриваемых с позиции статики, то есть насколько система сохраняет свои параметры и способность выполнять свои функции при воздействии со стороны различных факторов [28].

Учитывая выше сказанное, предлагаем понимать под финансовой безопасностью предприятия систему финансовой защиты от негативного влияния внешних и внутренних факторов и постоянное выявление, и использование внутренних финансовых резервов для его развития.

Финансовую безопасность предприятия предлагается рассматривать как меру гармонизации во времени и пространстве экономических интересов предприятия с интересами связанных с ним субъектов внешней среды, действующих за пределами предприятия.

Таким образом, понятие финансовой безопасности предприятия является комплексным и затрагивает практически все функциональные сферы деятельности предприятия, и при оценке финансовой безопасности ряд положений оценки пересекается с отдельными видами деятельности предприятия. Это касается, прежде всего, формулировка стратегических интересов предприятия и их количественной интерпретации. Эти поло-

жения оценки финансовой безопасности затрагивают область стратегического управления предприятием, и если на предприятии разработаны и приняты к реализации соответствующие функциональные стратегии (инновационная, ресурсная, инвестиционная, маркетинговая), то их цели должны корреспондироваться с формулировкой стратегических интересов предприятия в рассматриваемой функциональной области деятельности, а показатели, характеризующие цели стратегии, должны соответствовать количественной оценке стратегических интересов предприятия.

4.2 Критерии финансовой безопасности предприятия

Главной целью обеспечения финансовой безопасности предприятия является управление совокупностью финансовых рисков в целях их нейтрализации и минимизации негативных последствий их осуществления.

К наиболее важным критериальным характеристикам финансовой безопасности предприятия можно отнести [7]:

1. Объемы финансовых ресурсов предприятия.
2. Источники формирования финансовых ресурсов предприятия.
3. Направления и объемы использования финансовых ресурсов предприятия.
4. Соотношение доходов и расходов предприятия.
5. Соотношение объемов внутренних и внешних источников формирования финансовых ресурсов предприятия.
6. Выбранная стратегическая и оперативно-тактическая модель финансирования активов предприятия.
7. Уровень финансового риска и объемы формируемой прибыли предприятия.
8. Качество формируемой прибыли и ее достаточность для самофинансирования предприятия.
9. Доля и качество заемных средств в составе финансовых ресурсов предприятия.
10. Наличие резервов и способность предприятия быстро обеспечить мобилизацию финансовых ресурсов из различных, прежде всего внутренних, источников.
11. Гибкость системы финансового планирования предприятия.
12. Способность финансовой системы предприятия к необходимым изменениям под влиянием внешней и внутренней среды.

Выделенные критериальные характеристики финансовой безопасности для предприятия могут быть либо позитивными, либо нейтральными,

либо негативными. Исходя из этого положения очень важно точно знать позитивные, нейтральные или негативные для предприятия те или иные критериальные характеристики. Это можно определить по следующей схеме (табл. 1.4.1).

Таблица 1.4.1

Значения критериальных характеристик финансовой безопасности предприятия [7].

Критериальные характеристики	Значения		
	Позитивные	Нейтральные	Негативные
1	2	3	4
1. Объемы финансовых ресурсов предприятия.	большие	средние	ограниченные
2. Источники формирования финансовых ресурсов предприятия.	различные источники	несколько источников	один источник
3. Направления и объемы использования финансовых ресурсов предприятия.	на развитие производства (бизнеса)	производство =потребление	на потребление
4. Соотношение доходов и расходов предприятия.	>1	=1	<1
5. Соотношение объемов внутренних и внешних источников формирования финансовых ресурсов предприятия.	>1	=1	<1
6. Выбранная стратегическая и оперативно-тактическая модель финансирования активов предприятия.	смешанная	компромиссная	агрессивная
7. Уровень финансового риска и объемы формируемой прибыли	прибыль доминирует над риском	прибыль и риск уравновешены	риск доминирует над прибылью
8. Качество формируемой прибыли и ее достаточность для самофинансирования предприятия.	объем прибыли от основной деятельности достаточен для самофинансирования	объем прибыли от разных видов деятельности не достаточен для самофинансирования	доминируют убытки, самофинансирование не возможно

Продолжение табл. 1.4.1

1	2	3	4
9. Доля и качество заемных средств в составе финансовых ресурсов предприятия.	в составе заемных финансовых ресурсов преобладают долгосрочные заемные средства (60 и более %)	в составе заемных финансовых ресурсов соотношение краткосрочных и долгосрочных финансовых ресурсов примерно равное (по 50 %)	в составе заемных финансовых ресурсов преобладают краткосрочные заемные средства (60 и более %)
10. Наличие резервов и способность предприятия быстро обеспечить мобилизацию финансовых ресурсов из различных, прежде всего внутренних, источников.	достаточные резервы, есть возможность быстро мобилизовать средства	резервы имеются, возможность мобилизации средств ограничена	возможность мобилизации средств отсутствует
11. Гибкость системы финансового планирования предприятия.	высокая гибкость	средняя гибкость	жесткие планы
12. Способность финансовой системы предприятия к необходимым изменениям под влиянием внешней и внутренней среды.	высокая	средняя	отсутствует

Таким образом, если критериальные характеристики имею позитивное значение для предприятия, то уровень его финансовой безопасности достаточен. Если критеральные характеристики имеют нейтральное значение, то финансовая безопасность предприятия неустойчивая. Если критериальные характеристики имеют негативное значение для предприятия, то фактически предприятие не имеет финансовой безопасности.

4.3 Угрозы финансовой безопасности предприятия

Финансовая безопасность может быть обеспечена только на основе устойчивого финансового развития предприятия, в которой созданы условия для реализации финансового механизма, способного адаптиро-

ваться к изменяющимся условиям внутренней и внешней среды. Основными этапами обеспечения финансовой безопасности предприятия, являются следующие:

– определение угроз, влияющих на финансовую и производственную деятельность предприятия с последующей их формализацией;

– разработка механизмов и мер идентификации угроз финансовой безопасности предприятия;

– построение системы ограничений, основанной на использовании индикаторов (критериев) уровня угрозы финансовой безопасности предприятия;

– формирование механизмов и мер обеспечения финансовой безопасности предприятия, нейтрализующих или смягчающих воздействие внешних и внутренних угроз.

Внешние угрозы не зависят от деятельности предприятия, они относятся к факторам риска окружающей среды. Предприятие не имеет возможности ликвидировать угрозу, но может и должно разработать защитные механизмы, позволяющие минимизировать негативные последствия. Внутренние угрозы связаны с деятельностью самого предприятия и в значительно большей степени подлежат корректировке и предупреждению, чем внешние. Внутренние угрозы вызваны преднамеренными или случайными ошибками менеджмента в области управления финансами предприятия.

Таблица 1.4.2

Угрозы финансовой безопасности предприятия [34]

Внешние угрозы финансовой безопасности предприятия	Внутренние угрозы финансовой безопасности предприятия
1	2
Неблагоприятные макроэкономические условия: кризис денежной и финансово-кредитной систем	Неквалифицированное управление, ошибки или отсутствие стратегического планирования
Неблагоприятные условия кредитования предприятий, изменение процентных ставок по кредитам	Отсутствие на предприятии текущего финансового планирования
Нестабильность валютного курса или ограничения в проведении валютных операций	Недостаточная ликвидность активов предприятия
Природные катаклизмы	Неконкурентная ценовая политика
Неблагоприятная криминогенная обстановка в регионе, в том числе в финансово-кредитной сфере	Устаревшее или недостаточное техническое вооружение предприятия и связанные с этим перебои в работе
Нестабильность налоговой, кредитной и страховой политики	Низкий уровень квалификации основного персонала

Продолжение табл.1.4.2

1	2
Недостаток средств для инвестирования в регионе, низкий уровень инвестиционной активности	Ошибки в организации сохранности финансовых и материальных ценностей
Неразвитость рынков капитала и их инфраструктуры	Утечка стратегической и финансовой информации предприятия, недостатки в организации работы службы безопасности предприятия
Уровень инфляции и прогноз инфляции	Низкий уровень бизнес-репутации предприятия
Недобросовестная конкуренция на рынке	Отсутствие планирования деятельности предприятия в аварийных ситуациях
Неустойчивость нормативно-правовой базы	Несоблюдение контрактов и договорных обязательств

Перечисленные в табл. 1.4.2 возможные угрозы представляют собой неполный список. В зависимости от специфики работы предприятия или региона расположения он будет дополняться и конкретизироваться, учитывая определенную ситуацию. Проведя анализ возможных внешних и внутренних угроз, на предприятии следует разработать и реализовать комплексный подход к формированию финансовой безопасности предприятия, обеспечивающей защиту его финансовых интересов в процессе развития.

Для обеспечения финансовой безопасности на предприятии следует определить систему количественных и качественных показателей, позволяющих оценить текущий и перспективный уровень финансового состояния предприятия. Каждому виду финансового состояния предприятия будут соответствовать нормальные ограничения значений количественных показателей и набор качественных показателей, обеспечивающий стабильную защищенность финансовых интересов от идентифицированных реальных и потенциальных угроз внешнего и внутреннего характера. Количественные показатели целесообразней представить в виде индикаторов (критериев), отвечающих особенностям изучаемого объекта и позволяющих проводить диагностику и анализ финансовой безопасности предприятия.

Анализ выявленных отклонений и повлиявших на них факторов позволит оценить степень влияния на конечные результаты финансовой деятельности предприятия. По итогам проведенного анализа будет констатироваться уровень финансовой безопасности предприятия и близость полученных значений к кризисному финансовому состоянию. Максимальная степень финансовой безопасности достигается, если все показа-

тели находятся в пределах допустимых границ и нормальные значения одного показателя достигаются не за счет ухудшения другого показателя. Предприятие выстраивает алгоритм действий, направленных на поддержание финансовой безопасности и обеспечивающих ему принятие таких мер и шагов, которые не допустят возникновения кризисной финансовой ситуации. Планирование финансовой безопасности осуществляется на основе разработки нескольких альтернативных сценариев развития ситуации и выбора, на основании проведенных расчетов лучшего варианта. Управление финансовой безопасностью разделяется на два временных направления: возможный набор решений для реагирования на текущие проблемы и разработку стратегии финансовой безопасности с горизонтом планирования на три-пять лет. Постоянное соблюдение условий финансовой безопасности позволит предприятию стабильно функционировать и достичь поставленных целей деятельности в будущем [34].

Контрольные вопросы:

1. Охарактеризуйте понятие финансовой безопасности с разных точек зрения.
2. В чем заключаются принципиальные различия категорий «финансовая безопасность» и «финансовая устойчивость»?
3. Перечислите и охарактеризуйте основные критерии финансовой безопасности предприятия.
4. Назовите внешние угрозы финансовой безопасности предприятия?
5. Назовите внутренние угрозы финансовой безопасности предприятия?

ТЕМА №5. Технико-технологическая безопасность предприятия

5.1 Сущность технико-технологической безопасности предприятия

Технико-технологический уровень экономики зависит от двух факторов – инвестиций и инноваций.

Инвестиционный процесс – это составная часть общественного воспроизводства. Инвестиции – это долгосрочные вложения капитала в производство.

Источники инвестиции делятся на собственные средства и заемный капитал. Инвестиции делятся на прямые (непосредственное вложение денег в развитие бизнеса, оборудование, персонала) и портфельные (покупка ценных бумаг на фондовом рынке).

Обеспечение инвестиционных аспектов устойчивости развития экономики становится одним из условий стабилизации ситуации в экономике.

В условиях рыночной экономики общественная востребованность инноваций проявляется как обычный платежеспособный спрос на них. Значимость производственных инвестиций состоит в том, что они повышают производительность труда и за счет создания более качественного продукта позволяют предприятию удерживать лидерство в конкурентной борьбе.

Научно-технологический потенциал предприятия представляет собой совокупность имеющихся средств и возможностей по внедрению новой техники, технологий, совершенствованию предметов труда, форм и методов организации производства и труда с целью увеличения эффективности работы предприятия.

Технологические нововведения, особенно современные формы автоматизации и информационных технологий, оказывают самое существенное влияние на уровень и динамику эффективности производства продукции. По принципу цепной реакции они вызывают существенные (нередко коренные) изменения в техническом уровне и производительности технологического оборудования, методах и формах организации трудовых принципов, подготовке и квалификации кадров. Повышение эффективности производства в значительной степени зависит от лучшего использования основных фондов.

В России на инновационное развитие средств у предприятий не хватает по той причине, что невелик пока еще спрос на выпускаемую ими продукцию, а чтобы производить конкурентную продукцию высокого качества, на которую будет спрос, нужна модернизация производства, что требует больших финансовых вложений [20].

Одним из основных источников инвестиций в инновации являются накопления самих предприятий, которые складываются из части прибыли и амортизационных отчислений. Однако для технологического обновления производства внутренних накоплений предприятия, как правило, не хватает.

Сущность технико-технологической безопасности предприятия заключается в том, насколько уровень используемых на данном предприятии технологий соответствует лучшим мировым аналогам. Важным моментом здесь является и проблема наличия у этих технологий потенциала развития и их будущей конкурентоспособности с технологиями заместителями, чье влияние на технологическое развитие современной экономики возрастает с каждым днем.

Для предприятий материальной сферы обеспечение технико-технологической безопасности включает в себя следующие основные этапы:

1. Анализ рынка технологий по производству продукции, аналогичной профилю данного предприятия.

2. Анализ собственных технологических процессов предприятия, нахождение внутренних ресурсов улучшения используемых технологий.

3. Разработка технологической стратегии развития данного предприятия, включающей в себя:

- определение перспективных товаров;
- планирование комплекса технологий для производства этих товарных позиций;
- планирование бюджета на технологическое развитие предприятия;
- разработка общего плана технологического развития предприятия.

4. Оперативная реализация планов технического развития предприятия в процессе осуществления его хозяйственной деятельности.

5. Анализ результатов от применения мер по обеспечению технико-технологической составляющей экономической безопасности предприятия [8].

Процесс обеспечения технико-технологической безопасности предприятия нематериальной сферы тесно связан с обеспечением кадровой и информационной составляющих, т.к. меры по обеспечению технико-технологической составляющей касаются работы по повышению квалификации сотрудников, сбора и анализа информации по данной проблеме.

Важнейшие показатели, характеризующие технико-экономическую эффективность технологического процесса на предприятии:

- расход сырья, полуфабрикатов и энергии на единицу продукции; количество и качество
- получаемой готовой продукции, изделий; уровень производительности труда;
- интенсивность процесса;
- затраты на производство;
- себестоимость продукции, изделий.

При определении состояния технико-технологической безопасности предприятия используют традиционно включаемые для оценки производственного потенциала критерии, в частности:

- количество продаваемых и покупаемых предприятием лицензий;
- количество имеющихся в распоряжении предприятия патентов;
- соотношение получаемых и уплачиваемых лицензионных выплат;

- процент выпускаемой продукции, соответствующей лучшим мировым аналогам;

- аналогичный показатель соответствия мировым аналогам по используемым на предприятии видам технологического оборудования;

- процент выпускаемой продукции предприятия, защищенной патентами, принадлежащими данному предприятию;

- удельный вес технологического оборудования предприятия, разработанного на предприятии и защищенного патентами предприятия;

- удельный вес оборудования, приобретенного на основе лицензионных договоров.

Каждая технология, будучи определенной последовательностью операций, позволяющих достичь заранее заданного результата, характеризуется некоторой совокупностью входных и выходных параметров. Среди выходных параметров выделяется так называемый технологически значимый результат - параметр, определяемый функциональным назначением продукта труда, производимого согласно данной технологии.

5.2 Индикаторы технико-технологической безопасности предприятия

Оценка уровня экономической безопасности организации по всем функциональным составляющим на основе статистических методов обработки информации сильно затруднена из-за того, что большинство аспектов данной проблемы крайне сложно поддается математической формализации, а некоторые из них не поддаются и вовсе. Тем не менее, важность данной проблемы для эффективного функционирования организаций очень велика, поэтому необходимо оценивать уровень экономической безопасности предприятия на основе определения критериев.

Технико-технологическую безопасность предприятия, как составляющую экономической безопасности характеризуют соответствующие индикаторы. Пока не сложился единый подход к определению индикаторов технико-технологической безопасности, однако, специалисты советуют разделять их по следующим направлениям: [9].

- реновация и воспроизводство основных производственных фондов (ОПФ);

- эффективность использования ОПФ;

- степень износа ОПФ;

- интенсивность обновления технологии;

- научно-производственная новизна используемой техники и технологии;

- конкурентоспособность.

Принимая во внимание приведенные направления индикаторов, характеризующих элементы производственной сферы, к системе показателей технико-технологической безопасности необходимо отнести следующие:

- фактический уровень загрузки производственных мощностей;
- ритмичность производственного процесса;
- возрастная структура и технический ресурс оборудования;
- степень износа ОПФ;
- фондоотдача ОПФ;
- коэффициент выбытия ОПФ;
- коэффициент обновления ОПФ;
- доля НИОКР в общем объеме работ;
- процент продукции и технологий, соответствующих лучшим мировым аналогам или превосходят их и др.

Необходимо отметить, что для технико-технологической безопасности важное значение имеют не столько сами показатели, сколько их пороговые значения. В большинстве индикаторов не существует единых предельных значений. Для каждого конкретного случая можно установить свои границы и критерии для величин показателей, однако общие тенденции должны быть подобными для аналогичных показателей. В зависимости от характера показателя предельные значения могут иметь явное (численное) или неявное (описательное) выражение.

Для оценки технико-технологической безопасности предприятия рекомендуются индикаторы, представленные в табл. 1.5.1 [10].

Таблица 1.5.1

Индикаторы технико-технологической безопасности предприятия

Название индикатора	Методика расчета	Оптимальная величина / тенденция
1	2	3
Фондоотдача (руб./руб.)	$Ф_о$ = объем реализации продукции / среднегодовую стоимость основных фондов	Тенденция к увеличению. Нижняя граница – величина базисного периода, достигнутого на предприятии, или базисного значения по проекту
Фондовооруженность труда (руб./чел.)	$Ф_в$ – среднегодовая стоимость основных фондов / численность ППП	Тенденция к увеличению не столько за счет уменьшения численности персонала, сколько за счет наращивания объемов технического потенциала

Продолжение табл.1.5.1

Коэффициент выбытия основных фондов, доля единицы	$К_{выб.}$ = стоимость выбывших за год основных фондов /стоимость основных фондов на начало года	Тенденция к увеличению
Коэффициент обновления основных фондов, доля единицы	$К_{обн.}$ = стоимость введенных основных фондов /стоимость основных фондов на начало года	Тенденция к увеличению
Коэффициент износа основных фондов, доля единицы	$К_{изн.}$ = Стоимость износа основных фондов / первоначальная стоимость основных фондов	Меньше 50%, тенденция к уменьшению
Материалоемкость (руб./руб.)	$М_е$ = Величина материальных затрат / Объем реализации продукции	10-30%, тенденция к уменьшению
Коэффициент полезного использования материалов (руб./руб.)	$К_{п.и.м.}$ = Величина материальных затрат - стоимость отходов / Величина материальных затрат	Стремится к 1,0
Коэффициент брака (руб./руб.)	Кбр. – Стоимость брака/себестоимость реализованной продукции	1,0-3,0%, тенденция к сокращению
Средний срок использования наличного оборудования (лет)	-	5 лет, тенденция к уменьшению
Штрафы за некачественную продукцию	-	Тенденция к сокращению

К негативным воздействиям на технико-технологическую безопасность предприятия относят:

- действия, направленные на подрыв технологического потенциала предприятия;
- нарушение технологической дисциплины;
- моральное старение используемых технологий.

Кроме того, выделяют внешние и внутренние угрозы технико-технологической безопасности. Так, к внешним угрозам технико-технологической безопасности предприятий относят:

- повышение цен на ресурсы, отсутствие надежных поставщиков ресурсов, что повышает себестоимость выпускаемой продукции;

- отсутствие внешних и внутренних инвестиций, что не дает возможность своевременно обновлять используемую технику и технологии.

Внутренними угрозами технико-технологической безопасности предприятия являются неэффективная организация производственного процесса, недостаточная квалификация работников, неэффективное управление оборотными средствами, высокая степень износа основных фондов.

Тенденция роста износа основных фондов требует обновления техники и технологий, используемых на предприятиях. Проблемы с эффективностью использования материальных ресурсов также стимулируют внедрение в производство новых технологических процессов и техники. Основой обеспечения технико-технологической безопасности предприятия должна быть их активная инновационная деятельность, а, следовательно, инновационное развитие [20].

Таким образом, результаты активной инновационной деятельности обеспечивают технико-технологическую безопасность предприятия, поскольку способствуют повышению эффективности использования основных фондов и материальных ресурсов, обновлению активной части основных фондов, увеличению фондоотдачи и снижению материалоемкости, сокращению брака, а, следовательно, и штрафов за некачественную продукцию. В свою очередь, это повышает экономическую безопасность предприятия и способствует эффективному экономическому развитию.

5.3 Способы обеспечения технико-технологической безопасности предприятия

Для обеспечения технико-технологической безопасности предприятия необходимо применение комплекса мер правового, экономического, организационного, инженерно-технического и социально-психологического характера:

- реализация мер противодействия всем видам шпионажа;
- предупреждение переманивания сотрудников предприятия, обладающих конфиденциальной информацией;
- всестороннее изучение деловых партнеров и конкурентов;
- своевременное выявление и адекватное реагирование на дезинформационные мероприятия;
- разработка и совершенствование правовых актов предприятия, направленных на обеспечение его безопасности;
- реализация мер по защите коммерческой и иной информации;

- реализация мер по защите интеллектуальной собственности;

- выявление негативных тенденций среди персонала предприятия, информирование о них руководства предприятия и разработка соответствующих рекомендаций;

- организация взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;

- возмещение материального и морального ущерба, нанесенного предприятию в результате неправомерных действий организаций и отдельных лиц.

Для предотвращения экономических преступлений существует немало мер. Выделим основные из них:

а) технические меры – защита от несанкционированного доступа к документации предприятия, перестрахование информационных ресурсов в случае внештатных ситуаций, принятие конструкционных мер защиты от хищений, саботажа, взрывов, диверсий, установка сигнализации и многое другое;

б) организационные меры – охрана предприятия, тщательный подбор персонала, наличие определенной стратегии предприятия, возложение ответственности на лиц, которые должны обеспечить безопасность предприятия и т.д.;

в) правовые меры – разработка норм, устанавливающих ответственность за преступления в сфере информационных технологий, защита авторских прав, совершенствование уголовного и гражданского законодательства, судопроизводства и др.

Следует обратить внимание на то, что не на всех предприятиях используется независимый, общественный контроль со стороны государственных органов за инновационно-техническими разработками. Значение независимого контроля за важнейшими инновационными разработками выходит далеко за рамки отдельно взятого предприятия. Однозначно, такой контроль необходим на всех предприятиях, т.к. ошибки в технических расчетах могут привести к последствиям, имеющим социальное значение.

Несомненно, использование традиционных мер контроля является недостаточным, нужно искать новые формы для защиты предприятия от экономических преступлений. Постараемся сформулировать основные принципы, которые могут быть использованы при разработке процедур контроля по экономической безопасности предприятия:

- использование технических средств для контроля;

- ознакомление представителей других предприятий с технологией производства своей продукции;

- взаимное информирование об архитектуре построения компьютеризированных систем, их характеристиках, а также обо всех фактах их несанкционированного поведения;

- установление контроля по периметру особо важных объектов;

- проведение плановых инспекций на местах.

Естественно, что любые найденные решения в этой области не являются всеобъемлющими. Поэтому достигнутое соглашение должно предусматривать, по мере приобретенного опыта, возможность внесения в него изменений или дополнений. Важна здесь не столько выработка полностью надежных мер контроля, сколько установление контакта в части предотвращения экономических преступлений.

К данной проблеме необходимо подходить креативно и, конечно, более интенсивно. Есть немало примеров, когда такой подход приводил к желаемым результатам.

Дополнительные сложности возникают при создании службы экономической безопасности в связи с необходимостью тщательного выбора сотрудников: только надежные, высокомотивированные специалисты, обладающие надлежащей квалификацией, могут привлекаться к обеспечению безопасности работы предприятия. По словам американских исследователей Аржана Сингха и Эндрю Буршгенса, служба экономической безопасности на предприятии, начиная с момента формирования, проходит четыре стадии: от примитивного реагирования на команду «фас» до полной интеграции в процесс принятия решений.

Факторы успеха службы экономической безопасности:

а) руководство должно выступать в роли субъекта, задающего вектор в деятельности службы;

б) работа службы должна быть основана на тщательно продуманных и удобных для применения методиках, позволяющих оперативно обрабатывать поступающую информацию.

Сбор информации – процесс непрерывный, который начинается с систематизации уже имеющихся в распоряжении компании данных;

в) работа службы должна носить систематический и хорошо структурированный характер;

г) должен быть обеспечен доступ всех сотрудников к единой базе данных (системе «корпоративного знания»).

Наиболее эффективный принцип практической работы – разбивка целей на подзадачи и легко выполнимые операции, что обуславливает достижение наилучших результатов в кратчайшие сроки.

В процессе выполнения отдельных задач служба безопасности должна следовать стратегической цели.

С первого дня работы службы безопасности необходимо обеспечить ее взаимодействие с отделом реализации продукции предприятия.

Необходимо четко определить круг прав и обязанностей сотрудников службы безопасности (составить четкие должностные инструкции).

Служба экономической безопасности на предприятии не должна находиться во враждебной оппозиции к остальному персоналу компании (хотя одной из функций и должна быть проверка лояльности сотрудников). Эффективность деятельности службы безопасности – один из залогов успешного процветания предприятия.

Контрольные вопросы:

1. В чем заключается сущность понятия технико-технологическая безопасность предприятия?
2. Назовите основные этапы обеспечения технико-технологической безопасности на предприятия.
3. Перечислите основные индикаторы для оценки уровня технико-технологической безопасности предприятия.
4. Перечислите внешние и внутренние угрозы технико-технологической безопасности предприятия.
5. Какие меры могут быть использованы для обеспечения технико-технологической безопасности предприятия?
6. Назовите и охарактеризуйте основные направления предотвращения экономических преступлений на предприятии.
7. Перечислите основные принципы, которые могут быть использованы при разработке процедур контроля по экономической безопасности предприятия.

ТЕМА №6. Обеспечение информационной безопасности предприятия

6.1 Сущность информационной безопасности предприятия

Проблемы обеспечения информационной безопасности в России сегодня в большей степени рассматривается на национальном уровне. Области исследования информационной безопасности предприятий, уделяется меньше внимания, несмотря на то, что предприятия являются основным звеном в экономике любого государства, которое подвержено информационным рискам.

Многие проблемы информационной безопасности связаны с недооценкой важности такой угрозы, как конфиденциальность информации. В результате для предприятия это может обернуться банкротством. Даже единичный случай халатности персонала предприятия может принести ему многомиллионные убытки, потерю репутации фирмы и доверия клиентов. Чтобы этого избежать, специалисты службы безопасности предприятия используют специальное оборудование, производящее анализ электромагнитных излучений, получаемых во время работы на компьютере.

В общем виде под информационной безопасностью предприятия понимают защиту информации предприятия от случайного или умышленного несанкционированного доступа и тем самым причинения вреда нормальному процессу деятельности [19].

В свою очередь С. В. Петров, трактует информационную безопасность предприятия как «состояние защищенности информации от несанкционированного доступа, модификации, разрушения и раскрытия» [31].

В. Ф. Шаньгин определяет информационную безопасность как «состояние защищенности информационной среды предприятия, способное обеспечить его функционирование и устойчивое развитие» [19].

Зачастую понятие информационной безопасности связывают с категорией информационные риски. В. Ф. Шаньгин рассматривает информационный риск как «возможность возникновения ущерба в виде убытков в результате применения предприятием информационных технологий» [25].

А. А. Замула полагает, что риск информационной безопасности представляет собой «вероятность того, что некоторая информационная угроза сможет воспользоваться уязвимостью группы активов или отдельно взятого актива предприятия, тем самым нанеся ему значительный ущерб» [32].

Прежде всего, информационные риски связаны с приемом, получением, обработкой, хранением и дальнейшим использованием информации предприятия с помощью различных средств связи и электронных носителей.

На практике понятие «риск» принимают за понятие «угроза» или считают, что они являются синонимами. По мнению О. А. Крыжановского под угрозой в целом понимается «потенциальная возможность наступления неблагоприятного события, которое способно повредить механизмы защиты или воздействовать непосредственно на ценный ресурс, что

непременно приведет к негативным последствиям для деятельности предприятия» [20].

В свою очередь под информационной угрозой понимают «вероятное событие, которое с помощью воздействия на информацию или другие компоненты информационной системы предприятия может привести к нанесению ущерба» [19].

Угрозы информационным активам предприятия могут быть вызваны внутренними (программные и аппаратные сбои в работе оборудования, халатность сотрудников службы экономической безопасности, использование незащищенных каналов связи и т.д.) и внешними (стихийные бедствия, хакерские атаки, обострение конкуренция и т.д.) факторами [20].

Необходимо отметить, что информационные риски могут переходить в категорию информационных угроз при определенных условиях, что позволяет рассматривать их как потенциальные угрозы для экономической безопасности предприятия в целом.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается ее уязвимость: с одной стороны, возможность уничтожения или искажения информации (т.е. нарушение ее физической целостности), а с другой – возможность несанкционированного использования информации (т.е. опасность утечки информации ограниченного пользования). Второй вид уязвимости вызывает особую озабоченность пользователей ЭВМ.

Так, безопасность данных включает обеспечение достоверности данных и защиту данных и программ от несанкционированного доступа, копирования, изменения.

Под угрозой безопасности автоматизированных систем обработки информации понимают возможность воздействия на информационную систему, которое прямо или косвенно может нанести ущерб её безопасности.

При этом защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Основными каналами “*утечки”* информации являются:

1. Прямое хищение носителей и документов.

2. Запоминание или копирование информации.

3. Несанкционированное подключение к аппаратуре и линиям связи или незаконное использование "законной" (т.е. зарегистрированной) аппаратуры системы (чаще всего терминалов пользователей).

4. Несанкционированный доступ к информации за счет специального приспособления математического и программного обеспечения.

6.2 Современные методы обеспечения информационной безопасности

Полноценное обеспечение информационной безопасности на предприятии должно быть стандартизировано и находиться под полным контролем круглогодично, в реальном времени, в круглосуточном режиме. При этом система учитывает весь жизненный цикл информации, начиная с момента появления и до полного ее уничтожения или потери значимости для предприятия [24].

К настоящему времени разработано много различных средств, методов, мер и мероприятий, предназначенных для защиты информации. Сюда входят *аппаратные* и *программные* средства, *криптографическое* закрытие информации, *физические* меры (различные устройства и сооружения, а также мероприятия, которые затрудняют или делают невозможным проникновение потенциальных нарушителей в места, в которых можно иметь доступ к защищаемой информации), *организационные* мероприятия (нормативно-правовые акты, которые регламентируют процессы функционирования системы обработки данных, использование ее устройств и ресурсов, а также взаимоотношение пользователей и систем таким образом, что несанкционированный доступ к информации становится невозможным или существенно затрудняется), *законодательные* меры.

Технологии обеспечения информационной безопасности можно подразделить на две группы:

- 1-я группа - защищающие программные и аппаратные средства для обработки и хранения информации от отказов, нарушений, способных возникнуть в результате случайной ошибки;
- 2-я группа - защищающие программные и аппаратные средства обработки информации от всевозможных преднамеренных угроз, которые заранее планируются злоумышленниками.

Классификация мер по защите информации в соответствии с п. 1 ст. 16 Федерального закона № 149-ФЗ представляет собой сочетание правовых, организационных и технических мер. При широкой трактовке понятия защита информации, которое в этом случае правильнее заменить на сочетание "*информационная безопасность*", в перечень мер защиты должны быть включены и физические меры защиты.

Таким образом, охарактеризуем основные меры по защите информации:

Законодательные меры защиты информации.

Законодательные меры занимают около 5% объема средств, расходуемых на защиту информации. Это меры по разработке и практическому

применению законов, постановлений, инструкций и правил эксплуатации, контроля как аппаратного, так и программного обеспечения компьютерных и информационных систем, включая линии связи, а также все объекты инфраструктуры, обеспечивающие доступ к этим системам. В России деятельность в информационной сфере регулируют более 1000 нормативных документов. Уголовное преследование за преступления в этой сфере осуществляется в соответствии с гл. 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации», содержащей три статьи.

1. Ст. 272 – несанкционированный доступ к информации. *Несанкционированный доступ к информации* – нарушение установленных правил разграничения доступа с использованием штатных средств, предоставляемых ресурсами вычислительной техники и автоматизированными системами (сетями). Отметим, что при решении вопроса о санкционированности доступа к конкретной информации необходимо наличие документа об установлении правил разграничения доступа, если эти правила не прописаны законодательно.

2. Ст. 273 – создание, использование и распространение (включая продажу зараженных носителей) вредоносных программ для ЭВМ, хотя перечень и признаки их законодательно не закреплены. *Вредоносная программа* – специально созданная или измененная существующая программа, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или их сети.

3. Ст. 274 – нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Это – нарушение работы программ, баз данных, выдача искаженной информации, а также нештатное функционирование аппаратных средств и периферийных устройств; нарушение нормального функционирования сети, прекращение функционирования автоматизированной информационной систем в установленном режиме; сбой в обработке компьютерной информации.

Уголовное преследование за незаконные действия с общедоступной информацией осуществляется в соответствии со ст. 146 «Нарушение авторских и смежных прав» и 147 «Нарушение изобретательских и патентных прав» гл. 19 «Преступления против конституционных прав и свобод человека и гражданина» Уголовного кодекса РФ.

Ответственность за соблюдением сотрудниками организации или компании законодательных мер по защите информации лежит на каждом сотруднике организации или компании, а контроль за их соблюдением – на руководителе.

Аппаратные методы защиты информации.

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. Наибольшее распространение получили:

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;
- устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты;
- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (*криптографические методы*).

Криптографическое закрытие (шифрование) информации заключается в таком преобразовании защищаемой информации, при котором по внешнему виду нельзя определить содержание закрытых данных.

К шифрам, предназначенным для закрытия информации в ЭВМ и автоматизированных системах, предъявляется ряд требований, в том числе: достаточная стойкость (надежность закрытия), простота шифрования и расшифровывания, способ внутримашинного представления информации, нечувствительность к небольшим ошибкам шифрования, возможность внутримашинной обработки зашифрованной информации, незначительная избыточность информации за счет шифрования и ряд других. В той или иной степени этим требованиям отвечают некоторые виды шифров замены, перестановки, гаммирования, а также шифры, основанные на аналитических преобразованиях шифруемых данных.

Особенно эффективными являются комбинированные шифры, когда текст последовательно шифруется двумя или большим числом систем шифрования (например, замена и гаммирование, перестановка и гаммирование). Считается, что при этом стойкость шифрования превышает суммарную стойкость в составных шифрах.

Каждую из рассмотренных систем шифрования можно реализовать в автоматизированной системе либо программным путем, либо с помощью специальной аппаратуры. Программная реализация по сравнению с аппа-

ратной является более гибкой и обходится дешевле. Однако аппаратное шифрование в общем случае в несколько раз производительнее.

Физические меры защиты информации.

Физические меры (доля 15-20%) обеспечивают ограничение физического доступа к компьютеру, линии связи, телекоммуникационному оборудованию и контроль доступа. Физические меры защиты направлены на управление доступом физических лиц, автомобилей, грузов в охраняемую зону, а также на противодействие средствам агентурной и технической разведки. Эти меры включают: охрану периметра, территории, помещений; визуальное и видеонаблюдение; опознавание людей и грузов; идентификацию техники; сигнализацию и блокировку; ограничение физического доступа в помещения.

Выделяют три основные макрофункции физической защиты (рис. 1.6.1):

- внешнюю защиту;
- опознавание;
- внутреннюю защиту.

Рис. 1.6.1. Основные макрофункции физической защиты

Перечисленные средства служат для обнаружения угроз и оповещения сотрудников охраны или персонала объекта о появлении и нарастании угроз.

Из 12 разбитых по функциональному признаку групп более детально рассмотрим четыре группы, использующие в своей технической реализации собственные компьютерные средства либо пригодные для защиты самих рабочих помещений с компьютерами.

Охранная сигнализация. Основной элемент сигнализации – датчики, фиксирующие изменение одного или нескольких физических параметров, характеристик.

Датчики классифицируют по следующим группам:

- объемные, позволяющие контролировать пространство помещений, например, внутри компьютерных классов;
- линейные, или поверхностные, для контроля периметров территорий, зданий, стен, проемов (окна, двери);
- локальные, или точечные, для контроля состояния отдельных элементов (закрыто окно или дверь).

Датчики устанавливаются, как открыто, так и скрытно. Наиболее распространены:

- выключатели (размыкатели), механически или магнитным способом замыкающие (размыкающие) управляющую электрическую цепь при появлении нарушителя. Бывают напольные, настенные, на касание;
- инфраакустические, устанавливаемые на металлические ограждения для улавливания низкочастотных колебаний, возникающих во время их преодоления;
- датчики электрического поля, состоящие из излучателя и нескольких приемников. Выполняются в виде натянутых между столбами проводов-кабелей. Изменение поля при появлении нарушителя и фиксируется датчиком;
- инфракрасные датчики (излучатель – диод либо лазер), используемые для сканирования поверхностей или объемов помещений. Тепловая “фотография” запоминается и сравнивается с последующей для выявления факта перемещения объекта в защищаемом объеме;
- микроволновые – сверхвысокочастотный передатчик и приемник;
- датчики давления, реагирующие на изменение механической нагрузки на среду, в которой они уложены или установлены;
- магнитные датчики (в виде сетки), реагирующие на металлические предметы, имеющиеся у нарушителя;

- ультразвуковые датчики, реагирующие на звуковые колебания конструкций в области средних частот (до 30— 100 кГц);
- емкостные, реагирующие на изменение электрической емкости между полом помещения и решетчатым внутренним ограждением при появлении инородного объекта.

Средства оповещения и связи. Всевозможные сирены, звонки, лампы, подающие постоянный или прерывистые сигналы о том, что датчик зафиксировал появление угрозы. На больших расстояниях используют радиосвязь, на малых специальную экранированную защищенную кабельную разводку. Обязательное требование – наличие автоматического резервирования электропитания средств сигнализации.

Охранное телевидение. Распространенное физическое средство защиты. Главная особенность – возможность не только фиксировать визуально факт нарушения режима охраны объекта и контролировать обстановку вокруг объекта, но и документировать факт нарушения, как правило, с помощью видеомагнитофона.

В отличие от обычного телевидения, в системах охранного ТВ монитор принимает изображение от одной или нескольких видеокамер, установленных в известном только ограниченному кругу лиц месте (так называемое закрытое ТВ). Естественно, что кабельные линии для передачи сигналов охранного ТВ не должны быть доступны иным лицам, кроме охраны. Мониторы располагаются в отдельных помещениях, доступ в которые должен быть ограничен.

Рассмотренные выше три группы относятся к категории средств обнаружения вторжения или угрозы.

Естественные средства противодействия вторжению. Сюда относятся естественные или искусственные барьеры (водные преграды, сильно пересекающаяся местность, заборы, спецограждения, особые конструкции помещений, сейфы, запираемые металлические ящики для компьютеров и т.п.).

Средства ограничения доступа, в состав которых входит компьютерная техника. Сюда относятся биометрические или иные, использующие внешние по отношению к компьютеру носители паролей или идентифицирующих кодов, пластиковые карты, флеш-карты, таблетки Touch Memory и другие средства ограничения доступа.

Биометрические средства ограничения доступа. Особенность биометрических методов допуска состоит в их статистической природе. В процессе проверки объекта при наличии ранее запомненного кода устройство контроля выдает сообщение по принципу “совпадает” или “не совпадает”. В случае считывания копии биологического кода и его срав-

нения с оригиналом речь идет о вероятности ошибки, которая является функцией чувствительности, разрешающей способности и программного обеспечения контролирующего доступ прибора. Качество биометрической системы контроля доступа определяется следующими характеристиками:

- вероятностью ошибочного допуска “чужого” ошибка первого рода;
- вероятностью ошибочного задержания (отказа в допуске) “своего” легального пользователя – ошибка второго рода;
- временем доступа или временем идентификации;
- стоимостью аппаратной и программной частей биометрической системы контроля доступа, включая расходы на обучение персонала, установку, обслуживание и ремонт.

Большая часть биометрических средств защиты реализована на трех компонентах: сканер (датчик) – преобразователь (сигналы датчика в цифровой код для компьютера) компьютер (хранитель базы биометрических кодов – характеристик объекта, сравнение с принятой от датчика информацией, принятие решения о допуске объекта или блокировании его доступа).

В качестве уникального биологического кода человека в биометрии используются параметры двух групп:

- *Поведенческие*, основанные на специфике действий человека, – это тембр голоса, подпись, индивидуальная походка, клавиатурный почерк. Главный недостаток поведенческих характеристик – временная неустойчивость, т.е. возможность значительного изменения со временем. Это в значительной степени ограничивает применение поведенческих характеристик как средств ограничения доступа. Однако на протяжении относительно короткого временного интервала они применимы как идентифицирующие личность средства. Пример – фиксация клавиатурного почерка работающего в процессе осуществления им сетевой атаки и последующий (после задержания злоумышленника) контрольный набор определенного текста желательно на изъятой у него клавиатуре (лучше на его же компьютере).

- *Физиологические*, использующие анатомическую уникальность каждого человека, – радужная оболочка глаза, сетчатка глаза, отпечатки пальцев, отпечаток ладони, геометрия кисти руки, геометрия лица, термограмма лица, структура кожи (эпителия) на пальцах на основе ультразвукового цифрового сканирования, форма ушной раковины, трехмерное изображение лица, структура кровеносных сосудов руки, структура ДНК, анализ индивидуальных запахов. Справедливости ради отметим, что

большая часть перечисленных биометрических средств пока не производится в массовых масштабах.

Пластиковые карты. Лидером среди переносных носителей персональных идентификационных кодов (PIN) и кодов физического доступа остаются пластиковые карты.

Пластиковая карта представляет собой пластину стандартных размеров (85,6x53,9x0,76 мм), изготовленную из специальной устойчивой к механическим и термическим воздействиям пластмассы. Основная функция пластиковой карты обеспечение идентификации владельца карты как субъекта системы физического доступа или платежной системы.

По принципу действия карты делятся на две группы – пассивные и активные.

Пассивные карты только хранят информацию на носителе, но не обеспечивают ее автономной обработки. Пример – широко распространенные во всем мире карты с магнитной полосой на обратной стороне. Данный вид карт уязвим для мошенничества, поэтому, например, системы Visa и MasterCard/Europay используют дополнительные средства защиты карт голограммы и нестандартные шрифты для эмбоссирования.

Активные пластиковые карты содержат встроенную микросхему и допускают разную степень обработки информации. Типичный пример – карты-счетчики и карты с памятью. Но они уступают место интеллектуальным или смарт-картам.

Смарт-карты (англ. smart card) – пластиковые карты со встроенной микросхемой (англ. integrated circuit card, ICC – карта с интегрированными электронными цепями). В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти. Кроме того, смарт-карты, как правило, обладают возможностью проводить криптографические вычисления.

Назначение смарт-карт – одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.

Смарт-карты находят всё более широкое применение в различных областях, от систем накопительных скидок до кредитных и дебетовых карт, студенческих билетов, телефонов стандарта GSM и проездных билетов.

Однако, например, имеются случаи искажения информации, хранимой в смарт-картах, а также нарушения их работоспособности за счет воздействия высокой или низкой температуры, ионизирующих излучений и т.п. Данный вид карт обладает высокой надежностью и вытесняет другие виды карт.

Программные методы защиты информации

Программная защита информации – система специальных программ, включаемых в состав программного обеспечения, реализующих функции защиты информации. Защитный программный код может выступать как отдельно, в качестве отдельного защитного программного продукта, так и включаться в состав других, многофункциональных программ, с целью защиты обрабатываемых ими данных или самозащиты от вредоносного кода. Так как защитные функции многофункциональных программ зачастую даже не имеют существенных средств самозащиты и по определению проигрывают специализированному защитному программному обеспечению, любая значимая компьютерная система требует развёртывания и полноценной интеграции программных средств защиты информации на всех или хотя бы самых уязвимых элементах системы.

Программная защита является наиболее распространенным видом защиты, чему способствуют такие положительные свойства данного средства, как универсальность, гибкость, простота реализации, практически неограниченные возможности изменения и развития и т.п.

Так, Не следует путать программную защиту информации с защитой компьютеров от несанкционированного использования или защитой сети компьютеров, не смотря на то, что их функции во многом пересекаются. При использовании данного подхода защищается сама информация, будь то операционная система, специализированное программное обеспечение или некий документ в цифровом виде. При этом такая защита подразделяется на защиту данных и защиту программ.

Полноценная программная защита информации на сервере или рабочем компьютере требует использования различных типов защитных программ или специализированных защитных решений, совмещающих в себе несколько типов защиты одновременно.

Например, важно понимать, что господствующий на данный момент антивирусный подход, обычно объединяющий в себе антивирусы, антишпионы, анти-эксплуататоры и анти-модификаторы, недостаточен против целевых атак, так как он основан на сравнении программного кода с имеющимися у производителя сигнатурами вредоносного кода. Имеющаяся в некоторых случаях возможность применения поведенческого анализа также не даёт гарантии сохранности данных и сохранения работоспособности системы. Аналогично, контроль доступа сам по себе не способен гарантировать использование программ и данных исключительно имеющими право на это лицами, так как помимо программных уязвимостей такой тип защиты может быть «вскрыт» обычной социальной инженерией без использования высокотехнологичных способов нападения в

принципе. Системы обнаружения вторжений могут помочь при последующем расследовании инцидента, но без систем предотвращения вторжений повреждения, полученные при атаке, могут оказаться слишком серьёзными, чтобы расследование в принципе понадобилось. Шифрование данных может помочь против попыток украсть эти данные, но не остановит злоумышленника, желающего эти данные уничтожить.

Подобные недостатки узкоспециализированной защиты можно найти в любой комбинации малого числа схожих типов программных средств защиты информации, поэтому защита всегда должна быть основана на множестве параллельных и зачастую пересекающихся алгоритмах. При использовании нескольких решений это чревато внутренними конфликтами в системе, поэтому наиболее логичным выводом является использование комплексных защитных систем, использующих большинство упомянутых типов защиты информации для защиты данных, защиты программ и самозащиты от вторжений, копирования, модификации и уничтожения.

Желательно чтобы защитные программные решения обладали модульной структурой и единым управляющим сервером, что может гарантировать возможность полноценной интеграции в ИТ-инфраструктуру предприятия или организации, при этом защищая именно те области системы, которые защищены слабее всего. Кроме этого необходимо, чтобы программные средства были совместимы с уже установленными защитными решениями сторонних производителей, позволяющие, тем самым, исключить стандартную дилемму построения защищённой инфраструктуры о выборе того или иного производителя решений.

Выделяют следующую классификацию программных средств защиты информации:

По *функциональному назначению* их можно разделить на следующие группы:

- идентификация технических средств (терминалов, устройств группового управления вводом-выводом ЭВМ, носителей информации), задач и пользователей;
- определение прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей;
- контроль работы технических средств и пользователей;
- регистрация работы технических средств и пользователей при обработке информации ограниченного использования;
- уничтожения информации в запоминающем устройстве (ЗУ) после использования;
- сигнализации при несанкционированных действиях;

- вспомогательные программы различного назначения: контроля работы механизма защиты, проставления грифа секретности на выдаваемых документах.

По *назначению программного обеспечения* следует выделить:

- встроенные средства защиты информации. Примером может служить встроенные системы обеспечения безопасности операционных систем-производителей;

- антивирусная программа (антивирус) – программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом;

- специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых решений следует отметить следующие две системы, позволяющие ограничить и контролировать информационные потоки.

- межсетевые экраны (также называемые брандмауэрами или файрволами – от нем. Brandmauer, англ. firewall – “противопожарная стена”). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода – это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

- proxy-servers (proxy – доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вирусы, код Java и JavaScript).

- защищённые сетевые соединения. Примеров может служить технология VPN (Virtual Private Networks – виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно

прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

Кроме этого программные средства защиты информации делятся на такие типы так:

- контроль доступа;
- анти-кейлоггеры;
- анти-шпионы (anti-spyware);
- анти-эксплуататоры (anti-subversion);
- анти-модификаторы (anti-tampering);
- антивирусы;
- шифрование;
- брандмауэры (firewall);
- системы обнаружения вторжений;
- системы предотвращения вторжений;
- песочница.

Организационные (административные) меры защиты информации

Программно-аппаратные средства защиты обязательно должны дополняться организационными (административными) мерами защиты информации.

Так, административные меры (доля 50 – 60%) включают:

- разработку политики безопасности применительно к конкретной информационной системе (какие профили, какие пароли, какие атрибуты, какие права доступа);
- разработку средств управления безопасностью (кто, когда и в каком порядке изменяет политику безопасности);
- распределение ответственности за безопасность (кто и за что отвечает при нарушении политики безопасности);
- обучение персонала безопасной работе и периодический контроль за деятельностью сотрудников;
- контроль за соблюдением установленной политики безопасности;
- разработку мер безопасности на случай природных или техногенных катастроф и террористических актов.

Ответственность за соблюдением в организации или компании организационных (административных) мер по защите информации лежит на руководителе, начальнике службы безопасности (информационной безопасности), системном (сетевом) администраторе.

Кроме этого, отметим, что без постоянной квалифицированной поддержки со стороны администратора даже надёжная программно-аппаратная защита может давать сбои.

В заключение следует отметить, что комплексную защиту организаций сегодня осуществляет значительное количество специализированных охранно-детективных предприятий и служб безопасности. Они проводят различные виды работ по физической, экономической и информационной безопасности, поскольку в современной обстановке без решения этих вопросов любой вид деятельности не сможет быть эффективным и прибыльным [24].

Контрольные вопросы:

1. Охарактеризуете понятие информационная безопасность, информационный риск и защита информации.
2. Перечислите основные каналы утечки информации на предприятии.
3. Назовите основные группы технологий обеспечения информационной безопасности предприятия.
4. Перечислите и охарактеризуйте основные методы защиты информации на предприятии.

РАЗДЕЛ 2. ПРАКТИКУМ.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №1
Основы обеспечения экономической безопасности предприятия

Основные термины и понятия: экономическая безопасность предприятия, кадровая безопасность предприятия, угрозы экономической безопасности предприятия, риски экономической безопасности предприятия.

Основные вопросы для подготовки к занятию:

1. Основные компоненты экономической безопасности предприятия.
2. Внешние угрозы экономической безопасности предприятия.
3. Внутренние угрозы экономической безопасности предприятия.
4. Как соотносятся между собой понятия «угроза», «риск» и «ущерб» в теории экономической безопасности.

Практическое задание №1

Руководитель предложил работнику оплачивать его труд «в конверте». Оцените ситуацию, назвав причины и последствия. Предложите тактику действий работника.

Практическое задание №2

Имеются три предприятия, производственные мощности которых относятся друг к другу в соотношении 2:5:3. Арендная плата, налоги и другие выплаты составляют 1/3 прибыли у первого и второго предприятий и 25 % - у третьего. Какое из предприятий больше всех рискует разориться?

Практическое задание №3

Иностранные инвестиции концентрируются в основном в быстроокупаемых проектах пищевой промышленности, торговли, сферы услуг, а в промышленном производстве их доля сравнительно мала.

Прокомментируйте, почему это происходит? И какое влияние этот момент оказывает на экономическую безопасность предприятия?

Практическое задание №4

Подготовьте памятку по работе с информацией, составляющей коммерческую тайну, работнику предприятия, функционирующего в сфере промышленного производства.

Практическое задание №5

Для разработки программы экономической безопасности на предприятии необходимо иметь по возможности полную информацию об угрозах, рисках, ущербе.

Дайте определения угрозы, риска. Охарактеризуйте основные методики оценки угроз и рисков. Приведите методику оценки ущерба.

Темы рефератов:

1. Методы обеспечения экономической безопасности предприятия.
2. Стратегия обеспечения экономической безопасности предприятия.
3. Анализ и оценка угроз экономической безопасности предприятия.
4. Тема по выбору студента в рамках тематики практического занятия.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №2
Обеспечение режима на предприятии

Основные термины и понятия: режимный объект, пропускной режим, государственная тайна, коммерческая тайна, формы секретности.

Основные вопросы для подготовки к занятию:

1. Цель и задачи отдела режима и охраны на предприятии.
2. Характеристика форм секретности используемых на предприятии.
3. Формы пропускных документов на предприятии.
4. Разовые и материальные пропуска.

Практическое задание №1

Охраной отмечены случаи воровства рабочими слесарного инструмента. Руководство цеха не подтверждает случаи хищения.

Определите причины возникшей ситуации. Сформулируйте оценочные показатели диагностики ситуации. Разработайте мероприятия, исключающие возможность повторения ситуации.

Практическое задание №2

Организация работает с информацией, составляющей государственную тайну, и информацией, являющейся коммерческой тайной.

Дайте сравнительную характеристику государственной и коммерческой тайн. Предложите мероприятия по защите как государственной, так и коммерческой тайн.

Практическое задание №3

В 1983 г. произошло наводнение в юго-западной части США. Причиной стал компьютер, в который были введены неверные данные о погоде, в результате чего он дал ошибочный сигнал шлюзам, перекрывающим реку Колорадо.

Определите круг подозреваемых лиц. Кто, по вашему мнению, должен нести ответственность за ошибку компьютера?

Практическое задание №4

Подготовьте пакет документов, необходимых для организации работы по защите государственной тайны для предприятия, функционирующего в сфере промышленного производства.

Темы рефератов:

1. Методы обеспечения режима на предприятии.
2. Функции службы экономической безопасности в области обеспечения режима и охраны на предприятии.
3. Организация пропускного режима на предприятии.
4. Тема по выбору студента в рамках тематики практического занятия.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №3
Организация службы экономической безопасности на предприятии

Основные термины и понятия: организационная структура, должностные обязанности сотрудников, функции службы экономической безопасности, экономические преступления, проверка контрагентов.

Основные вопросы для подготовки к занятию:

1. Роль и место службы экономической безопасности в общей структуре предприятия.
2. Цель и задачи службы экономической безопасности на предприятии.
3. Методы проверки контрагентов.
4. Обеспечение лояльности персонала предприятия.

Практическое задание №1

Разработайте организационную структуру службы экономической безопасности на предприятии, функционирующем в сфере промышленного производства. Сформулируйте основные требования к начальнику службы экономической безопасности, его должностные инструкции, права и обязанности.

Практическое задание №2

Разработайте схему проверки надежности сторонних организаций, стремящихся установить с предприятием деловые отношения в сфере промышленного производства.

Практическое задание №3

Организация работает с информацией, составляющей государственную тайну, и информацией, являющейся коммерческой тайной. Дайте сравнительную характеристику государственной и коммерческой тайн. Предложите мероприятия по защите как государственной, так и коммерческой тайн.

Практическое задание №4

Описание практической ситуации на тему: «Воспитание лояльности».

Сотрудники пятигорской компании «Босфор», выпускающей окна и двери из ПВХ, начали параллельно работать на конкурентов – передавать им часть заказов. Проведя внутреннюю диагностику, в «Босфоре» пришли к выводу: виновата плохая система мотивации. Но исправить ситуацию пока не получается.

Итак, «Босфор» продает пластиковые окна и двери девять лет и входит в четверку крупнейших игроков этого рынка в Ставропольском крае. Три года назад в регионе резко вырос спрос на строительные и отделочные материалы: начала активно развиваться курортная база, строятся многочисленные коттеджные поселки. Благодаря этому с 2009 г. продажи компании ежегодно росли на 30 %. Естественно, что потенциал края заставил активизироваться всех крупных игроков рынка пластиковых окон дверей и привлек новых. Например, два года назад в Пятигорске появилась компания «Окна плюс», которая также наладила собственное сборочное производство и имеет все шансы стать серьезным конкурентом. Чтобы не сдавать позиции, «Босфору» нужна сплоченная команда. С этим-то и возникли сложности.

Компания работает с немецкими профилями KBE. Комплектующие закупаются в Германии и на принадлежащем немцам заводе в Воскресенске, а собирается продукция в пятигорском цехе «Босфора». Готовые окна и двери продаются через дилеров и собственное розничное подразделение. Ко многим отделам компании – продаж, монтажных работ – претензий нет. Единственным проблемным звеном были и остаются замерщики.

Подозрения, что некоторые из них «сливают» заказы конкурентам, возникли у руководителя отдела продаж компании «Босфор» Марины Черноусовой давно. Но в этом году, когда начала действовать своя служба безопасности, получили подтверждения. Стали известны случаи, когда замерщики приезжали к потенциальным клиентам и рекомендовали услуги другой компании, которая выполнит проект «быстрее и дешевле». Только в августе на сторону ушло не меньше десятка заказов.

Сколько всего заказов было потеряно из-за этого, в компании посчитать не могут. Но если раньше количество отказов от продолжения сотрудничества с «Босфором» после общения с замерщиком не превышало 3 - 4 % в год, то за последние полгода оно выросло до 10 %.

Первой мыслью было: сразу же выгнать нарушителей. Но потом руководство «Босфора» решило разобраться, почему так происходит, и дать

провинившимся шанс исправиться. Проштрафившиеся объясняли: работаем много, а получаем мало. Дело в том, что в задачи замерщика входит не только техническая работа (собственно замер, калькуляция и т. д.) и составление подробного отчета. Он должен провести небольшую презентацию: рассказать, в чем преимущество предлагаемых «Босфором» профилей, какой вариант подойдет в конкретном случае, насколько серьезная переделка потребуется для установки новых дверей или окон. Если клиент соглашается, далее им занимается менеджер по продажам, который составляет контракт и получает определенный процент.

Замерщикам выплачивается фиксированный оклад 12 - 15 тыс. руб. в месяц при средней нагрузке не менее 150 замеров в месяц. «Это неплохие деньги для нашего региона, – говорит Марина Черноусова. – Кроме того, если сотрудник был сильно загружен и выполнял сложные проекты, ему полагается премия 1,5 - 2 тыс. руб. в месяц или подарок от компании: новые жалюзи, помощь в установке окон или ремонте машины. Решение о поощрении принимала я лично, поскольку владела всей информацией о том, какой объем работы каждый проделал за месяц».

В высокий сезон, начинающийся в мае и заканчивающийся в ноябре, сотрудники получали премии и подарки практически каждый месяц. Но для некоторых это оказалось менее выгодным, чем передать клиента другой компании и получить за это свой процент.

Выяснилось, что в сговоре с замерщиками находились и некоторые дилеры компании: зачастую именно им нечистоплотные замерщики отдавали заказы, а те выставляли цены ниже «Босфора» (в компании признаются, что их цены – не самые низкие на рынке, поскольку включают значительные накладные расходы, которыми небольшие полулегальные артели не обременены). «К сожалению, договориться по-хорошему с дилерами не удалось, а давить на них мы не можем: грозятся уйти к другому производителю, – поясняет Марина Черноусова. – Для нас это потеря денег и брешь, которую наша розничная сеть, продающая всего 40 % произведенной нами продукции, не закроет. На расширение собственной розницы нет средств».

Размышляя над тем, с кем бороться в первую очередь – с внешним врагом или внутренним, в компании все же решили сконцентрироваться на собственном персонале: если у работника не будет стремления увести заказ, то и проблема взаимоотношений с партнерами отпадет сама собой. Создание службы контроля в компании отвергли: она затратна, и не совсем понятен механизм ее работы. «Босфор» решил сделать ставку на разработку эффективной мотивации сотрудников, при которой станет невыгодно работать на конкурента. Первым этапом создания

мотивационной схемы должен был стать отказ от субъективной оценки результатов труда и введение четких стандартов. В качестве основных критериев выбрали дальность поездок (чтобы добраться до клиента, иногда приходится ехать 40-100 км), количество заказов в день и уровень их сложности. Но, как признает Марина Черноусова, четкой шкалы не создали: практически каждый заказ обладал какой-либо спецификой. В итоге вместо стандартов получились приблизительные описания, с помощью которых проблему решить не удалось.

Следующим шагом стало стимулирование рублем. За каждый выезд к клиенту замерщику независимо от результата начали платить дополнительно по 15 руб. Если встреча заканчивалась подписанием договора, гонорар возрастал вдвое. При удачном раскладе выходило около 2 тыс. руб. в месяц.

В какой-то момент в «Босфоре» решили, что неправильно разрабатывать решения наверху, и предложили самим замерщикам придумать критерии оценки и способы стимулирования. Но из этой затеи ничего не вышло. Сотрудники просили увеличить зарплату до тысячи долларов, но при этом четко не могли объяснить, какой объем работ они готовы за эти деньги выполнить. Пока шел обмен мнениями, несколько заказов снова достались конкурентам. Поэтому в конце августа двоих сотрудников пришлось уволить. С одной стороны, это стало примером для остальных. С другой стороны, идти по такому пути в компании не хотят: найти квалифицированную замену не так просто, а обучать неопытных новичков времени нет.

Исчерпав запас идей, в «Босфоре» обратились к практике других игроков: с подобными проблемами в той или иной степени сталкиваются все продавцы пластиковых окон и дверей. Как выяснилось, в крупных компаниях стараются, чтобы замерщик был заинтересован в подписании контракта. Например, он выезжает к клиенту с ноутбуком, на котором установлено программное обеспечение, позволяющее точно рассчитать стоимость проекта, заключает контракт и наряду с менеджером по продажам получает 1 - 3 % от суммы заказа. При этом за день выходит не более двух-трех выездов на место.

Однако «Босфору» такой опыт не подошёл. «У нас нет возможности приобрести ноутбуки всем замерщикам: слишком дорого», – говорит Марина Черноусова. Пока на бизнесе утечка заказов заметно не сказывается: продажи продолжают расти. Но руководство «Босфора» сильно беспокоит то, что страдает имидж компании. У потребителя складывается далеко не самое лучшее впечатление о фирме, если ее же представитель советует обратиться к кому-нибудь другому.

Вопросы:

1. Как сделать, чтобы сотрудники не искали возможности заработать на стороне? В компании считают, что ответ на этот вопрос стоит искать в системе мотивации. Есть и альтернативная идея: контрольные и карательные мероприятия. Создание службы безопасности, внутреннее расследование и увольнение злостных нарушителей – первые шаги в этом направлении.

2. Каким путем идти «Босфору»?

Темы рефератов:

1. Методы оценки эффективности службы (отдела) экономической безопасности на предприятии.

2. Кадровый состав службы (отдела) экономической безопасности на предприятии.

3. Система мотивации сотрудников службы (отдела) экономической безопасности на предприятии.

4. Тема по выбору студента в рамках тематики практического занятия.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №4
Обеспечение финансовой безопасности предприятия

Основные термины и понятия: финансовая безопасность, индикаторы финансовой безопасности, платежеспособность, ликвидность, финансовая устойчивость, внешние и внутренние угрозы финансовой безопасности предприятия, банкротство.

Основные вопросы для подготовки к занятию:

1. Что такое финансовая безопасность предприятия?

2. Какие критерии используются для оценки финансовой безопасности предприятия?

3. В чем разница понятий «платежеспособность» и «ликвидность»?

4. В чем заключаются принципиальные различия категорий «финансовая безопасность» и «финансовая устойчивость»?

5. Какие существуют методы диагностики банкротства предприятия?

Практическое задание №1

Назначенный собственником финансовый менеджер фирмы неэффективно с позиции собственника управляет финансами.

Охарактеризуйте оценочные показатели работы менеджера. Сформулируйте мероприятия, позволяющие взять ситуацию под контроль. Оцените их эффективность.

Практическое задание №2

Оцените вероятность банкротства при помощи двухфакторной Модели, имеющей следующий вид:

$Z = - 0,3877 + К_{ТЛ} (-1,0736) + К_З 0,0579,$

где $К_{ТЛ}$ - коэффициент текущей ликвидности (оборотные активы/краткосрочные обязательства);

- $К_З$ - коэффициент заемных средств (заемный капитал/собственный капитал);

-0,3877 - постоянная величина;

-1,0736 и 0,0579 - соответствующие весовые значения коэффициентов.

Шкала вероятности банкротства:

-если $Z = 0$, то вероятность банкротства равна 50%;

-если $Z < 0$, то вероятность банкротства меньше 50% и далее снижается по мере уменьшения Z;

-если $Z > 0$, то вероятность банкротства больше 50% и возрастает с ростом Z.

Исходные данные для расчета коэффициентов двухфакторной модели вероятности банкротства по данным ООО «КУБ», представлены в табл.2.4.1.

Таблица 2.4.1

Исходные данные для расчета коэффициентов ООО КУБ

Показатели	Код строки	Значения показателей (на конец года)
Оборотные активы, тыс.руб.	290	3696
в т.ч. расходы будущих периодов	216	-
Краткосрочные обязательства, тыс.руб.	690	1215
в т. ч. доходы будущих периодов	640	-
- резервы предстоящих расходов	650	-
Долгосрочные обязательства, тыс. руб.	590	1042
Баланс (по пассиву)	700	5371

Практическое задание №3

На основе данных табл. 2.4.2 проанализируйте ликвидность организации, рассчитав показатели, представленные в табл. 2.4.3, сделайте вывод.

Таблица 2.4.2

Исходные данные

Наименование статей баланса	На начало периода	На конец периода	Темп роста, %
1. Внеоборотные активы	15000	25600	
Оборотные активы 2. запасы	47000	73000	
3. Дебиторская задолженность	5850	7200	
4. Денежные средства	23250	24300	
5. Краткосрочные финансовые вложения	520	840	
Краткосрочные пассивы: 6. краткосрочные кредиты банков	6900	17420	
7. Кредиторская задолженность	43600	65450	

Таблица 2.4.3

Показатели ликвидности организации

Показатели	На начало периода	На конец периода	Темп роста, %
1. Коэффициент срочной ликвидности (4+5) /(6+7) норма: 0,25-0,30			
2. Коэффициент промежуточной ликвидности (3+4+5) / (6+7) норма:0,3-1,0			
3. Коэффициент текущей ликвидности (2+3+4+5) / (6+7) норма:1-2			
4. Собственный оборотный капитал (средства) (2+3+4+5)-(6+7) - СОК			
5. Коэффициент обеспеченности текущих активов собственными средствами (СОК/(2+3+4+5) норма 0,1-0,5			

Темы рефератов:

1. Анализ состояния инвестиционной и финансовой составляющих экономической безопасности предприятия.

2. Анализ и оценка финансовых индикаторов экономической безопасности предприятия.

3. План финансового оздоровления предприятия.

4. Тема по выбору студента в рамках тематики практического занятия.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №5
Обеспечение технико-технологической безопасности предприятия

Основные термины и понятия: технико-технологическая безопасность, индикаторы технико-технологической безопасности, конкурентоспособность, инновации, наукоемкая продукция, коммерческая тайна.

Основные вопросы для подготовки к занятию:

1. Составляющие технико-технологической безопасности предприятия.
2. Критерии оценки технико-технологической безопасности предприятия.
3. Критерии наукоемкости производства.
4. Методы оценки интеллектуальных ресурсов предприятия.
5. Основные положения закона РФ «О государственной тайне» от 21.07.1993 №5485-1.

Практическое задание №1

Проблема экономической безопасности многих промышленных предприятий – это, прежде всего, разумная инвестиционная и инновационная политика. От успешной реализации инновационной политики зависит конкурентоспособность предприятия.

Что на ваш взгляд нужно сделать для преодоления отставания в области новейших научных разработок и технологий?

Практическое задание №2

Рабочие-станочники устраиваются на работу на завод, проходят производственное обучение, получают квалификационный разряд и увольняются с предприятия в течение года.

Оцените ситуацию, выявите причины и возможный ущерб.

Разработайте мероприятия, обеспечивающие закрепление рабочих на предприятии.

Практическое задание №3

Работник, допущенный к работе с конфиденциальной информацией, заявил о своем увольнении.

Оцените ситуацию и возможный ущерб для фирмы.

Сформулируйте мероприятия для нейтрализации ущерба.

Практическое задание №4

Руководством фирмы утвержден перечень документов, содержащих конфиденциальную информацию.

Предложите организационные мероприятия, обеспечивающие безопасный оборот подобных документов.

Практическое задание №5

Многие российские технологии были вытеснены зарубежными, доля финансовых средств, направляемых российскими предприятиями на инновационную деятельность, составляет не более 5%, что в 10 – 15 раз ниже, чем в промышленно-развитых странах. Объем России в мировом объеме торговли гражданской наукоемкой продукцией оценивается лишь в 0,3%. Так, например, в КНР этот показатель составляет 6%.

Объясните с чем это связано, и как это влияет на экономическую безопасность предприятия?

Практическое задание №6

Составьте перечень всех видов коммерческой тайны применительно к предприятию, функционирующему в сфере промышленного производства.

Темы рефератов:

1. Инновации как элемент технико-технологической безопасности предприятия.
2. Методы оценки технико-технологической безопасности предприятия.
3. Формы допуска к государственной тайне.
4. Тема по выбору студента в рамках тематики практического занятия.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №6
Обеспечение информационной безопасности предприятия

Основные термины и понятия: информационная безопасность, индикаторы информационной безопасности, информационные технологии, персональные данные, компьютерные преступления, государственная тайна.

Основные вопросы для подготовки к занятию:

1. Составляющие информационной безопасности предприятия.
2. Критерии оценки информационной безопасности предприятия.
3. Какую информацию можно отнести к персональным данным сотрудников предприятия.
4. Понятие кибер-безопасность предприятия.
5. Промышленный шпионаж и конкурентная разведка. Сходство и различие понятий.

Практическое задание №1

На предприятии широко используются информационные технологии. Для обеспечения информационной безопасности кадровой службе предложено разработать комплекс организационных мероприятий.

Сформулируйте концепцию. Определите основные задачи. Сформулируйте первоочередные меры.

Практическое задание №2

Работник обратился в суд по поводу нарушения сотрудниками отдела кадров предприятия его права на защиту персональной информации (зафиксирована утечка сведений персонального характера).

Оцените ситуацию, определите виновных и причины. Разработайте меры по предотвращению подобных ситуаций.

Практическое задание №3

Произошла на предприятии крупная авария, связанная с программной ошибкой. Кто, по вашему мнению, виноват и какова степень его вины?

Практическое задание №4

Почему раскрытие компьютерного преступления часто бывает связано с чистой случайностью?

Например, однажды сотрудник вычислительного центра, который обслуживал несколько нефтяных компаний, обратил внимание, что у одного из клиентов перед тем, как загорится световой индикатор записи, всегда долгое время светится индикатор считывания. Проведенное расследование показало, что этот человек занимался промышленным шпионажем и продавал данные компании компаниям-конкурентам.

Практическое задание №5

Подготовьте памятку по работе с информацией, составляющей государственную и коммерческую тайну, работнику предприятия, функционирующего в сфере промышленного производства.

Практическое задание №6

Проблемное поле для написания эссе:

В настоящее время одним из самых важных ресурсов предприятия становится информация. Развитие экономики и общества увеличивает потребность в информации. В современном мире роль информации определяется, прежде всего, следующими факторами: глобализацией рынков, усилением ориентации на потребности клиентов, развитием технического прогресса, увеличением подвижности и сложности внешней среды, усилением взаимозависимости различных факторов внешней среды, усложнением системы управления предприятием, ускорением жизненного цикла товара. Как бы Вы сформировали информационную систему предприятия (цель, принципы, этапы, техническое и программное обеспечение, показатели эффективности применения)?

Практическое задание №7

Заполните табл. 2.6.1 , определив основные методы и средства несанкционированного получения информации, а также методы защиты информации.

Таблица 2.6.1

Основные методы несанкционированного получения информации и методы защиты информации.

№	Действия человека (типовая ситуация)	Каналы утечки информации	Методы и средства получения информации	Методы и средства защиты информации
1	Разговор в помещении или на улице			
2	Разговор по мобильному телефону			
3	Разговор по стационарному телефону			
4	Документ на бумажном носителе			
5	Почтовое отправление			
6	Отправление по электронной почте			
7	Передача документа на флэш-накопителе			
8	Производственный процесс			

Темы рефератов:

1. Современные методы защиты информации на предприятии.
2. Кибер-преступления и их последствия.
3. Основные каналы утечки информации на предприятии.
4. Тема по выбору студента в рамках тематики практического занятия.

РАЗДЕЛ 3. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

ЛАБОРАТОРНАЯ РАБОТА №1
Обработка и графическое представление результатов экспресс-диагностики экономической безопасности предприятия

Цель работы: приобретение практических навыков экспресс-диагностики экономической безопасности предприятия, на основе использования экспертной оценки состояния ее элементов с применением прикладных программных продуктов "Prima" и " Microsoft Office ".

Общие положения

Диагностика состояния экономической безопасности предприятия проводится с целью определения характеристик ее элементов и предполагает сбор и анализ большого объема разнообразной информации.

Любое предприятие развивается по рассчитанной траектории в соответствии с определенной целью. Однако в реальной жизни запланированный процесс достижения цели подвергается различным воздействиям внешней и внутренней среды, в связи с чем, возникают отклонения реальной траектории развития, от ранее запланированной. Причем эти отклонения могут иметь как положительное, так и отрицательное влияние на уровень экономической безопасности предприятия. Принимая во внимание данные обстоятельства, состояние экономической безопасности предприятия в целях анализа, можно представить следующей моделью:

$$S = S^N + S^+ + S^-, \qquad (3.1.1)$$

где S^N - подмножество нормальных состояний элементов экономической безопасности предприятия, определенных плановой траекторией развития;

S^+ - подмножество отклонений от плановой траектории, способствующих более высокому уровню развития элементов экономической безопасности предприятия;

S^- – подмножество отклонений от плановой траектории, способствующих развитию кризисного состояния отдельных элементов экономической безопасности предприятия.

В целях диагностики экономическая безопасность предприятия может быть представлена как совокупность элементов.

Исходная информация

Эксперты осуществили оценку уровня элементов экономической безопасности предприятия по 9-балльной шкале. Результаты экспертизы представлены в таблице 1, где введены следующие обозначения:

F_1 - финансовая составляющая;

F_2 - интеллектуально-кадровая составляющая;
F_3 - технико-технологическая составляющая;
F_4 - правовая составляющая;
F_5 – информационная составляющая;
F_6 - экологическая составляющая;
F_7 - силовая составляющая.
S^N следует считать равным 5; $S^N < S^+ \leq 9$; $1 \leq S^- < S^N$

Таблица 3.1.1

Вариант 1 - Экспертные оценки состояния экономической безопасности предприятия

Эксперты/ элементы ЭБП	1	2	3	4	5	6
F 1	2	3	4	5	6	7
F 2	3	4	6	5	5	6
F 3	4	4	5	6	6	6
F 4	4	5	6	6	4	5
F 5	3	4	6	5	6	6
F 6	4	4	5	5	5	6
F 7	4	4	6	6	6	6

Таблица 3.1.2

Вариант 2 - Экспертные оценки состояния экономической безопасности предприятия

Эксперты/ элементы ЭБП	1	2	3	4	5	6
F 1	5	6	6	5	2	5
F 2	6	5	6	6	3	6
F 3	5	5	5	5	3	6
F 4	6	6	6	6	2	6
F 5	5	5	5	5	3	5
F 6	6	6	6	6	3	6
F 7	6	6	6	6	3	2

Таблица 3.1.3

Вариант 3 - Экспертные оценки состояния экономической безопасности предприятия

Эксперты/ элементы ЭБП	1	2	3	4	5	6
F 1	5	6	6	5	2	2
F 2	6	5	6	5	2	3
F 3	5	5	6	5	3	3
F 4	6	6	6	6	3	2
F 5	5	5	5	5	3	3
F 6	6	6	6	5	3	3
F 7	5	5	3	3	5	7

Таблица 3.1.4

Вариант 4 - Экспертные оценки состояния экономической безопасности предприятия

Эксперты/ элементы ЭБП	1	2	3	4	5	6
F 1	5	4	3	2	5	6
F 2	6	4	4	2	5	6
F 3	5	5	3	3	5	7
F 4	6	4	3	3	6	6
F 5	5	4	3	3	5	5
F 6	6	4	3	3	6	6
F 7	5	5	5	5	3	3

Содержание и порядок выполнения работы

1. На основе использования ППП "Prima" провести процедуру ранжирования непосредственных оценок экспертов, сформировать нормированную матрицу и определить согласованность и достоверность мнений экспертов с помощью коэффициента конкордации и критерия Пирсона. Проанализировать полученные показатели, сделать выводы о возможности использования экспертной информации.

2. На основе использования ППП «Microsoft Excel» определить среднюю арифметическую по каждому элементу экономической безопасности предприятия, выявить области отклонения показателей от нормальных параметров. Определить приоритетность проведения клинических исследований по тому или иному элементу экономической безопасности

предприятия посредством ранжирования полученных средних оценок состояния каждого элемента. Результаты представить в табл.3.1.5

Таблица 3.1.5

Результирующая таблица

Элементы ЭБП	Эксперты								
	1	2	3	4	5	6	Фактическое состояние элемента ЭБП	Норма	Приоритетность
F 1									
F 2									
F 3									
F 4									
F 5									
F 6									
F 7									

3. На основе использования ППП «Microsoft Excel» осуществить графическую интерпретацию результатов исследования:

- построить диагностический профиль экономической безопасности предприятия, характеризующий ее с точки зрения основных 7 элементов и отклонений от нормальных параметров (форма построения – диаграмма-график);
- построить диагностический профиль экономической безопасности предприятия, смоделированный с точки зрения элементов, (форма построения – лепестковая диаграмма);
- построить диагностический профиль экономической безопасности предприятия, смоделированный с точки зрения элементов, (форма построения – столбиковая диаграмма).

4. Сформировать диагностическую таблицу, демонстрирующую состояние каждого элемента экономической безопасности предприятия.

Таблица 3.1.6

Диагностическая таблица

Элементы ЭБП	S^+	S^N	S^-
F_1	5, 7		
F_2			2,1
…	…		
F_7		5	

Содержание отчета

Отчет должен представлять собой распечатанный документ MS Word, оформленный с применением творческих возможностей студента.

Отчет должен содержать:

- название, цель и ход выполнения работы;
- исходную информацию экспертной оценки элементов экономической безопасности предприятия;
- статистические показатели и таблицы, полученные с помощью ППП «Prima», соответствующие аналитические выводы;
- таблицу, демонстрирующую средние оценки экспертов по каждому оцениваемому элементу, нормативные параметры состояния экономической безопасности предприятия, а также ранги, присвоенные каждому элементу;
- диагностический профиль экономической безопасности предприятия;
- диагностическую таблицу;
- итоговые выводы.

ЛАБОРАТОРНАЯ РАБОТА №2.
Формирование программы клинической диагностики экономической безопасности предприятия

Цель работы: приобретение практических навыков разработки программы клинической диагностики экономической безопасности предприятия на базе данных экспресс-диагностики .

Исходная информация

Результаты экспресс-диагностики экономической безопасности предприятия, полученные и интерпретированные в лабораторной работе №1 согласно выданному варианту.

Содержание и порядок выполнения работы

1. Создать документ MS Word. Представить краткую информацию о результатах проведенной экспресс-диагностики экономической безопасности предприятия, определить элементы экономической безопасности

предприятия, требующие проведения детального диагностического обследования.

2. Сформулировать цель клинической диагностики экономической безопасности предприятия, исходя из результатов экспресс-диагностики. Определить субъект диагностического исследования. Охарактеризовать объект диагностики, с точки зрения содержания элементов экономической безопасности предприятия, требующих клинического исследования. Сформулировать основные задачи клинической диагностики экономической безопасности предприятия.

3. Представить перечень возможных проблем, способствующих развитию кризисного состояния исследуемых элементов экономической безопасности предприятия.

4. Предложить состав и форму рабочей группы по диагностике требующих исследования элементов экономической безопасности предприятия.

5. Разработать проект формы технического задания на проведение диагностики.

6. Разработать комплексный план-график проведения детальной диагностики экономической безопасности предприятия (табл. 3.2.1).

Таблица 3.2.1

Форма план-графика проведения детальной диагностики экономической безопасности предприятия

№ п.п.	наименование диагностического мероприятия	объект исследования	входная информ формация	выходная информация	испол полнители	сроки выполнения

Содержание отчета

Отчет должен представлять собой распечатанный документ «MS Word», оформленный с применением творческих возможностей студента.

Отчет должен содержать:

- название, цель и ход выполнения работы;
- информацию о целях диагностики, ее основных задачах, субъекте и объекте диагностики (презентацию);
- перечень возможных проблем, способствующих развитию кризисного состояния исследуемых элементов экономической безопасности предприятия;
- обоснование состава и формы рабочей группы диагностики;
- проект формы технического задания на проведение диагностики;

- комплексный план-график проведения детальной диагностики экономической безопасности предприятия.

ЛАБОРАТОРНАЯ РАБОТА №3.
Определение угроз экономической безопасности предприятия с помощью причинно-следственной диаграммы «Исикавы»

Цель работы: приобретение практических навыков декомпозиции угроз и основных факторов (причин) их возникновения путем построения диаграмм «Исикавы».

Общие положения

Причинно – следственная диаграмма «Исикавы» – инструмент, который позволяет выявить наиболее существенные факторы (причины), влияющие на конечный результат (следствие), в данной работе это - процесс обеспечения экономической безопасности предприятия.

Систематическое использование диаграммы причинно-следственных связей позволяет:

1. Выявить всевозможные причины, вызывающие определенную проблему (угрозу).
2. Отделить причины от признаков.
3. Проанализировать относительную важность соответствующих причин.

Для составления причинно-следственной диаграммы необходимо определить максимальное число факторов, имеющих отношение к характеристике.

Результат изображается на конце горизонтальной стрелки (рис.3.3.1). Возможные причины (угрозы) указываются на стрелках, ведущих к данной основной стрелке.

Причины (угрозы) и факторы определяются методом мозгового штурма. Метод мозгового штурма заключается в выдвижении множества идей о возможных причинах. На этапе мозгового штурма ни одна идея сразу не отвергается. Все высказывания записываются для последующего анализа.

Если причины и признаки определенной угрозы выявлены и записаны, то можно определить важность каждого из них, и таким образом узнать наиболее существенные элементы, которым нужно уделять особое внимание.

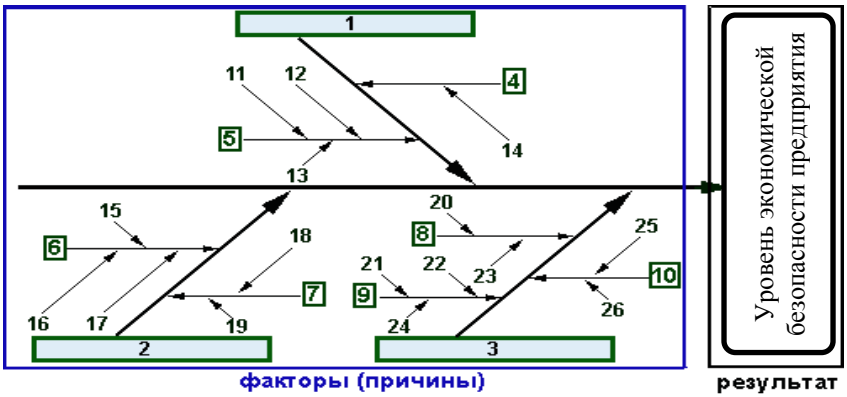

Рис. 3.3.1 – Примерная форма диаграммы «Исикавы».

1-3 – главные угрозы (факторы), влияющие на процесс;

4-10 – вторичные причины (4,5 воздействуют на фактор **1**; 6,7 – на фактор **2**; 8-10 – на фактор **3**);

11-26 – факторы, влияющие на вторичные причины.

Содержание и порядок выполнения работы

1. Определить максимальное число факторов, оказывающих влияние на процесс обеспечения экономической безопасности предприятия. Создать документ MS Word, в котором схематично по примеру на рис. 3.3.1 изобразить:

- главные угрозы (факторы), влияющие на процесс обеспечения экономической безопасности предприятия;
- вторичные причины, воздействующие на главные факторы;
- факторы, влияющие на вторичные причины.

2. Предложить варианты экономико-математических методов (не менее двух методов), с помощью которых можно выявить наиболее значимые факторы оказывающие влияние на уровень экономической безопасности на построенной вами диаграмме.

3. Произвести расчет по одному из предложенных экономико-математических методов, сделав соответствующие выводы о значимости того или иного фактора.

Содержание отчета

Отчет должен представлять собой распечатанный документ «MS Word», оформленный с применением творческих возможностей студента.

Отчет должен содержать:

- название, цель и ход выполнения работы;
- информацию об основных факторах, оказывающих влияние на процесс обеспечения экономической безопасности предприятия;
- перечень вторичных причин и факторов влияющих на вторичные причины;
- схему причинно-следственных связей в форме диаграммы «Исикавы»;
- обоснование экономико-математических методов, применение которых, позволит математически доказать степень влияния того или иного фактора на процесс обеспечения экономической безопасности предприятия;
- расчеты по одному из предложенных экономико-математических методов и итоговые выводы.

ЛАБОРАТОРНАЯ РАБОТА №4

Оценка элементов экономической безопасности предприятия на основе индикаторного подхода

Цель работы: приобретение практических навыков определения и оценки индикаторов основных составляющих экономической безопасности предприятия.

Исходная информация

Результаты экспресс-диагностики экономической безопасности предприятия, полученные и интерпретированные в лабораторной работе №1 согласно выданному варианту.

Общие положения

Индикатор - это свойство или признак, который положен в основу оценивания исследуемого объекта или явления, имеющий количественное выражение. При этом индикаторный подход предполагает не только выбор самих индикаторов, но и определение пороговых значений (предельно допустимых), превышение которых повлечет за собой снижение уровня безопасности исследуемой составляющей экономической безопасности.

Выбор индикаторов необходимо осуществлять на конкретных предприятиях строго индивидуально, так как при этом необходимо учитывать цели оценки, финансовые возможности, факторы влияния внутренней и внешней среды. Минимальный стандартный перечень индикаторов, подлежащих оценке, может быть типовым в зависимости от объекта (конкретной составляющей экономической безопасности) оценки. В

дальнейшем он может быть расширен с помощью дополнительных индикаторов.

Оценка экономической безопасности предприятия производится в результате сравнения (абсолютного либо относительного) текущих показателей деятельности предприятия с индикаторами.

Содержание и порядок выполнения работы

1. Создать документ MS Word. Представить краткую информацию о результатах проведенной экспресс-диагностики экономической безопасности предприятия, описать элементы экономической безопасности предприятия, для которых будут определены индикаторы, пороговые значения и проведена оценка.

2. Предложить индикаторы и распределить их по группам показателей используя следующую форму табл. 3.4.1:

Таблица 3.4.1

Группы индикаторов экономической безопасности предприятия

№	Группа показателей	Индикаторы
1.	Показатели состава и движения персонала	1. Коэффициент текучести кадров 2. Образовательный состав персонала
2.		1. 2.
3.		1. 2.
4.		1. 2.
5.		1. 2.

3. Охарактеризовать выбранные индикаторы.

4. Представить расчетные формулы индикаторов элементов экономической безопасности, определить направление оптимизации и рекомендуемый порог для каждого индикатора, используя следующую форму:

Таблица 3.4.2

Индикаторы экономической безопасности предприятия

Индикатор	Расчет	Направление оптимизации	Рекомендуемый порог
Коэффициент текучести кадров	$К_у/Ч_{ср}$, где $К_у$ – количество уволенных за отчетный период; $Ч_{ср}$ – среднесписочная численность персонала за отчетный период.	min	От 2 до 10%.

5. Бальным методом определить вес каждого из предложенных индикаторов от 1 до 10.

6. Предложить рекомендации по каждому индикатору ориентированные на его оптимизацию.

Содержание отчета

Отчет должен представлять собой распечатанный документ MS Word, оформленный с применением творческих возможностей студента.

Отчет должен содержать:

- название, цель и ход выполнения работы;
- информацию об оцениваемых элементах экономической безопасности предприятия;
- таблицу с выбранными индикаторами, разбитыми по группам;
- краткую характеристику по каждому предложенному индикатору;
- таблицу, содержащую расчетные формулы индикаторов, направление их оптимизации, а также рекомендуемый порог;
- бальную оценку каждого предложенного индикатора;
- рекомендации по каждому индикатору с целью его оптимизации.

ЛАБОРАТОРНАЯ РАБОТА №5
Расчет основных показателей деятельности предприятия, с целью определения уровня его экономической безопасности

Цель работы: приобретение практических навыков расчета и оценки основных показателей, характеризующих уровень экономической безопасности предприятия.

Исходная информация:

- отчет по практике по получению профессиональных умений и опыта профессиональной деятельности;
- материалы научно-исследовательской работы студента.

Содержание и порядок выполнения работы:

1. По результатам исследования деятельности реального предприятия, привести общую характеристику по следующему алгоритму:

- полное и сокращенное наименование предприятия, когда и кем зарегистрировано, вышестоящий орган;
- организационно-правовая форма: статус, форма собственности на землю и имущество, источники формирования имущества;
- главная миссия организации;
- основные цели деятельности;
- юридический адрес организации;

- основные учредительные документы и т.п.

2. В бизнес - справке предприятия необходимо привести сведения о размере кредиторской задолженности, убытках, конкурентных преимуществах предприятия, значимости в масштабе региона, деловой репутации руководящего состава и сотрудниках предприятия.

3. Провести расчет основных показателей работы за последние 3 года по материалам отчетности предприятия, с помощью программно-прикладного продукта MS Excel . Данные расчетов необходимо представить в табл.3.5.1.

Таблица 3.5.1

Основные показатели работы исследуемого предприятия

Показатели	20__ г.	20__ г.	20__ г.	Отклонение	
				абсолютное (+,-)	относительное (%)
1. Внеоборотные активы, тыс. руб.					
2. Оборотные активы, тыс. руб.					
3. Собственный капитал, тыс. руб.					
4. Валюта баланса, тыс. руб.					
5. Чистые активы, тыс. руб.					
6. Выручка, тыс. руб.					
7. Себестоимость, тыс. руб.					
8. Валовая прибыль, тыс. руб.					
9. Прибыль от продаж, тыс. руб.					
10. Чистая прибыль (убыток), тыс. руб.					
11. Рентабельность продаж, % (стр.9/стр.6)					
12. Рентабельность продукции, % (стр.8/стр.7)					

Отчет должен представлять собой распечатанный документ MS Word, оформленный с применением творческих возможностей студента.

Отчет должен содержать:

- название, цель и ход выполнения работы;

- информацию о исследуемом предприятии: история создания, организационно-правовая форма, миссия, цель и т.д.

- краткую характеристику финансово-хозяйственной деятельности предприятия;

- таблицу, содержащую расчет основных показателей деятельности предприятия за последние 3 года;

- пояснительную записку с выводами об уровне экономической безопасности предприятия.

ЛАБОРАТОРНАЯ РАБОТА №6
Оценка уровня финансовой безопасности предприятия

Цель работы: приобретение практических навыков расчета и оценки основных показателей, характеризующих уровень финансовой безопасности предприятия.

Исходная информация:

- отчет по практике по получению профессиональных умений и опыта профессиональной деятельности;

- материалы научно-исследовательской работы студента.

Общие положения

Финансовая безопасность рассматривает и регулирует вопросы финансово-экономической состоятельности предприятия, устойчивости к банкротству. Финансовая безопасность может быть определена как совокупность мер по формированию эффективной структуры капитала предприятия, повышению качества планирования и осуществления финансово-хозяйственной деятельности по всем направлениям стратегического, оперативного планирования и управления технологическим, интеллектуальным и кадровым потенциалом, его основным капиталом и оборотными активами с целью максимизации прибыли и повышения рентабельности.

Данная составляющая экономической безопасности находится в зоне ответственности финансовых и экономических служб предприятия.

Содержание и порядок выполнения работы:

1. Оценку финансовой составляющей экономической безопасности необходимо начать с анализа ликвидности баланса предприятия.

Для диагностики ликвидности бухгалтерского баланса активы группируются по степени убывания ликвидности:

А1 - наиболее ликвидные;

А2 - быстрореализуемые активы;

А3 - медленно реализуемые активы;

А4 - труднореализуемые активы.

С этой целью пассивы группируются по степени срочности оплаты:

П1 - наиболее срочные обязательства;

П2 - краткосрочные пассивы;

П3 - долгосрочные пассивы;

П4 - постоянные пассивы.

Условия абсолютной ликвидности баланса:

Если выполнимо неравенство А1 > П1, то это свидетельствует о платежеспособности предприятия на момент составления баланса. У предприятия достаточно ресурсов для покрытия наиболее срочных обязательств абсолютно и наиболее ликвидных активов.

Если выполнимо неравенство А2 > П2, то быстро реализуемые активы превышают краткосрочные пассивы и предприятие может быть платежеспособным в недалеком будущем с учетом своевременных расчетов с кредиторами, получения средств от продажи продукции в кредит.

Если выполнимо неравенство А3 > П3, то в будущем при своевременном поступлении денежных средств от продаж и платежей предприятие может быть платежеспособным на период, равный средней продолжительности одного оборота оборотных средств после даты составления баланса.

Выполнение первых трех условий приводит автоматически к выполнению условия: А4<=П4

Выполнение этого условия свидетельствует о соблюдении минимального условия финансовой устойчивости предприятия, наличия у него собственных оборотных средств.

На основе сопоставления групп активов с соответствующими группами пассивов делается вывод о ликвидности предприятия.

Сопоставление ликвидных средств и обязательств позволит вычислить следующие показатели:

- текущая ликвидность, которая свидетельствует о платежеспособности (+) или неплатежеспособности (-) предприятия на ближайший к рассматриваемому моменту промежуток времени: А1 +А2=>П 1+П2, А4<=П4;

- перспективная ликвидность - это прогноз платежеспособности на основе сравнения будущих поступлений и платежей: А3>=П3, А4<=П4;

- недостаточный уровень перспективной ликвидности: А4<=П4;

- баланс не ликвиден: А4=>П4.

Расчеты по исследуемому предприятию за 3 года следует представить в табл. 3.6.1.

Таблица 3.6.1

Группировка активов и пассивов бухгалтерского баланса по степени ликвидности и срочности оплаты

Актив	На конец года	Пассив	На конец года	Величина платежного избытка (недостатка)
201_ год				
А1 (стр. 1250+стр.1240)		П1 (стр.1520)		
А2 (стр. 1230+стр.1260)		П2 (стр.1510+стр.1550)		
А3 (стр.1210+стр.1220+стр.1170)		П3 (стр.1400)		
А4 (стр.1100-+стр.1170)		П4(стр.1300+стр.1530+стр.1540)		
Баланс		Баланс		
201_ год				
А1		П1		
А2		П2		
А3		П3		
А4		П4		
Баланс		Баланс		
201_ год				
А1		П1		
А2		П2		
А3		П3		
А4		П4		
Баланс		Баланс		

По результатам заполнения таблицы, необходимо написать краткий вывод.

2. Необходимо провести более детальный анализ платежеспособности при помощи финансовых коэффициентов.

Состояние финансовой безопасности предприятия характеризуют следующие четыре группы показателей:

- показатели ликвидности, характеризующие возможность предприятия в конкретный момент времени рассчитаться с кредиторами собственными средствами;

- показатели финансовой устойчивости, характеризующие степень защищенности привлеченного капитала;

- показатели деловой активности, характеризующие эффективность использования ресурсов предприятия с позиции скорости осуществления финансово-хозяйственных операций;

- показатели рентабельности, характеризующие эффективность работы предприятия в целом, доходность различных направлений деятельности (производственной, коммерческой, инвестиционной), выгодность производства отдельных видов продукции и услуг.

Необходимо самостоятельно сформировать систему показателей финансового состояния предприятия, с учетом её специфики; вычислить показатели за исследуемый период; полученные значения сравнить с их нормативными (рекомендованными); охарактеризовать динамику показателей; сделать вывод о финансовом состоянии предприятия.

Таблица 3.6.2

Показатели финансового состояния предприятия

Показатели	Нормативное значение	201_ год	201_ год	201_ год	Отклонение от нормативного значения / базового уровня (+,-)
1	2	3	4	5	6
1. Показатели ликвидности					
Коэффициент абсолютной ликвидности					
Коэффициент быстрой ликвидности					
Коэффициент текущей ликвидности					
2. Показатели финансовой устойчивости					
Коэффициент автономии					
Коэффициент заемного капитала					
Коэффициент финансовой зависимости					

Продолжение табл. 3.6.2

1	2	3	4	5	6
Коэффициент финансовой устойчивости					
Коэффициент маневренности собственного капитала					
Коэффициент структуры долгосрочных вложений					
Коэффициент долгосрочного привлечения заемных средств					
Коэффициент финансового риска					
3. Оценка деловой активности					
Коэффициент оборачиваемости активов	х				
Коэффициент оборачиваемости оборотных активов	х				
Коэффициент оборачиваемости запасов	х				
Продолжительность операционного цикла в днях	х				
Продолжительность финансового цикла	х				
4. Показатели рентабельности					
Рентабельность основной деятельности, %	х				
Рентабельность продаж, %	х				
Рентабельность продаж по чистой прибыли, %	х				
Рентабельность активов по чистой прибыли, %	х				

По результатам заполнения табл. 3.6.2, необходимо написать краткий вывод.

При написании выводов следует учесть, что для первых двух групп показателей существуют нормативные значения и сигналами ослабления финансовой безопасности являются существенные отклонения рассчитанных показателей от нормативов. Для показателей деловой активности и рентабельности, не имеющих нормативных значений, необходимо охарактеризовать выявленные тенденции.

3. Оценку финансовой безопасности следует дополнить прогнозом вероятности банкротства предприяти, например, на основе модифицированной модели Э. Альтмана (Z-счет):

$$Z = 0{,}717 \bullet X_1 + 0{,}843 \bullet X_2 + 3{,}107 \bullet X_3 + 0{,}42 \bullet X_4, + 0{,}995 \bullet X_5$$

Таблица 3.6.3

Оценка вероятности банкротства методом Э. Альтмана

Показатели	201_ год	201_ год	201_ год
Оборотный капитал/сумма активов (X_1)			
Нераспределенная прибыль/сумма активов (X_2)			
Прибыль до налогообложения/сумма активов (X_3)			
Балансовая стоимость собственного капитала/заемный капитал (X_4)			
Объем продаж/сумма активов (X_5)			
Z - счет			

Уровень ожидаемого банкротства с помощью модели Альтмана оценивается по следующей шкале в табл. 3.6.4:

Таблица 3.6.4

Z - счет	Вероятность банкротства
До 1,8	Очень высокая
1,81-2,70	Высокая
2,71-2,99	Возможная
3,00 и выше	Очень низкая

По результатам заполнения табл.3.6.4, необходимо написать краткий вывод.

4. Окончательный вывод о том, на каком уровне находится финансовая безопасность предприятия, формулируется на основе обобщающего анализа показателей табл. 3.6.1-3.6.4

Уровень финансовой безопасности оценивается по следующей шкале:

- ***абсолютным,*** если показатели соответствуют нормативным значениям и наблюдается положительная динамика показателей, не имеющих нормативных значений;

- ***нормальным,*** если большинство показателей соответствуют своим нормативным значениям и наблюдается в основном положительная динамика показателей, не имеющих нормативных значений;

- ***нестабильным,*** если часть показателей не соответствуют своим нормативным значениям и наблюдается отрицательная динамика отдельных показателей, не имеющих нормативных значений;

- ***критическим,*** если большинство показателей не соответствуют своим нормативным значениям и наблюдается отрицательная динамика большинства показателей, не имеющих нормативных значений;

- ***кризисным***, если предприятие находится на грани банкротства.

Отчет должен содержать:

- название, цель и ход выполнения работы;

- заполненную по материалам предприятия таблицу с группировкой активов и пассивов бухгалтерского баланса по степени ликвидности и срочности оплаты;

- заполненную по материалам предприятия таблицу показателями финансового состояния предприятия;

- заполненную по материалам предприятия таблицу с оценкой вероятности банкротства методом Э. Альтмана;

- пояснительную записку с выводами по каждому этапу оценки и итоговым выводом об уровне финансовой безопасности предприятия.

ЛАБОРАТОРНАЯ РАБОТА №7
Оценка уровня технико-технологической безопасности предприятия

Цель работы: приобретение практических навыков расчета и оценки основных показателей, характеризующих уровень технико-технологической безопасности предприятия.

Исходная информация:

- отчет по практике по получению профессиональных умений и опыта профессиональной деятельности.

Содержание и порядок выполнения работы:

Технико-технологическая безопасность предполагает создание и использование такой материально-технической базы, технологических процессов, которые усиливают конкурентоспособность предприятия.

1. Поскольку одним из важнейших условий выпуска конкурентоспособной продукции является обеспеченность основными средствами и повышение отдачи от их использования, то необходимо дать характеристику состава основных средств исследуемого предприятия и их структуры (табл. 3.7.1), а также рассчитать показатели воспроизводства основных средств и эффективности их использования (табл. 3.7.2).

Таблица 3.7.1

Основные средства предприятия

Виды	201_ год		201_ год		201_ год		Отклонение	
	тыс.р.	%	тыс.р.	%	тыс.р.	%	тыс.р.	%
1. Здания, сооружения и передаточные устройства								
2. Машины и оборудование								
3. Транспортные средства								
4. Продуктивный скот								
5. Многолетние насаждения								
и др.								
Итого								
В т.ч. активная часть								

По результатам заполнения табл. 3.7.1, необходимо написать краткий вывод.

Таблица 3.7.2

Показатели воспроизводства основных средств и эффективности их использования

Показатели	201_ год	201_ год	201_ год	Отклонение (+,-)
1. Срок обновления, лет				
2. Коэффициент выбытия				
3. Коэффициент прироста				
4. Фондоотдача				
5. Фондоемкость				
6. Рентабельность основных средств, %				
и др.				

По результатам заполнения таблицы, необходимо написать краткий вывод.

2. Материально-техническая база предприятия определяется наличием не только основных средств, но и оборотных ресурсов, в ходе управления которыми принято контролировать объем и структуру оборотных средств, их динамику по видам (табл. 3.7.3), а также показатели экономической эффективности их использования (табл. 3.7.4).

Таблица 3.7.3

Оборотные средства предприятия

Наименование	201_ год		201_ год		201_ год		Отклонение	
	тыс.р.	%	тыс.р.	%	тыс.р.	%	тыс.р.	%
1. Запасы								
2. НДС по приобретенным ценностям								
3. Дебиторская задолженность								
4. Финансовые вложения (за исключением денежных эквивалентов)								
5. Денежные средства и денежные эквиваленты								
6. Прочие оборотные активы								
Итого								

По результатам заполнения табл.3.7.3, необходимо написать краткий вывод.

Таблица 3.7.4

Эффективность использования оборотных средств

Показатели	201_ год	201_ год	201_ год	Отклонение (+,-)	
				абсолютное (+,-)	относительное (%)
1	2	3	4	5	6
1. Выручка от продаж, тыс.руб.					
2. Среднегодовой остаток оборотных средств, тыс.руб.					
3. Длительность одного оборота, дни (стр.2×360/стр.1)					

Продолжение табл. 3.7.4

1	2	3	4	5	6
4. Коэффициент оборачиваемости оборотных средств (стр.1/стр.2)					
5. Прибыль, тыс.руб.					
6. Коэффициент загрузки оборотных средств (стр.2/стр.1)					
7. Рентабельность оборотных средств (стр.3/стр.2), %					

По результатам заполнения таблицы, необходимо написать вывод о состоянии уровня технико-технологической безопасности предприятия.

Отчет должен содержать:

- название, цель и ход выполнения работы;
- заполненную по материалам предприятия таблицу основные средства предприятия;
- заполненную по материалам предприятия таблицу показатели воспроизводства основных средств и эффективности их использования;
- заполненные по материалам предприятия таблицы оборотные средства предприятия и эффективность использования основных средств;
- пояснительную записку с выводами по каждому этапу оценки и итоговым выводом об уровне технико-технологической безопасности предприятия.

ЛАБОРАТОРНАЯ РАБОТА №8
Оценка уровня интеллектуально-кадровой безопасности предприятия

Цель работы: приобретение практических навыков расчета и оценки основных показателей, характеризующих уровень интеллектуально-кадровой безопасности предприятия.

Исходная информация:

- отчет по практике по получению профессиональных умений и опыта профессиональной деятельности;
- материалы научно-исследовательской работы студента.

Общие положения

Интеллектуально-кадровая безопасность обеспечивается в процессе предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным и трудовым потенциалом.

Требуется дать оценку обеспеченности предприятия необходимыми трудовыми ресурсами, их рационального использования и уровня про-

изводительности труда, имеющих большое значение для увеличения объемов продукции и повышения эффективности производства. Например, от обеспеченности предприятия трудовыми ресурсами и эффективности их использования зависят объем и своевременность выполнения всех работ, эффективность использования оборудования, машин, механизмов и как результат объем производства продукции, ее себестоимость, прибыль и ряд других экономических показателей.

Содержание и порядок выполнения работы:

1. Необходимо провести анализ состава работников предприятия, его структуры, а также выполнить оценку эффективности использования трудовых ресурсов.

Таблица 3.8.1

Состав работников предприятия и его структура

Категория работников	20_ год		20_ год		20_ год		Отклонение	
	Чел.	%	Чел.	%	Чел.	%	Чел.	%
Служащие								
из них: - руководители - специалисты								
Рабочие								
Итого								

В выводе необходимо охарактеризовать изменения в составе работников и его структуре.

Таблица 3.8.2

Половозрастная структура работников в 20_ г.

Распределение работающих по возрасту	Человек			В процентах к итогу		
	Муж.	Жен.	всего	Муж.	Жен.	всего
До 25						
С 26 до 35 лет						
С 36 до 45 лет						
С 46 до 55 лет						
После 55						
Итого						

В выводе охарактеризуйте сложившуюся половозрастную структуру работников.

Таблица 3.8.3

Кадровый состав предприятия в 20_ г.

Должность	Образование	Опыт работы
Генеральный директор		
Заместитель генерального директора		
Главный бухгалтер и др.		

В выводе необходимо охарактеризовать руководящий (кадровый) состав предприятия с точки зрения образования и опыта работы.

2. Затем необходимо выполнить анализ эффективности использования трудовых ресурсов (табл. 3.8.4).

Таблица 3.8.4

Эффективность использования трудовых ресурсов

Показатели	20_ год	20_ год	20_ год	Отклонение (+,-)	
				абсолютное (+,-)	относительное (%)
1. Производительность труда, тыс. руб./чел.-час					
2. Производительность труда, тыс.руб./чел.					
3. Темп роста (или снижения) производительности труда, %	х				
4. Темпы роста (или снижения) оплаты труда, %.	х				
5. Коэффициент опережения роста (или снижения) производительности труда над оплатой труда	х				

Характеристика интеллектуально-кадровой безопасности может быть дополнена расчетом и анализом следующих показателей:

- текучесть работников высокой квалификации (отношение количества уволившихся работников к общему количеству работников данной квалификации);
- удельный вес инженерно-технических и научных работников (отношение их количества ко всему количеству работающих);
- показатель изобретательской (рационализаторской) активности (отношение количества изобретений (рацпредложений) к количеству работающих или инженерно-технических работников);
- показатель образовательного уровня (отношение количества лиц, имеющих высшее (специальное) образование в соответствии с профилем деятельности предприятия к общему количеству работающих) и т.п.

По результатам заполнения таблицы, необходимо написать краткий вывод.

Также для объективной оценки интеллектуально-кадровой безопасности предприятия следует учесть трудовые и кадровые потери.

Трудовые потери - это потери рабочего времени, вызванные случайными непредвиденными обстоятельствами, измеряемые в человеко-часах, человеко-днях или просто в часах рабочего времени. Перевод трудовых потерь в денежное выражение осуществляется умножением часов потери рабочего времени на стоимость одного часа. Рекомендуется обратить внимание на причины потерь рабочего времени, например, является ли причиной общее заболевание работника или производственная травма.

Кадровые потери - потери необходимых предприятию профессиональных, высококвалифицированных работников. Измеряются в затратах на подбор и обучение нового кадрового состава в денежном выражении.

По результатам заполнения таблиц, учета кадровых и трудовых потерь, необходимо написать вывод о состоянии уровня интеллектуально-кадровой безопасности предприятия.

Отчет должен содержать:

- название, цель и ход выполнения работы;
- заполненную по материалам предприятия таблицу с анализом состава работников предприятия, его структуры;
- заполненную по материалам предприятия таблицу половозрастной структуры работников и кадрового состава предприятия;
- заполненную по материалам предприятия таблицу с показателями эффективности использования трудовых ресурсов;
- пояснительную записку с выводами по каждому этапу оценки и итоговым выводом об уровне интеллектуально-кадровой безопасности предприятия.

ЛАБОРАТОРНАЯ РАБОТА №9
Факторы, оказывающие влияние на экономическую безопасность предприятия

Цель работы: приобретение практических навыков работы с бизнес информацией, с целью анализа и оценки факторов, оказывающих влияние на уровень экономической безопасности предприятия.

Исходная информация:

- отчет по практике по получению профессиональных умений и опыта профессиональной деятельности;
- материалы научно-исследовательской работы студента.

Содержание и порядок выполнения работы:

1. Изучите новости, представленные на официальном сайте исследуемого предприятия и областной администрации.

2. Используя материалы, представленные на сайтах, заполните табл. 3.9.1, определив события, которые можно рассматривать как:

- внешние факторы, оказывающие влияние на экономическую безопасность предприятия (не менее 5 примеров);
- внутренние факторы, оказывающие влияние на экономическую безопасность предприятия (не менее 5 примеров).

Таблица 3.9.1

Факторы оказывающие влияние на экономическую безопасность предприятия

Дата	Событие	Фактор, оказывающий влияние на экономическую безопасность предприятия
17.01.2020	Министерство обороны сформировало гособоронзаказ на продукцию предприятия	Внешний политический фактор (покупка государством военной техники с целью укрепления обороноспособности страны)
27.02.2020	Внедрение элементов системы бережливого производства на предприятии позволило повысить уровень производительности труда	Внутренний экономический фактор (эффективность производственной деятельности предприятия)

Отчет должен содержать:

- название, цель и ход выполнения работы;
- заполненную по материалам предприятия таблицу с анализом факторов оказывающих влияние на уровень экономической безопасности предприятия;
- пояснительную записку с выводами по выделенному фактору, оказывающему влияние на уровень экономической безопасности предприятия.

ЗАКЛЮЧЕНИЕ

Таким образом, обеспечение экономической безопасности на режимных предприятиях является одним из ключевых аспектов эффективного функционирования таких организаций и формирования успешной стратегии их развития. Кроме того, должны быть учтены специфика работы на режимных предприятиях, масштаб их деятельности, отраслевые характеристики, а также динамика нормативно--правового регулирования экономической безопасности на региональном и федеральном уровнях.

Только комплексный подход к формированию, поддержанию и развитию мер по обеспечению экономической безопасности на режимных предприятиях может дать длительный положительный результат.

С этой целью следует определить для каждого конкретного предприятия основные компоненты экономической безопасности, разработать методический подход и действенные методики для оценки экономической безопасности предприятия, а также экономических угроз. Все это позволит сформировать систему мероприятий по предупреждению чрезвычайных ситуаций на режимных объектах, в том числе ведущей отрасли российской промышленности - машиностроения.

В учебно-методическом пособии представлен конспект лекций по курсу «Экономическая безопасность на режимных объектах», перечень практических занятий и лабораторных работ по дисциплине.

Для получения дополнительной информации, необходимой для выполнения практических занятий и лабораторных работ необходимо использовать материалы официальных сайтов в Интернете:

- Министерство экономического развития и торговли РФ (http://www.economy.gov.ru);
- Министерство промышленности и энергетики РФ (http://www.mte.gov.ru);
- Министерство финансов РФ (http://www.minfin.ru);
- Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) (http://www.fatf-gafi.org/);
- Институт финансовой и экономической безопасности (http://www.ifes.mephi.ru/podft/mezhdunarodnaya-sistema-podft);
- Федеральная служба РФ по финансовому мониторингу (Росфинмониторинг) (http://www.fedsfm.ru/);
- Информационные системы (Консультант-Плюс, Гарант);
- Материалы периодических изданий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алимов А. А. Экологическая безопасность и мировая политика: что происходит, кто виноват и что делать? [Текст] / А. А. Алимов // Вестник МГИМО. – 2011. – № 4. – С. 226–232.

2. Арбузов С. А. Методологические основы оценки уровня экономической безопасности предприятия [Текст] / С.А. Арбузов // Общество и экономика. - 2017. - №6. - С.28-37.

3. Бадаева О.Н. Оценка финансовой безопасности малых и средних предприятий [Текст] / О.Н. Бадаева, Е.В. Цупко // Российское предпринимательство. – 2013. - №14 (236). - С. 71-83.

4. Беспалько А. А. Экономическая безопасность строительных предприятий : автореф. дис….канд. экон. наук : 08.00.05 [Текст] / А. А. Беспалько. – Москва, 2005. – 23 с.

5. Бланк И.А. Управление финансовой безопасностью предприятия [Текст] / И.А. Бланк.– 2-е изд., перераб. и доп.;– К.: Эльга, 2009.– 776 с.

6. Богомолов В. А. Введение в специальность «Экономическая безопасность»: учебное пособие для вузов [Текст] / В.А. Богомолов. - М.: Изд-во ЮНИТИ-ДАНА, 2012. - 279 с.

7. Воробьев Ю.Н. Сущность финансовой безопасности предприятия [Текст] / Ю.Н. Воробьев, О.Г. Блажевич // Науковий вісник: Фінанси, банки, інвестиції/ - 2011. - №3. – С. 37-40.

8. Глазьев С. Ю. Основы обеспечения экономической безопасности страны [Текст] / С.Ю. Глазьев // Российский экономический журнал. - 2013. - № 1. - С. 12-18.

9. Грунин, О. А. Экономическая безопасность организации [Текст] / О.А. Грунин, С. О. Грунин; – СПб. и др.: Питер, 2002 – 160 с.

10. Доценко Д.В. Экономическая безопасность: Методологические аспекты и составляющие [Текст] / Д.В. Доценко, В.Н. Круглов // Аудит и финансовый анализ. – 2009. - №4. – С. 415-427.

11. Евсеева А.Ю. Экономическая безопасность и ее значение для предпринимательской деятельности [Текст] / А.Ю. Евсеева, С.В. Котик // Налоговое планирование. - 2012. - № 3. - С. 46 - 48.

12. Илякова И.Е. Диагностика интеллектуальной и кадровой составляющих экономической безопасности корпорации: угрозы и условия нейтрализации [Текст] / И.Е. Ильякова, О.С. Саушева // Интернет-журнал «НАУКОВЕДЕНИЕ», 2015 - Т.7, №5 (2015) – URL: http://naukovedenie.ru /PDF/221EVN515.pdf (доступ свободный).

13. Кашин А. В. Экономическая безопасность предприятия: управленческие решения: автореф. дис….канд. экон. наук: 08.00.05 [Текст] / А. В. Кашин. – Москва, 2008. – 25 с.

14. Килинкарова С.Г. International innovation research [Текст] / С.Г. Килинкарова, С.О. Кибизова // Сборник статей IX Международной научно-практической конференции: В 2 ч. – 2017. – С.88-91.

15. Козаченко А.В., Пономарев В.П., Ляшенко А.Н. Экономическая безопасность предприятия: сущность и механизм обеспечения: монография [Текст] / А.В. Козаченко, В.П. Пономарев, А.Н. Ляшенко. - К.: Либра, 2003. - 280 с.

16. Коноплева И. А. Управление безопасностью и безопасность бизнеса: учеб. пособие для вузов [Текст] / И. А. Коноплева, И. А. Богданов. - М.: Изд-во ИНФРА-М., 2012. - 447 с.

17. Королев М.И. Система экономической безопасности предприятия [Текст] / М.И. Королев. -М.: Изд-во Маска, 2011. - 347 с.

18. Кривякин К. С. Основы разработки стратегии экономической безопасности предприятия [Текст] / К. С. Кривякин, Д.С. Карякина // Экономинфо. – 2017. – № 4. – С. 24-27.

19. Кривякин К. С. Методический подход к оценке рисков информационной безопасности предприятия [Текст] / К. С. Кривякин, А.Р. Изотова, В.М. Федоров // Экономинфо. – 2018. – Т.15. - № 2. – С. 82-90.

20. Мамаева Л.Н. Экономическая безопасность предприятия: учеб. пособие [Текст] / Л.Н. Мамаева. – Саратов: Изд-во Саратовский социально-экономический институт (филиал) ФГБОУ ВПО «РЭУ им. Г.В. Плехонова», 2015. – 112 с.

21. Матвеев Н. В. Экономическая безопасность предприятия : автореф. дис….канд. экон. наук : 08.00.05 [Текст] / Н. В. Матвеев. – Москва, 1999. – 23 с.

22. Меламедов С. Л. Формирование стратегии экономической безопасности предпринимательских структур: автореф. дис….канд. экон. наук : 08.00.05 [Текст] / С. Л. Меламедов. – Санкт-Петербург, 2002. – 15 с.

23. Муратова Н. К. Экономическая безопасность предприятия как успешная составляющая современного бизнеса / Н.К. Муратова // Государственное управление. Электронный вестник. – 2012. - №32. – С. 1-6.

24. Обеспечение экономической безопасности на режимных объектах: монография [Текст] / С.А. Волкова, И.А. Гунина, О.В. Дударева [и др.]; под. ред. С.В. Свиридовой. – Воронеж: Издательско-полиграфический центр «Научная книга», 2019. – 227с.

25. Одинцов А.А. Экономическая и информационная безопасность предпринимательства [Текст] / А.А. Одинцов. - М.: Изд-во Академия, 2008. – 336 с.

26. Раздорожный А.А. Организация производства и управление предприятием [Текст] / А.А. Раздорожный. – М.: Изд-во «Экзамен», 2009. – 877 с.

27.Указ Президента РФ от 24.01.1998 № 61 "О перечне сведений, отнесенных к государственной тайне" [Электронный ресурс] : Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_17631/de05c3e5586ac7ac5c8f62e2c129ed105bbc2422/ (дата обращения 15.03.2020)

28. Филимонова Е.А. О соотношении понятий финансовой устойчивости и финансовой безопасности [Текст] / Е.А. Филимонова // Новая наука: Стратегии и векторы развития. – 2016. - №11. – С. 262-264.

29. Хайитматов У.Т., Азаматов О.Х., Мажидов Р.Р., Хакимов А.Ф. Обеспечение экономической безопасности предприятий в современном бизнесе [Текст] / У.Т. Хайитматов , О.Х. Азаматов , Р.Р. Мажидов. // Иктисодиѐт ва инновацион технологиялар. 2012. № 4.

30. Шаваев А. Г. Безопасность корпораций. Криминологические, уголовно-правовые и организационные проблемы [Текст] / А.Г. Шаваев - М.: Изд-во Концерн "Банковский Деловой Центр", 1998. - 240 с.

31. Шаньгин В. Ф. Информационная безопасность и защита информации [Текст] / В.Ф. Шаньгин. // Электрон. Текстовые данные.- Саратов: Изд-во Профобразование, 2017. - 702 с.

32. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия [Текст] / В.В. Шлыков - СПб.: Изд-во Алетейя, 1999. - 144 с.

33. Экономическая и национальная безопасность : учебник для студентов вузов [Текст] / Е. А. Олейников [и др.]; отв. ред. Е. А. Олейников. – М.: Экзамен, 2004 – 768 с.

34 Якушина Н.В. Финансовая безопасность предприятия [Текст] / Н.В. Якушина // Вестник управления. – 2013. - №11. – С. 132-135.

35. Ярочкин В.И. Информационная безопасность: учебник [Текст] / В.И. Ярочкин.- М.: Фонд «Мир»; Акад. проект, 2003. - 639 с.

ОГЛАВЛЕНИЕ

Учебное издание

КРИВЯКИН Кирилл Сергеевич
МАКАРОВ Николай Николаевич
ШОТЫЛО Денис Михайлович

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ НА РЕЖИМНЫХ ОБЪЕКТАХ

Учебно-методическое пособие

Издание публикуется в авторской редакции
и авторском наборе

Подписано в печать 13.11.2020. Формат 60×84/16.
Усл. печ. л. 5,93. Тираж 100 экз. Заказ 226.

ООО Издательско-полиграфический центр «Научная книга»
394018, г. Воронеж, ул. Никитинская, 38, оф. 308
Тел. +7 (473) 200-81-02, 200-81-04
htth://www.n-kniga.ru. E-mail: zakaz@n-kniga.ru

Отпечатано в типографии ООО ИПЦ «Научная книга».
394026, г. Воронеж, Московский пр-т, 11/5
Тел. +7 (473) 220-57-15
http://www.n-kniga.ru. E-mail: typ@n-kniga.ru