Министерство сельского хозяйства Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БРЯНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

КАФЕДРА БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ И ИНЖЕНЕРНОЙ ЭКОЛОГИИ

ХРИСТОФОРОВ Е.Н.
САКОВИЧ Н.Е.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

Учебное пособие

Брянск – 2024

УДК 338.2:331.45 (07)
ББК 65.050.17
Х 93

Христофоров, Е. Н. Управление безопасностью предприятия: учебное пособие, краткий курс лекций для магистрантов направления подготовки 20.04.01 Техносферная безопасность, направленность (профиль) Безопасность жизнедеятельности в чрезвычайных ситуациях / Е. Н. Христофоров, Н. Е. Сакович. – Брянск: Изд-во Брянский ГАУ, 2024. – 72 с.

Краткий курс лекций по дисциплине «Управление безопасностью предприятия» составлен в соответствие с рабочей программой. Краткий курс лекций содержит теоретический материал по основным вопросам дисциплины.

Рецензенты:

профессор кафедры технологического оборудования животноводства и перерабатывающих производств ФГБОУ ВО Брянский ГАУ д.т.н., профессор А.И. Купреенко;

доцент кафедры безопасность жизнедеятельности и инженерной экологии ФГБОУ ВО Брянский ГАУ к.т.н., доцент Т.В. Панова.

Рекомендовано к изданию методической комиссией инженерно-технологического института Брянского ГАУ, протокол №9 от 26 апреля 2024 г.

Содержание

Введение

Материальная база любого общества состоит из сотен тысяч хозяйствующих субъектов. Поэтому успешное, полноценное и эффективное решение задач, стоящих перед экономикой государства в целом, во многом зависит от результативности деятельности ее производственных единиц (экономических агентов). Если экономика опирается на мощную производственную базу, на крепкие, высокоразвитые производственные единицы, способные успешно добиваться поставленных целей, то и вся совокупность экономических потребностей общества будет удовлетворяться своевременно и полно.

Условия рыночной экономики, в которых осуществляют свою деятельность производственные единицы, существующие в различных организационно – правовых формах, неопределенны и непредсказуемы. Затянувшийся и очень глубокий экономический кризис породил многие опасности и угрозы зарождающемуся, еще не окрепшему бизнесу. Кроме того, на развитие предпринимательства оказывают влияние и такие факторы, как нестабильная политическая и социально – экономическая ситуация в стране, межнациональные, региональные, территориальные конфликты, несовершенство коммерческого законодательства, криминализация общества, мошенничество, коррупция и другие. Все это резко обострило проблему обеспечения безопасности предприятия.

Глава 1. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЙ

1.1 Теоретические основы понятия безопасности

Предприятие – это не только здания, сооружения, средства производства, рабочая сила и т.д.; это, прежде всего, работающий организм, который выпускает продукцию, находясь в постоянном запутанном клубке связей и отношений в определенной окружающей среде. В самом общем виде ***под предприятием понимается*** самостоятельный хозяйствующий субъект с правом юридического лица, который на основе имеющихся у него (или закрепленных за ним) ресурсов производит и реализует продукцию, выполняет работы и оказывает услуги. Все это должно учитываться при обеспечении его безопасности.

Безопасность предприятия – понятие емкое. В самом узком виде его можно представить как отсутствие различного рода опасностей и угроз или наличие возможностей по их предупреждению, защите своих интересов, недопущение ущерба больше критического предела. Это требует кропотливой повседневной работы соответствующего персонала, служб безопасности, которые бы обеспечили безубыточную работу предприятия, сохранение его имущества, недопущение разглашения тайны, пресечение факторов насильственных преступлений, сохранение интеллектуальной собственности и т.д.

Экономическая безопасность – это материальная база безопасности предприятия в целом. Разработка теории экономической безопасности предпринимательства находится на начальной стадии. В настоящее время в научной литературе, даже специальной, сущность теории экономической безопасности предпринимательства, его слагаемых, индикаторов раскрывается крайне редко. В определениях данная сущность выражается либо не всегда четко, либо неполно. Очень часто обеспечение экономической безопасности бизнеса сводится к противостоянию, защите от разного рода экономических преступлений. Несомненно, что это важно, но нельзя сводить понятие «экономической безопасности предприятия» лишь к такой защите.

По нашему мнению, ***экономическая безопасность предприятия*** – это

такое состояние хозяйствующего субъекта, при котором он при наиболее эффективном использовании корпоративных ресурсов добивается предотвращения, ослабления или защиты от существующих опасностей и угроз или других непредвиденных обстоятельств и обеспечивает достижение целей бизнеса в условиях конкуренции и хозяйственного риска.

Такое понимание экономической безопасности предприятия позволяет показать, что:

– производственное предприятие находится в ситуации неопределенности, непредсказуемости, изменения, как внутренних условий хозяйствования, так и внешних политических, макроэкономических, экологических, правовых;

– принимает рисковые решения в условиях жесткой конкуренции, добивается предотвращения, ослабления или защиты от существующих или прогнозируемых опасностей или угроз;

– и это убедительно свидетельствует, что в данных условиях оно обеспечивает достижение целей бизнеса.

То есть в данной ситуации корпоративные ресурсы предприятия (земля, капитал, кадровый потенциал, предпринимательские способности менеджеров, информация, интеллектуальная собственность, технология и т.д.) используются в первую очередь для достижения целей бизнеса, а не только для предотвращения опасностей и угроз. И такой путь – это путь достижения стратегических целей предпринимательской деятельности и обеспечения устойчивого интенсивного развития предприятия.

В рыночной экономике производственные единицы обладают полной экономической самостоятельностью. Они сами определяют свою экономическую политику, формируют портфель заказов, организуют производство и сбыт продукции, полностью отвечают за результаты хозяйственной деятельности. Все это, несомненно, актуализирует проблему обеспечения экономической безопасности бизнеса.

В связи с этим очевидно, что обеспечение экономической безопасности производственной деятельности требует, чтобы на предприятии была создана собственная система безопасности.

Давая характеристику системе безопасности предприятия, сразу же определим некоторые, на наш взгляд, важные методологические положения.

Во – первых, система безопасности предприятия не может быть шаблонной. Она должна быть уникальной на каждом предприятии, так как зависит от уровня развития и структуры производственного потенциала, эффективности его использования и направленности производственной деятельности, качественного состояния кадров, производственной дисциплины, состояния окружающей среды, рискованности производства и т.д.

Во – вторых, система безопасности предприятия является самостоятельной, обособленной от аналогичных систем других производственных единиц. Но ее обособленность относительна, поскольку система безопасности предприятия - это составной элемент безопасности более высокого уровня – города, региона, страны. Очень многие задачи безопасности предприятия не могут быть решены самостоятельно, без решений, принимаемых на более высоком системном уровне, и прежде всего государственном. Именно на этом уровне принимаются важнейшие политические, макроэкономические, правовые и другие решения, создающие среду безопасности производственной деятельности. Служба безопасности конкретного предприятия зависит также и от активности служб безопасности конкурентных предприятий, и прежде всего их разведывательных подразделений. Она создается и функционирует на основе принятых законодательных актов, зависит от возможностей приобретения средств защиты, уровня подготовки и квалификации кадров и т.д.

В – третьих, система безопасности предприятия должна быть комплексной. Она призвана обеспечить безопасность экономическую, научно-техническую, кадровую, интеллектуальную, экологическую, информационную, физическую, техногенную, пожарную и т.д. Значит, в ее составе должны быть соответствующие элементы, органы, силы, средства и прочие.

1.2 Создание системы безопасности предприятия

Создание системы безопасности предприятия и организация ее успешного функционирования должны опираться на методологические основы научной теории безопасности.

Целью системы безопасности является своевременное выявление и предотвращение как внешних, так и внутренних опасностей и угроз, обеспечение защищенности деятельности предприятия и достижения им целей бизнеса. Безусловно, что достижение поставленной цели возможно лишь на основе решения комплекса задач.

К наиболее значимым из них можно отнести:

– выявление реальных и прогнозирование потенциальных опасностей и угроз;

– нахождение способов их предотвращения, ослабления или ликвидации последствий их воздействия;

– нахождение сил и средств, необходимых для обеспечения безопасности предприятия;

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

– создание собственной, соответствующей опасностям и угрозам, службы безопасности предприятия и др.

Система безопасности предприятия призвана выполнять определенные функции.

К наиболее значимым из них следует отнести следующие:

– прогнозирование, выявление, предупреждение, ослабление опасностей и угроз;

– обеспечение защищенности деятельности предприятия и его персонала;

– сохранение имущества;

– создание благотворительной конкурентной среды, ликвидация последствий нанесенного ущерба и другие.

Система безопасности предприятия строится на ряде принципов:

1. **Комплексность**, или ***системность***. Этот принцип предполагает создание такой системы безопасности, которая бы обеспечила защищенность предприятия, его имущества, персонала, информации, различных сфер деятельности от всевозможных опасностей и угроз, форс – мажорных обстоятельств,

т.е. система безопасности (ее составные элементы, силы, средства) должна быть достаточной, чтобы обеспечить экономическую, экологическую, научно – техническую, кадровую, пожарную и другие виды безопасности. В обеспечении безопасности предприятия должны принимать участие не только штатные сотрудники и специальные службы, а практически все служащие предприятия. Организационной формой комплексного использования сил и средств должна стать программа обеспечения безопасности предприятия.

2. **Приоритет мер предупреждения** (***своевременность***)

Система безопасности должна быть построена таким образом, чтобы она могла на ранних стадиях выявлять различные деструктивные факторы, принимать меры по предотвращению их вредного воздействия и нанесения ущерба предприятию. Реализация данного принципа экономически значительно выгоднее, чем устранение нанесенного ущерба.

3. **Непрерывность.** Система безопасности должна быть построена таким образом, чтобы она действовала, постоянно защищая интересы предприятия в условиях риска и противодействия злоумышленникам.

4. **Законность.** Все действия по обеспечению безопасности предприятия должны осуществляться на основе действующего законодательства и не противоречить ему. Те меры безопасности, которые разрабатываются на самом предприятии, также должны опираться и осуществляться в рамках действующих правовых актов.

5. **Плановость.** Данный принцип вносит организованность в функционирование системы безопасности. Он позволяет каждому участнику процесса действовать логически последовательно, строго выполняя возложенные на него обязанности. Деятельность по обеспечению безопасности организуется на основе единого замысла, изложенного в комплексной программе и конкретных планах по отдельным направлениям и подвидам безопасности.

6. **Экономность.** Система безопасности должна быть выстроена таким образом, чтобы затраты на ее обеспечение были экономически целесообразными, а стоимость затрат была оптимальной и не превышала тот уровень, при котором теряется экономический смысл их применения.

7. **Взаимодействие.** Для обеспечения безопасности предприятия необходимо, чтобы усилия всех обеспечивающих ее лиц, подразделений, служб были скоординированы. То есть все субъекты, участники данного процесса должны взаимодействовать друг с другом, четко знать, кто за что отвечает и кто что делает. Принцип взаимодействия предполагает также установление тесных деловых контактов и согласование действий с внешними организациями (правоохранительными органами, местными или районными службами безопасности, органами власти и т.д.), способными оказать необходимое содействие в обеспечении безопасности предприятия. Выполнить эту задачу может комитет (группа, совет и т.д.) безопасности предприятия.

8. **Сочетание гласности и конфиденциальности**. Система основных мер безопасности должна быть известна всем сотрудникам предприятия; ее требования должны выполняться. Это даст возможность своевременно выявить и предотвратить потенциальные и реальные опасности и угрозы. В то же время целый ряд способов, сил, средств, методов обеспечения безопасности должен быть законспирирован и известен очень узкому кругу специалистов, что позволит более эффективно бороться как с внутренними, так и внешними угрозами, своевременно предотвращать нанесение ущерба предприятию.

9. **Компетентность.** Вопрос обеспечения безопасности предприятия является жизненно важным. В результате преднамеренных действий злоумышленников, недобросовестной конкуренции, принятия катастрофически рискованных решений и т.д. предприятию может быть нанесен непоправимый ущерб. Поэтому вопросами обеспечения безопасности предприятия должны заниматься не дилетанты, а профессионалы, глубоко знающие сущность проблемы, умеющие своевременно оценить обстановку и принять правильное решение.

Система безопасности предприятия должна строиться в соответствии с проводимой ***политикой и стратегией безопасности***.

Политика безопасности представляет собой систему взглядов, мер, решений, действий в области безопасности, которые создают благоприятные условия для достижения целей бизнеса, т.е. политика безопасности позволяет предприятию выполнять производственную программу, выпускать конкуренто-способную

продукцию (товары, услуги, работы), повышать эффективность производства, преумножать собственность, получать прибыль и т.д.

Под стратегией безопасности понимается совокупность наиболее значимых решений, направленных на обеспечение программного уровня безопасности функционирования предприятия. Стратегии безопасности по своему содержанию бывают различными. Представляется, что можно выделить три типа стратегий безопасности.

Первый – это стратегия, связанная с необходимостью внезапно реагировать на реально возникшие угрозы производственной деятельности, имуществу, персоналу и т.д. То есть в данном случае действует принцип «угроза - отражение». Созданные (часто поспешно) для решения этой задачи подразделения службы, выделенные силы и средства могут ослабить или предотвратить воздействие угроз; в то же время предприятию может быть нанесен ущерб.

Второй – это стратегия, ориентированная на прогнозирование, заблаговременное выявление опасностей и угроз, целенаправленное исследование экономической и криминогенной ситуаций как внутри предприятия, так и в окружающей среде. Выделенные для решения этой задачи специалисты, созданные подразделения и службы безопасности дают возможность осознанно и целенаправленно проводить работу по созданию благоприятных условий для предпринимательской деятельности.

Третий тип – это стратегия безопасности, направленная на возмещение (восстановление, компенсацию) нанесенного ущерба. Данная стратегия может считаться приемлемой лишь тогда, когда ущерб восполним, или тогда, когда нет возможности осуществить стратегии первого или второго типа.

Система безопасности предприятия представляет собой ограниченное множество взаимосвязанных элементов, обеспечивающих безопасность предприятия и достижение им целей бизнеса. Составными элементами такой системы являются объект и субъект безопасности, механизм управления безопасностью, а также стратегические действия по управлению безопасностью.

Объектом безопасности выступает все то, на что направлены усилия по обеспечению безопасности. К объектам следует отнести:

– различные виды деятельности предприятия (производственная, коммерческая, снабженческая, управленческая и др.);

– имущество и ресурсы предприятия (финансовые, материально-технические, информационные, интеллектуальные и др.);

– персонал фирмы, ее руководителей, акционеров, различные структурные подразделения, службы, партнеров, сотрудников, владеющих информацией, составляющей коммерческую тайну, и т.д.

Субъектами безопасности предприятия являются те лица, подразделения, службы, органы, ведомства, учреждения, которые непосредственно занимаются обеспечением безопасности бизнеса. Поскольку деятельность по обеспечению безопасности предприятия многоаспектна, эту задачу невозможно решить с помощью одного – двух органов.

Как правило, к субъектам безопасности предприятия относятся многие органы, которые можно классифицировать по различным признакам:

1. В зависимости от принадлежности:

– на субъекты, занимающиеся этой деятельностью непосредственно на предприятии;

– внешние органы и организации.

2. В зависимости от непосредственного участия:

– на специальные субъекты;

– весь остальной персонал фирмы.

3. В зависимости от воздействия (влияния) на объект безопасности на:

– субъекты прямого назначения;

–косвенного.

4. В зависимости от легитимности на:

– официальные органы;

– криминальные структуры («крыши»),

5. В зависимости от подчиненности на:

– государственные органы;

– негосударственные.

Синтезировав представленную классификацию субъектов безопасности, можно выделить две группы субъектов безопасности.

К первой группе относятся те субъекты, которые входят в структуру самого предприятия и решают задачи по обеспечению его безопасности. В состав этой группы входят специальные субъекты (служба безопасности, или охрана, пожарная команда, спасательная служба), а также весь остальной персонал фирмы, который также заботится о безопасности своего предприятия.

Ко второй группе относятся те субъекты, которые находятся за пределами предприятия и не подчиняются его руководству. Это прежде всего государственные органы, которые создают условия обеспечения безопасности предприятия.

К ним относятся:

1. Законодательные органы – принимают законы, создающие правовую основу деятельности по обеспечению безопасности на уровне государства, региона, предприятия и личности.

2. Исполнительные органы власти – проводят политику, детализируют механизмы безопасности,

3. Судебные органы – обеспечивают соблюдение законных прав предприятия и его сотрудников;

4. Государственные институты – осуществляют охрану границы, таможенный, валютно-экспортный, налоговый контроль и т.п.

5. Правоохранительные органы – ведут борьбу с правонарушениями и преступлениями.

6. Система научно – преобразовательных учреждений – реализует задачи по научным проработкам проблем безопасности и подготовки кадров.

С началом рыночных реформ параллельно с государственными стали образовываться ***негосударственные организации***, агентства, учреждения:

– частные охранные и детективные организации,

– аналитические центры,

– информационные службы,

– учебные, научные и консультационные организации и т.д.

Они, как правило, за плату оказывают услуги по охране объектов, обеспечивают защиту информации, коммерческой тайны, накапливают и представляют информацию о конкурентах, ненадежных партнерах и т.д.

Мировой опыт свидетельствует, что именно негосударственные организации в основном решают задачи по обеспечению безопасности предпринимательства.

Криминализация хозяйственной жизни привела к тому, что на рынке охранных услуг появились и криминальные структуры, так называемые «крыши», которые на основе угроз, шантажа, насилия, погромов, эксплуатируя предпринимателей, втягивают их в криминальный бизнес. Как правило, «крышу» обеспечивает организованная преступная группа, которая за вознаграждение организует прикрытие предприятию или отдельному лицу, имеющему существенные доходы.

Наиболее распространенными видами услуг «крыши» являются:

– защита от притязаний, вымогательств, нападений других организованных преступных групп;

– обеспечение личной безопасности предпринимателей; противодействие конкурентам фирмы;

– улаживание споров с партнерами; взыскание долгов с должников и другие.

Механизм управления экономической безопасностью предприятия представляет собой объективно обусловленную последовательность действий по обеспечению экономической безопасности предприятия. К основным его элементам можно отнести: определение потребностей в обеспечении безопасности, сил и средств, а также организационно-хозяйственного механизма, формулировку целей и задач обеспечения безопасности. Проведение в жизнь выработанных мер обеспечивает достижение поставленных целей.

Формирование системы безопасности, и прежде всего создание ее органов (субъектов), зависит от размеров предприятия, его экономических, финансовых, производственно – технических, информационных, интеллектуальных, профессиональных, организационных и других возможностей. Как показывает опыт, малые предприятия чаще всего пользуются услугами внешних специализированных частных организаций: консалтинговых, охранных, информационных и прочие.

К ним относятся:

– регистрационные палаты,

– фирмы по подбору и аттестации кадров,

– кредитные бюро, оказывающие информационные услуги по деловому реноме партнеров,

– центры маркетинговых исследований,

– частные охранные и детективные организации и др.

Средние предприятия могут использовать ***комбинированную систему безопасности***. С одной стороны, в случае необходимости они могут получать услуги от внешних организаций, а с другой – активно опираться на возможности своих служб и подразделений, в частности, юридической, финансовой, маркетинга, охраны, техники безопасности, кадров, экономического анализа, пропускного режима, делопроизводства и т.д. В целях повышения эффективности деятельности служб и подразделений по защите экономических интересов фирмы на предприятии должен быть создан координирующий (управляющий) орган или назначен один из руководителей, ***отвечающий за экономическую безопасность***. Для крупного предприятия целесообразно создание ***собственной службы безопасности***. Как правило, всю деятельность по обеспечению безопасности координирует ***один*** из руководителей предприятия. Для выработки предложений и выполнения консультативных функций может создаваться совет по безопасности.

Служба безопасности может включать самые разные отделы, группы, подразделения.

К наиболее значимым из них следует отнести следующие подразделения:

– охраны, режима;

– по работе с кадрами,

– инженерно – технической защиты;

– разведки и контрразведки (детективная группа),

– информационно – аналитической деятельности;

– оперативного реагирования;

– кризисную группу и др.

При этом обеспечивается пожарная безопасность, сохранность имущества, предотвращается несанкционированный доступ на объект, осуществляется контроль и другие. С помощью организационных мер создаются специальные подразделения, посты, патрули, зоны безопасности и т.д.

Финансовые средства необходимы для приобретения технических устройств безопасности, содержания службы безопасности, подготовки кадров, стимулирования труда и т.д. Аналогичным образом по прямому назначению должны использоваться и другие силы и средства.

Система безопасности предприятия сможет решать стоящие перед ней задачи только тогда, когда будет действовать, т.е. ее неотъемлемым составным элементом являются практические действия по обеспечению безопасности бизнеса.

Таким образом, в результате рассмотрения системы экономической безопасности предприятия можно сделать следующий вывод: служба безопасности предприятия призвана на основе эффективного использования корпоративных ресурсов создать условия для достижения целей бизнеса, своевременно обнаружить и максимально ослабить воздействие различного рода опасностей и угроз в условиях конкуренции и хозяйственного риска.

Глава 2. Организация системы безопасности предприятия

2.1 Концепция безопасности предприятия

Под концепцией безопасности предприятия понимают научно обоснованную систему взглядов на определение основных направлений, условий и порядка практического решения задач защиты от противоправных действий недобросовестной конкуренции. Концепция является методологической основой политики руководителя организации по ее реализации. На основе сформированных в концепции целей, задач и возможных путей решения формируются конкретные планы обеспечения информационной безопасности предприятия.

Современная концепция безопасности предприятия представлена на рисунке. 2.1.

Рис. 2.1 – Концепция безопасности предприятия

Структура концепции может выглядеть следующим образом.

1. Описание проблемной ситуации в сфере безопасности предприятия:

– перечень потенциальных и реальных угроз безопасности, их классификация и ранжирование;

– причины и факторы зарождения угроз;

– негативные последствия угроз для предприятия.

– механизм обеспечения безопасности:

– определение объекта и предмета безопасности предприятия;

– формулирование политики и стратегии безопасности;

– принципы обеспечения безопасности;

– цели обеспечения безопасности;

– задачи обеспечения безопасности;

–критерии и показатели безопасности предприятия;

–создание оргструктуры по управлению системой безопасности предприятия.

2. Предприятия по реализации мер безопасности:

– формирование подсистем общей системы безопасности предприятия;

– определение субъектов безопасности предприятия и их роли;

– расчет средств и определение методов обеспечения безопасности.

2.1.1 Современная концепция безопасности предприятия

Сформированная на научной основе система безопасности предприятия является организационной основой структурного подразделения – службы безопасности.

Система безопасности представляет собой умение и способность противостоять любым попыткам различных структур нанести ущерб организации, защиту ее интересов от внутренних и внешних угроз.

В своей свое система безопасности является неотъемлемой составной частью деятельности предприятия.

В вопросах защищенности система безопасности представляет собой умение и способность организации надежно противостоять любой деятельности криминальных структур или недобросовестных конкурентов нанести ущерб законным интересам предприятия.

Целями системы безопасности являются:

– обеспечение устойчивого функционирования предприятия и снижение угроз его безопасности,

– защита законных интересов организации от противоправных действий криминальных структур, охрана жизни и здоровья персонала,

– недопущение хищения финансовых и материально – технических средств, уничтожения имущества и ценностей, разглашения, утечки и несанкционированного доступа к информации,

– нарушения работы технических средств обеспечения производственной деятельности, защита средства информатизации.

Система безопасности выполняет следующие функции:

– руководит работами по правовому и организационному регулированию безопасности фирмы и ее структура подразделений;

– участвует в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации;

– разрабатывает документы, регламентирующие порядок и организацию мер безопасности;

– разрабатывает и осуществляет меры по сохранности информации и сведений конфиденциального характер;

– осуществляет контакты с правоохранительными органами и обмен с ними информацией в установленном порядке, целях выполнения задач, возложенных на службу безопасности в интересах изучения криминогенной обстановки;

– проводит, привлекая соответствующие подразделения, служебные расследования по фактам нарушения требований безопасности, несоблюдения правил охраны средств и имущества, разглашения служебной и коммерческой

– организовывает физическую охрану имущества и материальных ценностей;

– осуществляет выявление и локализацию возможных каналов утечки информации;

– осуществляет контроль за соблюдением требований по защите коммерческой тайны;

– выполняет разработку и осуществляет меры по защите информации при ее обработке средствами вычислительной техники;

– организует обучение и проверку уровня подготовки специалистов по вопросам безопасности;

– участвует в разработке приказов, распоряжений и других документов по вопросам безопасности.

Служба безопасности действует на основе следующих организационно – правовых документов:

– распоряжения о системе собственной безопасности;

– правил мер защиты конфиденциальной информации;

– инструкций о порядке работы с иностранными специалистами;

– правил по инженерно – технической защите помещений и технических средств.

Для обеспечения достижения целей предприятия, в том числе в области безопасности важное значение имеют вопросы безопасности. Это обусловлено тем физической, экономической, информационной и экологической безопасностью отсутствие которых могут привести к возникновению различных видов ущербов, характер и уровень конкурентоспособности и эффективность хозяйственной дел, что может встать вопрос о его банкротстве и ликвидации.

В Словаре русского языка С.И. Ожегова это понятие определяется следующим – это положение, при котором не угрожает опасность кому – чему - либо;

Для решения задач управления безопасностью необходимо однозначно определить термин «безопасность», поскольку на практике оно часто толкуется в двух вариантах:

1. Как безопасность соответствующих видов объектов от внешних угроз которые нуждаются в защите;

2. Как причисление соответствующих объектов к возможным источникам являющихся внешними по отношению к ним (т.е. отданных объекту).

Анализ определений «безопасность» включает в себя существенные, базовые терминологические элементы, которые помогут в определении понятия «безопасности предприятия».

Во – первых, большая часть авторов под безопасностью понимают состояние объекта опасности.

Во – вторых, безопасность часто рассматривается как способность объекта, явления, процесса сохранить свои характеристики в условиях целенаправленного, разрушающего воздействия, направленного из вне.

В – третьих, безопасность – категория системная, поскольку является свойством системы, построенной на процессах саморегуляции, целостности. Отсюда роль безопасности заключается в защите каждого из этих свойств системное воздействие на любое из этих свойств приведет к гибели системы в целом.

В – четвертых, безопасность рассматривается как решающее условие (гарант) жизнедеятельности личности позволяет им сохранять и умножать их материальные и духовные ценности.

В – пятых, безопасность в абсолютном своем выражении – отсутствие опасностей и угроз материальной безопасности и других;

В – шестых, базовым элементом всех определений выступает угроза как реальный признак существования опасности.

Отсюда следует, что угроза и борьба с ней являются сущностью безопасности.

Под опасностью понимаются возможные или реальные явления, события и процессы, способные нанести группе, народу, обществу, государству, человеческому сообществу и Земле или даже уничтожить их, нанес разрушить материальные, духовные или природные ценности, вызвать деградацию, закрыть путь к развитию охватывает также явления, процессы и действия, которыми люди наносят вред природе, а природа людям.

Опасность может выступать в различных формах, а именно в виде намерений, планов подготовки действий направленных на подчинение, ослабление, уничтожение объектов безопасности и т.д. Количество признаков может быть увеличено или уменьшено в зависимости от целей анализа. Например, признаками опасности объекта, являются:

– угроза для жизни;

– возможность нанесения ущерба здоровью;

– нарушение условий нормального функционирования органов и систем организма человека.

Опасность понятие относительное и носит потенциальный (т.е. скрытый) характер, ее актуализация происходит при определенных условиях, именуемых *причинами*. Триада «опасность – причины – нежелательные следствия» процесс развития, реализующий потенциальную опасность в реальный ущерб (последствие). Как правило, многопричинными, т.е. одна и та же опасность может реализоваться в нежелательное событие через разные нежелательные события составляет поиск причин.

Понятие «угроза» родственно понятию «опасность». Угроза – это опасность на стадии перехода из возможно высказанного намерения или демонстрации готовности одним из субъектов нанести ущерб другим.

В методологическом аспекте не угрозы, а причины опасности, которые обусловлены имеющимися ключевыми для идентификации опасностей и дея-

тельности по защите от них. Таким образом, угрозу следует принимать как имеющиеся и формирующиеся в человеке, коллективе, обществе, в межличностных, общественных групп в отношениях противоречий. Без выявления и решения этих противоречий никакая безопасность обеспечена не будет.

Угроза всегда носит предметный характер, наполнена конкретным содержанием и в случае четко выражена, она может приобретать конкретную правовую характеристику. Эта характеристика чаще всего фиксируется в законах кодекса об измене Родине, терроризме, контрабанде и т.д.).

Системный, проблемный и факторный анализ зарождающихся и затухающих противоречий, характера их проявления на состояние безопасности на каждый конкретный период, определять стратегию ее обеспечения на более длительные сроки, реагировать на имеющиеся и потенциальные угрозы.

Например, с помощью факторного анализа можно выделить и сгруппировать факторы дестабилизирующего характера, а затем разработать и реализовать конкретные меры в системе обеспечения безопасности, например подавление дестабилизирующих факторов и стимулирование действия стабилизирующих факторов. В этом защитная функция обеспечения безопасности, сколько способствующая позитивному развитию.

Количественной оценкой опасности является риск, который определяется частотой или вероятностью возникновения риска связанного с опасностью, при наступлении другого. По мнению специалистов, использование риска в качестве количественной оценки, предпочтительнее чем использование традиционных показателей.

Поскольку обеспечить нулевой риск в действующих системах абсолютно невозможно, то во всех сферах деятельности людей чаще всего имеет место осознанный риск. В этом случае имеет место концепция приемлемого (допустимого) риска, сущность которого заключается в стремлении к такой безопасности, которую приемлет индивид или общество в данный период времени.

Следует отметить, что восприятие человеком и обществом риска и опасностей субъективно. Например, общество болезненно реагирует на редкие, но которые сопровождаются большим числом единовременных жертв. В то же

время частые события где погибают единицы или небольшие группы людей, не вызывают столь напряженного негативного отношения.

Например, на фоне того, что ежедневно на производстве погибает от 40 до 50 человек, а в целом по стране лишаются жизни более 1000 человек в день, новость о гибели более десятка человек в одной аварии отмечается в средствах массовой информации, вызывает более выраженную реакцию со стороны населения.

Данное явление необходимо иметь в виду при рассмотрении проблемы приемлемого риска. Субъективное мнение при оценке риска вызывает необходимость использования приемов и методологий, лишенных этого недостатка.

На практике применяются следующие методологические подходы к определению риска:

– инженерный (опирающийся на статистику);

– вероятностный анализ безопасности, построенных на решении вероятностных задач;

– модельный (основанный па построении моделей воздействия вредных факторов на отдельного человека);

– экспертный (когда вероятность событий определяется на основе опроса опытных специалистов, т.е. экспертов;

– социологический (основанный на опросе населения).

Для получения объективных результатов оценки рисков целесообразно применять указанные методы в комплексе.

При разработке концепций и систем управления безопасностью предприятия следует иметь ввиду, что системы повышения безопасности технических систем небезграничны, поэтому приемлемый риск сочетает в себе социальные и политические аспекты и представляет некоторый компромисс между уровнем безопасности.

Например, при увеличении затрат на технические мероприятия технический риск снижается, но растет социальный риск, поскольку эти средства могли бы быть направлены на решение социальных проблем работников. Таким образом предприятию необходимо соблюдать оптимальное соотношение между ин-

вестициями в техническую и социальную безопасности предприятия. При этом критерием решения является минимальная величина суммарного риска, что необходимо учитывать при выборе уровня риска, который должен быть приемлем для предприятия с точки технических и других возможностей и удовлетворять требованиям заинтересованных сторон (например, техническим регламентам, стандартам, договорам, а также требованиям общественности и населения).

В некоторых зарубежных странах официально и неофициально используются приемлемые уровни риска либо риска гибели людей и экономические эквиваленты человеческой жизни. Например, максимально приемлемым считается тот, при котором может пострадать 5% видов биогеоценоза. В Голландии в законодательном порядке риски индивидуального риска гибели (максимально приемлемым уровнем считается 10^{-6} в год, пренебрегая тем, что человеческая жизнь оценивается от 650 тыс. до 7 млн. долл. США, что отражает количество средств, на спасение одной человеческой жизни.

Следует отметить, что на практике приемлемые риски на 2 – 3 порядка «строже» фактических и поэтому их направляют на реальную защиту людей и окружающей природной среды.

Многообразие опасностей, угроз и источников их возникновения (образования) требует их классификации, целесообразно группировать опасности и угрозы по следующим признакам:

1. По направленности против определенных субъектов, их интересов и потребностей, а также против техногенных и природных опасностей.

2. По отношению к объектам воздействия (внутренние, внешние, аутоугроза).

3. По сферам действия (экология, экономика, социальная область, культурология и т.д.).

4. По масштабам (глобальные, региональные, государственные, местные и т.д.).

5. По способам и формам проявления (заявления, конкретные действия, совокупность обстоятельств, которые в перспективе и требуют защитного реагирования и т.д.).

6. По источникам и движущим силам (обусловленные деятельностью людей, природные и т.д.).

7. По ожиданию воздействия на объекты (внезапные, неожиданные; ожидаемые с малым временем задержки).

8 По умыслу (правомерная, т.е. вытекающая из реализации правовых норм, противоправная, внеправовая).

9. По форме (прямая, косвенная, завуалированная, манифестированная, латентная, несформировавшаяся).

10 По времени (мгновенная, длящаяся, дискретная, «законсервированная»).

11 По последствиям (необратимая, обратимая, мутагенная, доминантная, катализирующая).

12. По значению (допустимая, недопустимая).

13. По составу (разовая, бинарная, кумулятивная, диффузная).

14. По природе происхождения (социальная, техногенная, природная).

15. По актуализации (вероятная, потенциальная, реальная, осуществленная).

16. По причинности (закономерная, случайная).

С учетом вышесказанного, так же в контексте задач по управлению комплексной безопасностью предприятия понятия безопасности можно сформулировать следующим образом.

Безопасность предприятия – эго состояние защищенности структурных элементов предприятия, ключевых форм деятельности и конкурентоспособности, которое достигается, поддерживается и/или улучшается по выявлению (идентификации), предупреждению, ослаблению, устранению (ликвидации) и отражению внешних угроз, способных нанести неприемлемый (недопустимый в данный период времени) ущерб законным интересам предприятии выражаемых , в том числе, в потребности его самосохранения и развития.

Таким образом, исходя из определения, субъектами правоотношений при решении проблемы безопасности могут быть:

– государство как собственник ресурсов, создаваемых, приобретаемых и накапливаемых за счет средств и информационных ресурсов, отнесенных к категории государственной тайны;

– юридические и физические лица, являющиеся владельцами предприятия;

– юридические и физические лица, участвующие или заинтересованные в результатах деятельности предприятия;

– правовые отношения (поставщики, партнеры, клиенты, частные охранно – детективные структуры, надзор государственной власти и т.д., включая зарубежных представителей контактной аудитории предприятия;

– физические лица, относящиеся к руководству и персоналу предприятия.

К основным объектам безопасности на предприятии относятся:

– владельцы (от решений которых зависит сохранение целостности и возможности стратегического развит кадрового состава руководства и т.п.);

– влиятельные поставщики, партнеры и клиенты предприятия (от решений которых зависит получение высокого качества продукции, достижение и поддержание престижа и общественной репутации предприятия, а так же задержки с оплатой отгруженной продукции, невозврата крупных кредитных ссуд и т.п.);

– персонал предприятия (руководящие работники, производственный и обслуживающий персонал, от работы которых зависит финансовое состояние предприятия и/или которые осведомлены о сведениях, составляющих коммерческую тайну и другие).

– финансовые ресурсы (денежные средства, ценные бумаги и т.п., от сохранности которых зависит финансовая безопасность, предприятия, возможности по решению социально – экономических проблем, а также стратегическое разрушение;

– производственные и материальные средства (ценное имущество предприятия);

– нематериальные активы (в том числе «ноу – хау», методы, модели, программы для ЭВМ и т.п.)

– информационные ресурсы (информация с ограниченным доступом, составляющая коммерческую тайну предоставленная в виде документов и массивов данных независимо от формы и вида их представления, поля различного характера);

– средства и системы информатизации (автоматизированные системы и вычислительные сети различного телеграфной, телефонной, факсимильной, ра-

дио– космической связи, технические средства передачи отображения информации, вспомогательные технические средства и системы).

Все объекты, в отношении которых могут быть осуществлены угрозы безопасности или противоправные действия, имеющие потенциальную уязвимость с точки зрения возможного материального или морального ущерба. Исходя из этого опасности классифицированы по уровням уязвимости (опасности) и степени риска.

На практике наибольшей уязвимостью обладают финансовые средства, особенно в процессе транспортирования, некоторые категории персонала.

В процессе выявления, анализа и прогнозирования потенциальных угроз интересам предприятия учитываются внешние и внутренние факторы (условия), влияющие на его безопасность. Например, в настоящее время существуют следующие ***внешние неблагоприятные по отношению к предприятию факторы***:

– нестабильная политическая, социально – экономическая обстановка и обострение криминогенных ситуаций;

– невыполнение законодательных актов, правовой нигилизм, отсутствие ряда законов по жизненно важным вопросам;

– снижение моральной, психологической и производственной ответственности граждан.

Для концептуального понимания вопросов безопасности предприятия рассмотрим наиболее общий состав потенциальных угроз.

По отношению к отдельному предприятию различаются следующие виды внешних угроз:

– недобросовестные конкуренты

– преступные группы и формирования

– противозаконные действия отдельных лиц и организаций административного аппарата, в том числе начальствующего состава.

– промышленный шпионаж, хакерские атаки на информационные системы предприятия.

Внутренние угрозы можно классифицировать следующим образом:

– преднамеренные преступные действия персонала самого предприятия;

– непреднамеренные действия и ошибки сотрудников;

– отказ производственного оборудования и технических средств, включая системы охраны и защиты материальных ценностей;

– сбои программного обеспечения средств обработки информации.

Соотношение внутренних и внешних угроз для предприятия по экспертной оценке может быть охарактеризовано показателями:

– 81,7% угроз совершается либо самими сотрудниками организации, либо при их прямом или опосредованном участием;

– 17,3% – внешние угрозы или преступные действия;

– 1,0% – угрозы со стороны случайных лиц.

В общем плане к угрозам безопасности личности относятся:

– похищения и угрозы похищения владельцев, клиентов и персонала предприятия, членов их семей и близких;

– убийства;

– психологический террор, угрозы, запугивание, шантаж, вымогательство;

– нападение с целью завладения денежными средствами, ценностями и документами.

Реализованные угрозы личной безопасности персонала, как правило, приводят к крупным экономическим предприятиям (например, утрата ценных работников, затраты на возмещение работникам и членам их семей понесенной: материального ущерба, включая утрату здоровья и пр.). Ярким примером здесь могут служить убийства ряда российских банкиров.

Угрозы материальным ценностям проявляются в:

– краже продукции;

– в нападении, вторжении, захвате, пикетировании, блокировании, повреждении (уничтожении) зданий, и другого недвижимого имущества;

– выводе из строя средств связи и систем коммунального обслуживания предприятия;

– краже, угоне и уничтожении транспортных средств, принадлежащих предприятию;

– авариях, пожарах (поджогах).

Цель подобных акций заключается в:

– нанесении серьезного морального и материального ущерба руководству и персоналу предприятия;

– срыве на длительное время нормального функционирования предприятия;

– вымогательстве значительных сумм денег или каких-либо льгот (кредиты, отсрочка или погашение плат совершения противоправных действий.

Эта категория угроз приводит в случае их актуализации к наиболее явному и наиболее значительному имиджу предприятия.

Угрозы финансовым ресурсам проявляются в виде:

– хищения финансовых средств из касс и инкассаторских машин;

– невозврата кредитных ссуд (в том числе путем криминальных банкротств);

– мошенничества со счетами, фальсификации валюты;

– подложных платежных документов и пластиковых карт;

– взимания незаконных налогов, штрафов и прочее.

Угрозы информационным ресурсам проявляются в виде:

– разглашения конфиденциальной информации;

– утечки конфиденциальной информации через технические средства обеспечения производственной деятельности;

– несанкционированного доступа к охраняемым сведениям со стороны конкурентных организаций и прессы;

– неправомерного ознакомления с охраняемыми сведениями (составляющими коммерческую тайну);

– изменения информации с криминальными целями

– уничтожения информации с целью нанесения морального и материального ущерба предприятию и его представителям;

Осуществление угроз информационным ресурсам может быть произведено:

– путем неофициального доступа и съема конфиденциальной информации;

– путем подкупа лиц, работающих на предприятии или в структурах, непосредственно связанных с его безопасностью;

– путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники разведки и съема информации, несанкционированного доступа к информации и преднамеренных программ;

– путем подслушивания конфиденциальных переговоров, ведущихся в служебных помещениях, служебных кабинетах и дачах;

– через переговорные процессы между иностранными или отечественными фирмами, используя неосторожность;

– через отдельных сотрудников предприятия, стремящихся заполучить больший, чем их зарплата, доход и заинтересованность.

Далее рассмотрим основные способы и технические средства, которые могут быть использованы в системе предприятия для выявления (идентификации), предупреждения, ослабления, устранения (ликвидации) опасностей и угроз, способных нанести неприемлемый (недопустимый в данный период времени) ущерб (рис. 2.2).

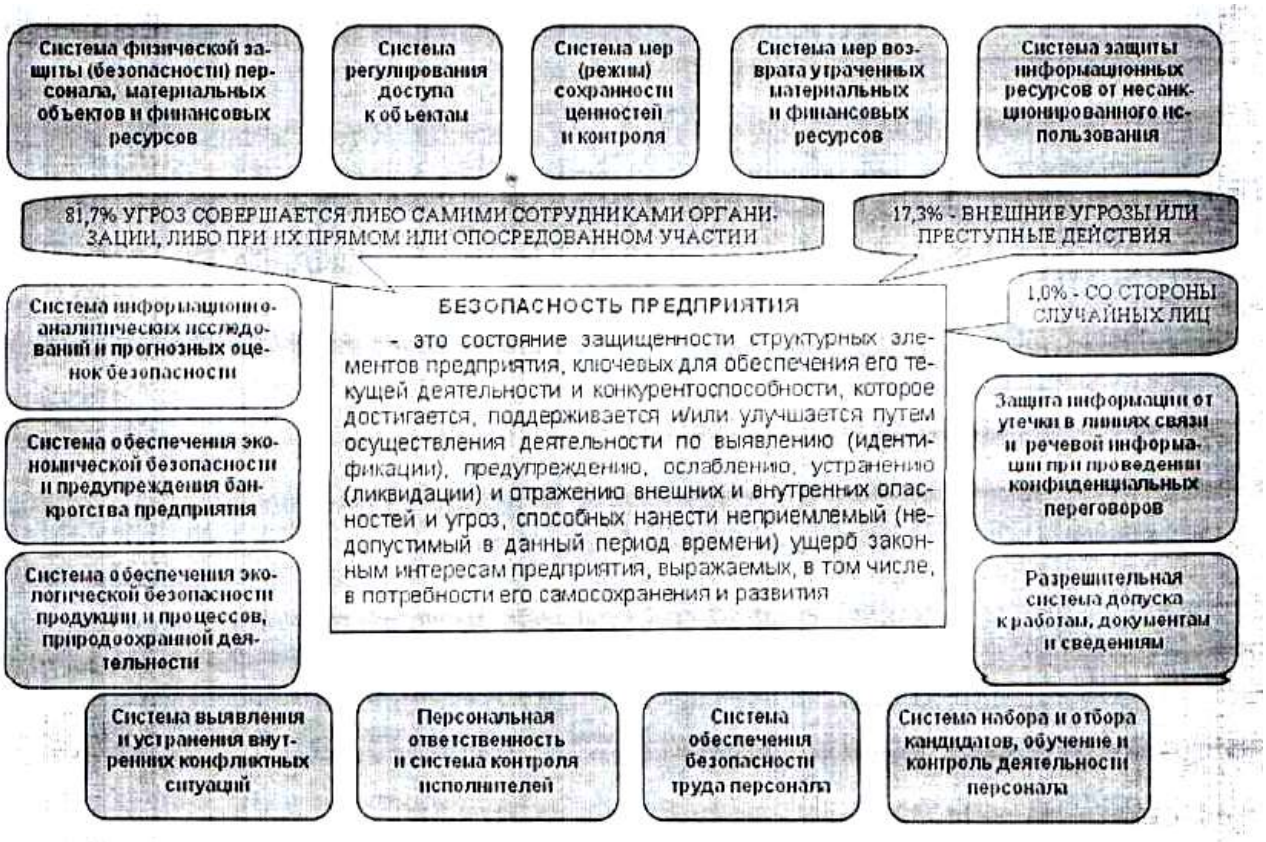

Рисунок 2.2 – Основные компоненты системы безопасности предприятия

2.2 Организация системы безопасности предприятия

Созданию службы безопасности предприятия обычно предшествуют два события:

– либо это острое желание руководителей предприятия отреагировать на внезапно возникшие реальные угрозы имущества до расправы с персоналом;

– либо это основанный на результатах исследования вывод о неудовлетворительной деятельности предприятия.

В первом случае созданная поспешно служба безопасности способна в некоторой степени отразить угрозы и в дальнейшем реагировать на их появление по принципу "угроза – отражение". Дело меняется существенным образом при реализации **Второго варианта**. После детального изучения состояния безопасности предприятия, с привлечением специалистов, если их нет на предприятии, у его руководителей появится реальное представление о системе безопасности предприятия.

Такое системное представление позволяет осознанно и целенаправленно проводить работу по обеспечению безопасности предпринимательской деятельности и самого предприятия всеми его подразделениями и сотрудниками. При этом ведущая роль службы безопасности не исчезает, наоборот, понимание своей роли и места в системе безопасности предприятия приведет только к положительным результатам.

Следует, однако, подчеркнуть, что до настоящего времени нет единого подхода к определению понятия "система безопасности предприятия". Чтобы дать такое определение, необходимо предварительно выявить элементы этой системы. Изучение научной литературы и практики позволяют прийти к выводу, что структурными элементами системы безопасности предприятия являются научная теория безопасности, политика и стратегия безопасности, средства и методы обеспечения безопасности и, наконец, концепция безопасности предприятия.

Совокупность вышеперечисленных элементов составляет систему безопасности предприятия.

2.2.1 Научная теория безопасности предприятия

Понятие безопасности приведено в ст. 1 Закона РФ от 5 марта 1992 года "О безопасности": "состояние защищенности жизненно интересов личности, общества и государства от внутренних и внешних угроз". Раскрытие этого понятия через термин "защищенность" значительно суживает ее смысл, подчеркивает пассивность при реагировании на угрозы. Сущность безопасности, как представляется, связана с понятиями "развитие" и "устойчивость". В связи с этим под безопасностью следует понимать состояние объекта (в нашем случае – предприятия) в системе его связей с точки зрения способности к устойчивости (самовыживанию) и развитию в условиях внутренних и внешних угроз, действий непредсказуемых и трудно прогнозируемых факторов. Отталкиваясь от этого понятия, определим следующие функции **безопасности:** выявление, предупреждение, снижение, ослабление, нейтрализация, пресечение, локализация, отражение и устранение угроз.

Под угрозой безопасности предприятия следует понимать потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его деятельности. Угрозу можно классифицировать по различным основаниям и измерить их в количественных параметрах. Например, возможный ущерб оценивается числом погибших людей, потерявших (ухудшивших) здоровье, денежной сумме экономических потерь и т. д.

По степени вероятности **угроза** оценивается как невероятная, маловероятная, вероятная, весьма вероятная и вполне вероятная.

По степени развития угроза проходит четыре этапа: возникновение (зарождение), экспансия, стабилизация и ликвидация.

Отдаленность угрозы во времени определяется как непосредственная, близкая (до 1 года) и далекая (свыше 1 года), а отдаленность в пространстве – территория предприятия, прилегающая к предприятию территория, территория региона, территория страны, зарубежная территория.

Темпы нарастания угрозы измеряются по месяцам, кварталам, годам.

Напряженность угрозы отражается в двух измерениях:

– нормальная, повышенная, близкая к пределу (порог), избыточная,

– рост, стабильность или снижение.

Кроме этого, угрозы делятся по природе их возникновения на два класса:

1. Естественные (объективные), т. е. вызванные стихийными природными явлениями, не зависящими от человека ч (наводнения, землетрясения, ураганы и т. п.);

2. Искусственные (субъективные), т. е. вызванные деятельностью человека непреднамеренные (неумышленные) и преднамеренные (умышленные) угрозы.

Различают также экономические, социальные, правовые, организационные, информационные, экологические, технические и криминальные угрозы.

Под объектом безопасности предприятия следует понимать степень устойчивости и развития предприятия, его способность противостоять угрозам.

В объекте безопасности предприятия можно выделить:

– различные структурные подразделения или группы сотрудников либо владельцы акций предприятия;

– ресурсы предприятия (информационные, кадровые, материально-технические, информационные, интеллектуальные и финансовые);

– различные виды деятельности (управленческая, производственная, снабженческая и т. д.).

Целью обеспечения безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, дозволяющее ему успешно функционировать в нестабильных условиях внешней и внутренней среды.

Достижение этой цели требует реализации следующих задач:

– выявление угроз для стабильности и развития предприятия и выработка мер по их противодействию;

– обеспечение защиты технологических процессов;

– реализация мер противодействия всех видов шпионажа (промышленного, научно-технического, экономического и т. д.);

– своевременное информирование руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных

органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия;

– предупреждение переманивания сотрудников предприятия, обладающих конфиденциальной информацией;

– всестороннее изучение деловых партнеров;

–своевременное выявление и адекватное реагирование на дезинформационные мероприятия;

– разработка, усовершенствование локальных правовых актов, направленных на обеспечение безопасности предприятия;

– реализация мер по защите коммерческой и иной информации;

– организация мероприятий по противодействию недобросовестной конкуренции;

– обеспечение защиты всех видов ресурсов предприятия;

– реализация мер по защите интеллектуальной собственности;

– организация и проведение мер по предотвращению чрезвычайных ситуаций;

– выявление негативных тенденции 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;

– разработка и реализация мер по предупреждению угроз физической безопасности имуществу предприятия и его персоналу;

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

Система безопасности предприятия может быть построена на основе следующих принципов:

1. **Приоритет мер предупреждения.** Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих

развитию угроз, на основе анализа которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

2. **Законность.** Меры безопасности предприятия разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

3. **Комплексное использование сил и средств.** Для обеспечения безопасности используются все имеющиеся в распоряжении Предприятия силы и средства. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа обеспечения безопасности предприятия.

4. **Координация и взаимодействие внутри и вне предприятия.** Меры противодействия угрозам осуществляются на основе взаимодействия и скоординированности усилий всех подразделений, служб предприятия, а также установления необходимых контактов: с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности Предприятия. Организовать координацию и взаимодействие внутри и вне предприятия может комитет (группа совет и т. д.) безопасности предприятия.

5. **Сочетание гласности с конспирацией.** Доведение до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль – предотвращение потенциальных и реальных угроз. Такая гласность, однако должна непременно дополняться в оправданных случаях мерами конспиративного характера.

6. **Компетентность.** Сотрудники и группы сотрудников должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

7. **Экономическая целесообразность.** Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

8. **Плановая основа деятельности.** Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения

безопасности предприятия, подпрограмм обеспечения безопасности пр основным его видам (экономическая, научно – техническая, экологическая, технологическая и т.д. и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников, защита безопасность угроза.

9 .**Системность.** Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств

Система безопасности предприятия включает в себя ряд следующих подсистем:

1. **Экономическая безопасность** - состояние наиболее эффективного использования всех видов ресурсов в целях предотвращения (нейтрализации, ликвидации) угроз и обеспечения стабильного функционирования предприятия в условиях рыночной экономики.

2. **Техногенная безопасность** – совокупность действий по обеспечению проектирования, строительства и эксплуатации сложных технических устройств с соблюдением необходимых требований безаварийной их работы.

3. **Экологическая безопасность** – состояние защищенности жизненно важных интересов персонала предприятия и его имущества от потенциальных или реальных угроз, создаваемых последствиями антропогенного воздействия на окружающую среду, а также от стихийных бедствий и катастроф.

4. **Информационная безопасность** – это способность персонала предприятия обеспечить защиту информационных ресурсов и потоков от угроз несанкционированного доступа к ним).

5. **Психологическая безопасность** – состояние защищенности от негативных психологических воздействий персонала предприятия и других лиц, вовлеченных в ее деятельность.

6. **Физическая безопасность** – состояние защищенности жизни и здоровья отдельных лиц (групп, всех лиц) предприятия от насильственных преступлений.

7. **Научно – техническая безопасность** – способность персонала предприятия обеспечить защиту собственной ценной научно- технической продукции от недобросовестных конкурентов.

8. **Пожарная безопасность** – состояние объектов предприятия, при котором меры предупреждения пожаров и противопожарной защиты соответствуют нормативным требованиям.

Следует отметить, что вышеуказанные подсистемы второго уровня могут включать в себя подсистемы третьего уровня. Например, подсистемами экономической безопасности могут быть финансовая, коммерческая, имущественная и другие подсистемы безопасности.

Кроме этого, сами подсистемы не разделены между собой непроходимой границей, поскольку они настолько взаимосвязаны друг с другом, что в органическом единстве образуют единую систему безопасности предприятия. Разделение же единой системы безопасности предприятия на подсистемы второго и третьего уровня производится из методических соображений, (кэфФльку это позволяет более детально изучить все его элементы.

Надежность и эффективность системы безопасности предприятия оценивается на основе одного критерия – степени отсутствия или наличия нанесенного ему материального ущерба и морального вреда.

Содержание этого критерия раскрывается через ряд показателей:

– недопущение фактов утечки (разглашения) конфиденциальных сведений;

– предупреждение или пресечение противоправных действий со стороны персонала предприятия, его посетителей, клиентов, сохранность имущества и интеллектуальной собственности предприятия;

– предупреждение чрезвычайных ситуаций;

– пресечение насильственных преступлений в отношении отдельных (специально выделенных) сотрудников и групп сотрудников предприятия;

– своевременное выявление и пресечение попыток несанкционированного проникновения на охраняемые объекты предприятия.

2.3 Политика и стратегия безопасности предприятия

Политика безопасности предприятия – это общие ориентиры для действий и принятия решений, которые облегчают достижение целей. Таким образом, для установления этих общих ориентиров необходимо первоначально сформулировать цели обеспечения безопасности предприятия (общая цель нами уже определена ранее).

Такими целями могут быть:

– укрепление дисциплины труда и повышение его производительности;

– защита законных прав и интересов предприятия;

– укрепление интеллектуального потенциала предприятия;

– сохранением приумножение собственности;

– повышение конкурентоспособности производимой продукции;

– максимально полное информационное обеспечение деятельности предприятия и повышение его эффективности;

– ориентация на мировые стандарты и лидерство в разработке и освоении новой технологии и выпускаемой продукции;

– выполнение производственных программ;

– оказание содействия управленческим структурам в достижении целей предприятия;

– недопущение зависимости от случайных и недобросовестных деловых партнеров.

С учетом вышеизложенного можно определить следующие общие ориентиры для действий и принятия решений, которые облегчают достижение этих целей:

– сохранение и наращивание ресурсного потенциала;

– проведение комплекса превентивных мероприятий по повышению уровня защищенности собственности и персонала предприятия;

– включение в деятельность по обеспечению безопасности предприятия всех его сотрудников;

– профессионализм и специализация персонала предприятия;

– приоритетность не силовых методов предотвращения и нейтрализации угроз.

Для успешного выполнения этой политики необходимо реализовать стратегию безопасности предприятия, под которой понимается совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия.

Выделяются следующие типы стратегий безопасности:

– ориентированные на устранение существующих или предотвращение возникновения возможных угроз;

– нацеленные на предотвращение воздействия существующих или возможных угроз на предмет безопасности;

– направленные на восстановление (компенсацию) наносимого ущерба.

Первые два типа стратегий предусматривают такую деятельность по обеспечению безопасности, в результате которой не происходит угрозы либо создается заслон ее влиянию. В третьем случае ущерб допускается (возникает), однако он компенсируется действиями, которые предусматривает соответствующая стратегия. Совершенно очевидно, что стратегии третьего типа могут разрабатываться и реализовываться применительно к ситуациям, где ущербы восполняемы, либо тогда, ’ когда нет возможности осуществить какую – либо программу реализации стратегий первого или второго типа.

2.4 Субъекты безопасности предприятия

Обеспечением безопасности предприятия занимаются две группы субъектов.

Первая группа занимается этой деятельностью непосредственно на предприятии и подчинены его руководству. Среди этой группы можно выделить специализированные субъекты (совет или комитет безопасности предприятия, служба безопасности, пожарная часть, спасательная служба и т. д.), основным предназначением которых является постоянная профессиональная Деятельность по обеспечению безопасности предприятия (в рамках своей компетен-

ции). Другую часть субъектов этой группы условно можно назвать полуспециализированной, т. к. часть функций этих субъектов предназначена для обеспечения безопасности предприятия (медицинская часть, юридический отдел и т. д.). Наконец, к третьей части этой группы субъектов относится весь остальной персонал и подразделения предприятия, которые в рамках своих должностных инструкций и положений о подразделениях обязаны принимать меры к обеспечению безопасности. Следует иметь в виду, что эффективно обеспечивать безопасность предприятия эти субъекты могут только в том случае, если цели, задачи, функции, права и обязанности будут распределены между ними таким образом, чтобы они не пересекались друг с другом.

Ко второй группе субъектов относятся внешние органы и организации, которые функционируют самостоятельно и не подчиняются Руководству предприятия, но при этом их деятельность оказывает существенное (положительное или отрицательное) влияние на безопасность предприятия.

Субъектами этой группы являются:

1. **Законодательные органы.** Принятые на уровне Российской Федерации и субъектов Федерации законы составляют правовую основу деятельности по обеспечению безопасности предприятия.

2. **Органы исполнительной власти.** Принятые на уровне этих органов подзаконные акты во многом дополняют, уточняют, детализируют требования, законов.

3. **Суды.** Судебные органы обеспечивают соблюдение законных прав и интересов предприятия, в т. ч. в сфере безопасности.

4. **Правоохранительные органы.** Такие органы осуществляют борьбу с правонарушениями, которые отрицательным образом влияют на состояние безопасности предприятия.

5. **Научно – образовательные учреждения.** Последние (особенно негосударственные образовательные учреждения для Подготовки частных охранников и детективов) призваны обеспечить научно – методическую проработку проблем безопасности предприятия и подготовку соответствующих специалистов в сфере безопасности предприятий.

Совершенно очевидно, что субъекты второй группы по своей инициативе подключаются эпизодически (или никогда) к деятельности предприятия по обеспечению своей безопасности. Организационной формой такого подключения может стать комплексная программа безопасности предприятия, в которой необходимо предусмотреть формы и методы этой работы.

Кроме того, можно рекомендовать разработку планов структурных подразделений и всего предприятия в целом по организации взаимодействия с вышеуказанными органами и организациями.

2.5 Средства и методы обеспечения безопасности предприятия

Среди существующих средств обеспечения безопасности можно выделить следующие:

1. **Технические средства.** К ним относятся охранно-пожарные системы, видео-радиоаппаратура, средства обнаружения взрывных-устройств, бронежилеты, заграждения и т. д.

2. **Организационные средства.** Создание специализированных оргструктурных формирований, обеспечивающих безопасность предприятия.

3. **Информационные средства.** Прежде всего это печатная и видеопродукция по вопросам сохранения конфиденциальной информации. Кроме этого, важнейшая информация для принятия решений по вопросам безопасности сохраняется в компьютерах.

4. **Финансовые средства.** Совершенно очевидно, что без достаточных финансовых средств невозможно функционирование системы безопасности, вопрос лишь в том, чтобы использовать их целенаправленно и с высокой отдачей.

5. **Правовые средства.** Здесь имеется ввиду использование не только изданных вышестоящими органами власти законов и подзаконных актов, но также разработка собственных, так называемых локальных правовых актов по вопросам обеспечения безопасности.

6. **Кадровые средства.** Имеется в виду, прежде всего достаточность кадров, занимающихся вопросами обеспечения безопасности. Одновременно с

этим решают задачи повышения их профессионального мастерства в этой сфере деятельности.

7. **Интеллектуальные средства.** Привлечение к работе высококлассных специалистов, научных работников (иногда целесообразно привлекать их со стороны) позволяет внедрять новые системы безопасности.

Следует заметить, что применение каждого из вышеуказанных средств в отдельности не дает необходимого эффекта, он возможен только на комплексной основе. В то же время необходимо отметить, что одновременной внедрение всех вышёуказанных средств в принципе невозможно. Оно проходит обычно ряд этапов:

I этап. Выделение финансовых средств.

II этап: Формирование кадровых и организационных средств.

III этап. Разработка системы правовых средств.

IV этап. Привлечение технических, информационных и интеллектуальных средств.

Переведенные из статичного в динамичное состояние вышеуказанные средства становятся методами, т. е. приемами, способами действия. Соответственно, можно говорить о технических, организационных, информационных, финансовых, правовых, кадровых и интеллектуальных методах.

Приведем краткий конкретный перечень этих методов:

1. Технические – наблюдение, контроль, идентификация и т. д.;

2. Организационные – создание зон безопасности, режим, расследование, посты, патрули и т.д.

3. Информационные – составление детективами характеристик на сотрудников, аналитические материалы и учеты конфиденциального характера.

4. Финансовые – материальное стимулирование сотрудников, имеющих достижения в обеспечении безопасности, денежно поощрение информаторов и т. д.

5. Правовые – судебная защита законных прав и интересов, содействие правоохранительным органам и т. д.;

6. Кадровые – подбор, расстановка и обучение кадров, обеспечивающих безопасность предприятия, их воспитание и т. д.

6. Интеллектуальные – патентование, ноу – хау и т.д.

2.6 Организация концепция безопасности предприятия

После изучения всех вышеописанных элементов системы безопасности предприятия необходимо перейти к составлению ее **концепции**. Как известно, концепция определяется как система взглядов, идей, целевых установок, пронизанных единым, определяющим замыслом, ведущей мыслью, содержащей постановку и пути решения выявленных проблем.

К любой концепции существуют следующие требования:

1. **Конструктивность.** Такое требование будет признано реализованным, если в концепции найдет отражение:

– исходное состояние объекта, на преобразование которого направлена концепция;

– состояние объекта, достигнутое в результате реализации концепции;

– меры, необходимые для достижения сформулированных в концепции целей;

– средства, необходимые и достаточные для достижения поставленных целей;

– источники ресурсного обеспечения, используемые в ходе реализации концепции;

– механизм реализации концепции, т. е. способы (методы) использования выделенных средств и ресурсов.

2. **Вписываемость.** Имеется в виду встроенность концепции преобразования какого – либо объекта в систему концепции преобразования взаимосвязанных в единую систему объектов, одним из компонентов которой этот объект является.

3. **Открытость.** Разработанная концепция должна давать возможность в ее рамках реагировать на изменение условий реализаций концепции и вносить коррективы в реализацию в случае их необходимости.

Вышеуказанные требования диктуют в качестве обязательного условия включение в логическую структуру концепции следующих позиций:

1. Выявление объекта и предмета, определения их сущности, места среди множества других.

2. Четкая формулировка роли реализации концепции и задач, стоящих при ее реализации.

3. Выделение условий, необходимых и достаточных для реализации концепции, и сопоставление их с реально существующими.

4. Определение круга мероприятий, обеспечивающих преобразование объекта реализации концепции, а также путей ее реализации.

5. Формулирование критериев успешности мероприятий по разработке концепции, а также по оценке результатов ее реализации.

6. Концепция безопасности предприятия представляет собой официально утвержденный документ, в котором отражена система взглядов, требований и условий организации мер безопасности персонала и собственности предприятия.

Примерная структура концепции может выглядеть следующим образом:

1. ***Описание проблемной ситуации в сфере безопасности предприятия***.

– перечень потенциальных и реальных угроз безопасности, их классификация и ранжирование;

– причины и факторы зарождения угроз;

– негативные последствия угроз для предприятия;

2. ***Механизм обеспечения безопасности***.

– определение объекта и предмета безопасности предприятия;

– формулирование политики и стратегии безопасности;

– принципы обеспечения безопасности.

– цели обеспечения безопасности;

– задачи обеспечения безопасности;

– критерии и показатели безопасности предприятия;

– создание оргструктуры по управлению системой безопасности предприятия.

3. ***Мероприятия по реализации мер безопасности***:

– формирование подсистем общей системы безопасности предприятия;

– определение субъектов безопасности предприятия и их роли;

– расчет средств и определение методов обеспечения безопасности;

– контроль и оценка процесса реализации концепции.

Необходимо иметь в виду, что наиболее полное представление о системе безопасности предприятия можно получить после изучения официально принятых документов по концепции безопасности предприятия, комплексной программы обеспечения безопасности предприятия и планов подразделений предприятия по реализации этой программы. Сформированная на научной основе система безопасности предприятия является организационной основой создания ее структурного подразделения – службы безопасности.

Глава 3. Обеспечение безопасности предприятия

В общественном сознании все еще очень сильны стереотипы восприятия понятия «обеспечение безопасности» как чего-то, связанного с государственными интересами, осуществляемыми специальными государственными органами. Между тем законодательство под безопасностью понимает «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» (закон от 05.03.1992 г. № 2446-1 «О безопасности»). Таким образом, на первое место законодатель ставит интересы личности. Одним из таких интересов является предпринимательская деятельность, осуществляемая индивидуально или путем совместного участия в создании юридического лица. В настоящей статье мы попытаемся дать несколько советов по обеспечению безопасности фирмы.

Основной целью обеспечения безопасности организации является ограждение ее собственности и работников от внутренних и внешних угроз, выявление и, по возможности, устранение причин их возникновения.

3.1 Угрозы безопасности предприятия

К сожалению, обеспечение безопасности организации достаточно часто недооценивается ее участниками (акционерами) и руководителем Организации. Нередко это приводит к очень серьезным последствиям, ; начиная с краж имущества и заканчивая захватами юридического лица целиком. Тогда как ряд достаточно простых, но проводимых в комплексе мероприятий может серьезно снизить данные риски. Прежде чем определять список этих мероприятий, необходимо оценить реальные угрозы.

Их принято разделять на два вида:

1. ***Внешние угрозы.*** К внешние угрозы относятся:

– деятельность недобросовестных конкурентов, направленная на подрыв деловой репутации организации, хищения – принадлежащих ей ноу – хау, коммерческой тайны;

– действия рейдерских компаний или отдельных лиц, направленные на перехват управления организации или на захват ее имущества;

– гринмейл (greenmail, производное от green – «деньги» и blackmail – «шантаж»), то есть корпоративный шантаж в отношении организации;

– причинение ущерба материальным ценностям общества или его деловой репутации;

– неправомерные действия работников государственных силовых органов и т.д.

2. ***К внутренним угрозам относятся***:

– нарушения работниками трудовой дисциплины;

– правонарушения работников, направленные на причинение материального ущерба организации или подрыв ее деловой репутации;

– «некачественный» подбор персонала и другие.

Что стоит защищать?

Принято считать, что обеспечение безопасности организации направлено на защиту двух основных интересов общества:

Первый – сохранение и приумножение его имущества,

Второй – обеспечение и защита деловой репутации.

Если с первым интересом все ясно, то второй часто вызывает вопросы. Прежде всего – в виду сложности определения правовой природы самого явления и выбора способов защиты.

Под деловой репутацией принято понимать качественную оценку участниками гражданского оборота деятельности организации, а также действий ее реальных владельцев, аффилированных лиц, дочерних и зависимых организаций (письмо ЦБ РФ от 30.06.2005 г. № 92-Т «Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах»). Она может быть оценена, а ущерб, ей нанесенный, измерен в денежном эквиваленте. Поэтому можно считать, что практически все действия, направленные на обеспечение безопасности организации, защищают ее имущественные интересы. В том числе и такие, на первый взгляд далекие от имущественной оценки, как контроль над подбором персонала или организация

в СМИ публикаций с позитивными оценками деятельности организации или ее руководителей.

3.2 Построение системы безопасности предприятия

Система безопасности организации строится на целом ряде принципов. Они отражают основные требования к формированию стратегии и тактики действий по защите жизненно важных интересов организации. Основными принципами являются:

– ***своевременность и непрерывность.*** Предсказать покушения на интересы общества практически невозможно, поэтому при построении системы защиты необходимо действовать на

– ***комплексность.*** Защита должна строиться, исходя из готовности отражать посягательства одновременно по нескольким направлениям;

– ***активность.*** Система безопасности не может базироваться только на мерах пассивной защиты, но и должна исходить из готовности противодействия посягательствам всеми возможными способами, включая нестандартные меры защиты;

– ***законность.*** Система безопасности организации должна быть четко разработанной и действовать на основе и в рамках правил, разрешенных действующим законодательством;

– ***централизация управления.*** Высокотехничная и эффективная система обеспечения безопасности требует управления, основанного на четкой координации действий всех входящих в нее элементов. Такая координация предполагает наличие единого управленческого центра;

– ***взаимодействие и координация.*** Безопасность в функционировании организации достигается через четкое взаимодействие подразделений, непосредственно занимающихся обеспечением безопасности, и остальными подразделениями организации.

3.2.1 Нормативно – правовые акты по безопасности предприятия

Высокий уровень взаимодействия между подразделениями возможен лишь при наличии общего регламента их действий, четко закрепленного в системе локальных нормативных актов организации Основными документами, входящими в эту систему, являются:

1. Положение о системе безопасности (концепция собственной безопасности).

2. Положение о контрольно – пропускном режиме;

3. Положение о коммерческой тайне

4. Положение о проведении служебных расследований.

Кроме того, отдельные положения, регламентирующие действия по обеспечению безопасности, содержатся практически во всех локальных нормативных актах организации, в частности, правилах внутреннего трудового – распорядка, положениях о структурных подразделениях и многих других.

Можно выделить следующие направления деятельности по обеспечению безопасности организации:

– ***работа с контрагентами.*** В данную область входит проверка будущих контрагентов, в зависимости от глубины планируемого сотрудничества устанавливаются: финансовое и имущественное состояние контрагента, наличие у лица, которое будет заключать сделку, прав на ее совершение, наличие и действительность лицензии (если его деятельность лицензируемая), отсутствие в отношении приобретаемого имущества спора или прав на него поиски скрывающихся должников, осуществление комплекса мероприятий по взысканию просроченных долгов, реализация мер по розыску похищенного имущества;

– ***работа с правоохранительными органами*** по вопросам расследования преступлений и правонарушений, причинивших ущерб организации;

– информационно – аналитическое обеспечение (отслеживание – материалов в прессе, содержащих упоминания об организации);

– ***информационно – пропагандистское*** обеспечение (создание в общественном сознании положительного имиджа организации);

– ***информационная защита*** (создание в организации системы защиты коммерческой тайны и обеспечение ее функционирования, в том числе через работу с персоналом, создание максимально защищенных от взлома компьютерных сетей, соблюдение режима работы с данной категорией информации (ст. 10,11 закона от 29.07,2004 г. № 98-ФЗ «О коммерческой тайне»);

– ***правовая и психологическая работа с сотрудниками***, нарушающими дисциплину труда и правила внутреннего распорядка организации. При этом под правовой работой понимается проведение служебных расследований, подготовка и составление всех необходимых документов для привлечения сотрудников к дисциплинарной ответственности;

– ***охрана объектов***, принадлежащих организации, в том числе от проникновения третьих лиц;

– ***обеспечение личной безопасности руководителя и первых лиц*** – организации, охрана жизни и здоровья работников.

Кроме вышеперечисленных, в условиях российской действительности можно выделить также такое специфическое направление, как /становление контакта с представителями муниципальной власти по месту расположения организации и представителями органов федеральной власти. В свете сложившейся в нашей стране практики данный вид превентивных мер по обеспечению безопасности может сыграть очень важную роль. Возможность прямого контакта с представителями властных и правоохранительных органов зачастую оказывается решающим фактором во многих ситуациях и просто необходима в случае попытки корпоративного захвата организации.

Исходя из приоритетности этих направлений, для организации строится и система Внутренних органов, которая решает определенные задачи:

1. **Подразделение охраны.** Оно осуществляет непосредственные мероприятия по защите имущества и физической защите сотрудников организации;

2. **Оперативное подразделение.** Занимается проведением служебных расследований, а также оперативно-розыскными мероприятиями. При этой необходимо помнить, что любые действия по сбору информации о физических или юридических лицах должны производиться в соответствии с действующим законодательством;

3. **Подразделение технической поддержки.** Данный отдел занимается работой с высокотехнологическими приборами, без которых в настоящее время невозможно представить ни одну систему безопасности. Прежде всего речь идет о системах сигнализации и видеонаблюдения;

4. **Аналитический отдел.** Данное подразделение, как правило, самое небольшое по численности, но выполняющее наиболее значимые функции в системе безопасности, такие, как разработка основных мероприятий по защите имущества, охрана коммерческой тайны общества и координация работы остальных подразделений системы безопасности.

В некоторых случаях под контроль служб безопасности передают и отдел по связям с общественностью. Это особо актуально при проведении агрессивной брэндинговой политики, направленной на завоевание новых рынков сбыта. Во время подобных мероприятий организация становится особо уязвимой для так называемого «черного пиара» и, соответственно, должна максимально быстро реагировать на любые его проявления всеми доступными для нее средствами.

Делать самим или привлечь специалистов?

Практически все организации строят систему защиты на условиях объединения внутренних и внешних ресурсов. Данная политика, безусловно, оправдана. Привлечение сторонних организаций, специализирующихся на подобной деятельности, позволяет получить максимальный результат с минимальными затратами по сравнению с созданием системы безопасности с нуля.

Наиболее часто по договору (аутсорсинг) специализированным агентствам передаются функции общей охраны объектов и физической защиты первых лиц организации. При этом необходимо учитывать, что в соответствии с законом от 11.03.1992 г. № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» данный вид предпринимательской деятельности является лицензируемым. Соответственно, прежде чем заключить договор с ЧОПом, следует проверить наличие у него необходимой документации. Также часто внешним профессионалам передается создание и поддержание работоспособности системы технических средств охраны и наблюдения.

Разумным можно счесть привлечение со стороны высококлассных специалистов в области юриспруденции для разработки методов и мер корпоративной защиты организации. Много нитей контроля оказывается в руках, не подконтрольных руководству организации. Соответственно, чтобы решиться на такую передачу; необходимо быть уверенным не только в высоком уровне профессионализма специалистов, но и в высокой степени их лояльности.

Создание единой системы безопасности – довольно сложный процесс, требующий серьезных финансовых вложений. Подобные вложения достаточно часто не представляются руководителям организации оправданными. К сожалению, нередко они меняют свою точку зрения только после того, как понесут серьезные убытки.

3.2.2 Понятие и сущность безопасности предприятия

В соответствии с вышеприведенным толкованием безопасности под ***безопасностью предприятия*** в широком смысле следует понимать состояние защищенности жизненно важных интересов предприятия от внутренних и внешних угроз (источников опасности).

В узком смысле ***безопасность предприятия*** – это такое состояние его правовых, экономических и производственных отношений, материальных, интеллектуальных и информационных ресурсов, которое выражает способность предприятия к стабильному функционированию и научно-техническому прогрессу, как основе эффективной финансово-коммерческой деятельности и условию реализации важнейших социальных интересов трудовых коллективов дочерних структур и акционерного общества в целом.

Целями обеспечения безопасности предприятия являются:

– выполнение производственных программ, достижение требуемого качества выпускаемой продукции, развитие производительных сил предприятия на передовой научно-технической базе, активная инвестиционная политика;

– защита законных прав и интересов предприятия, всех его дочерних компаний, трудовых коллективов и работников во взаимоотношениях с государственными органами и зарубежными партнерами и конкурентами;

– поддержание устойчивости порядка внутреннего управления;

– сохранение и приумножение собственности предприятия, ее рациональное и эффективное использование в решении производственных задач и удовлетворения потребностей трудовых коллективов работников предприятия;

– повышение конкурентоспособности производимых товаров и услуг;

– реализации в условиях конкуренции на внутреннем и мировом рынках, рост прибылей предприятия;

– достижение внутренней и внешней стабильности предприятия, надежности кооперативных связей и недопущение

– односторонней зависимости от случайных и недобросовестных партнеров;

– укрепление дисциплины труда и его производительности, формирование стимулов и условий повышения творческой

– активности сотрудников и трудовых коллективов предприятия;

– максимально полное информационное обеспечение экономической, производственной и научно – технической деятельности предприятия, сохранение коммерческих и государственных секретов, охрана прав на интеллектуальную собственность предприятия, включая право на пресечение недобросовестной конкуренции.

В качестве объектов безопасности выступают:

– части предприятия, например, различные структурные подразделения или группы сотрудников либо владельцев акций предприятия и т.п.;

– виды ресурсов или имущества, например, основные или оборотные фонды предприятия,

– качественные характеристики ресурсов или имущества, например, возраст основных фондов, показатели качества окружающей предприятие среды;

– отдельные виды деятельности и процессы, например, обновление основных фондов, формирование портфеля инвестиционных проектов, диверсификация производственной программы;

– качественные характеристики упомянутых выше видов деятельности, такие как, например, скорость обновления основных фондов или темпы технологического развития.

Концепция безопасности предприятия – целостное и системное пони-

мание, видение и представление путей устранения опасностей, которые грозят или будут грозить предприятию извне в силу того, что деятельность протекает в рамках более общих политических, экономических и социальных процессов, а также обнаружение способов ликвидации опасностей, которые угрожает предприятию изнутри в силу частных специфических внутриорганизационных процессов позволяющим юридическим и физическим лицам успешно осуществлять свою деятельность в условиях возникновения стихийных бедствий, катастроф, а также при незаконных действиях конкурентов и преступных групп. К таким мерам можно отнести общеправовые, административные, организационно-управленческие, инженерно-технические, воспитательные, специальные, и другие. Комплексное применение мер безопасности помогает хозяйствующему субъекту оградить себя от воздействия недобросовестных конкурентов и уменьшить риск при возникновении стихийных бедствий.

В этом определении следует особо отметить три момента:

1. Состояние защищенности носит динамический характер.

2. Угроза, исходящая изнутри предприятия, не менее опасна, чем извне.

3. Система экономической безопасности предприятия может соприкасаться и даже взаимодействовать на правовой основе с государственной системой обеспечения безопасности.

Таким образом, экономическая безопасность предприятия – состояние динамической устойчивости юридических, производственных отношений и организационных связей предприятия, материальных и интеллектуальных ресурсов, при котором гарантируется стабильность его функционирования, финансово – коммерческий успех, прогрессивное научно – техническое и социальное развитие.

3.3 Безопасность материальных объектов и ресурсов

Основными составляющими обеспечения безопасности различных ресурсов предприятия являются:

– система физической защиты (безопасности) материальных объектов;

– система безопасности информационных ресурсов.

На практике все мероприятия по использованию технических средств безопасности делятся на:

– организационные

– организационно – технические

– технические.

Система физической защиты (безопасности) материальных объектов должна предусматривать:

– систему инженерно – технических и организационных мер охраны;

– систему регулирования доступа;

– систему мер (режим) по сохранности и контролю ценностей;

– систему мер возврата материальных ценностей.

Система охранных мер должна предусматривать:

– многорубежность построения охраны (территории, здания, помещения подходы оберегаемому объекту;

– комплексное применение современных технических средств охраны, обработки информации, обеспечивающих достоверное отображение событий;

– надежное инженерно – техническое перекрытие вероятных путей несанкционированные охраняемые пределы;

– устойчивую (дублированную) систему связи и управления всех взаимодействующих в охране структур;

– высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию;

– самоохрану персонала.

Система регулирования доступа должна предусматривать:

– объективное определение «надежности» лиц, допускаемых к работе на объектах предприятия;

– максимальное ограничение количества лиц, допускаемых на объекты предприятия;

– установление для каждого работника (или посетителя) дифференцированного по времени, месту и виду;

– четкое определение порядка выдачи разрешений и оформления документов для входа (въезда) на объект;

– определение объемов контрольно – пропускных функций на каждом проходном и проездном пункте;

– оборудование контрольно – пропускных пунктов (постов) техническими средствами, обеспечивающими; объективную регистрацию прохода и предотвращение несанкционированного (в том числе силового) проникновения;

– высокую подготовленность и защищенность персонала (нарядов) контрольно – пропускных пунктов.

Система мер (режим) по сохранности и контролю ценностей должна предусматривать:

– строго контролируемый доступ лиц в режимные зоны (зоны обращения и хранения финансов);

– максимальное ограничение посещений режимных зон лицами, не участвующими в работе предприятия;

– максимальное сокращение количества лиц, обладающих досмотровым иммунитетом;

– организацию и осуществление присутственного (явочного) и дистанционного (по техническим каналам режима безопасности предприятия;

– организацию тщательного контроля любых предметов и веществ, перемещаемых за пределы режимных объектов;

– обеспечение защищенного хранения документов, финансовых средств и ценных бумаг;

– соблюдение персональной и коллективной материальной и финансовой ответственности в процессе ОТК и материальных ценностей;

– организацию тщательного контроля на каналах возможной утечки информации;

– оперативное выявление причин тревожных ситуаций в режимных зонах, пресечение их развития или ли охраны.

Система мер возврата утраченных материальных и финансовых ресурсов слагается из совместных усилий безопасности и государственных органов охраны правопорядка и безопасности.

На объектовую службу безопасности возлагаются:

– обнаружение противоправного изъятия материальных и финансовых средств из обращения или хранения;

– оперативное информирование правоохранительных органов о событиях и критических ситуациях;

– установление субъекта преступления;

– проведение поиска возможного «схоронения» утраченных средств в районе объекта.

Дальнейший поиск и возврат пропавших ресурсов организуются в установленном порядке через соответствующие органы безопасности.

Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, программных и криптографических средств и мер по защите информации в процессе традиционного документоведения:

– работе исполнителей с конфиденциальными документами и сведениями;

– обработке информации в автоматизированных системах различного уровня и назначения;

– передаче по каналам связи, а также при ведении конфиденциальных переговоров.

Инженерно – техническая безопасность информационных ресурсов реализуется путем использования различных систем, обеспечивающих безопасность предприятия, в том числе:

– аппаратных средств обеспечения безопасности;

– программных средств защиты информации в технических средствах обработки;

– математическими способами защиты информации от различных угроз и несанкционированных действий.

Основными направлениями обеспечения информационной безопасности предприятия являются:

– защита информационных ресурсов от разглашения, хищения, уничтожения, искажения и подделки за счет специальных воздействий;

– защита информации от утечки вследствие наличия физических полей за

счет ПЭМИН (побочные электрические цепи, трубопроводы и конструкции зданий.

Система обеспечения информационной безопасности должна предусматривать:

– реализацию разрешительной системы допуска исполнителей (пользователей) к работам, документам служебного характера;

– ограничение доступа исполнителей и посторонних лиц в здания, помещения, где проводятся работы, на объекты информатизации, на которых обрабатывается (хранится) информация конфиденциального характера;

– разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;

– учет документов, информационных массивов, регистрация действий пользователей информационных систем, доступом и действиями пользователей;

– криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники;

– снижение уровня и информативности ПЭМИН, создаваемых различными элементами технических средств деятельности и автоматизированных информационных систем;

– снижение уровня акустических излучений;

– электрическую развязку цепей питания, заземления и других цепей технических средств, выходящих за активное зашумление в различных диапазонах;

– противодействие оптическим и лазерным средствам наблюдения;

– проверку технических средств и объектов информатизации на предмет выявления включенных в них задач;

– предотвращение внедрения в автоматизированные информационные системы программ вирусного характера;

Защита информационных ресурсов от несанкционированного доступа должна предусматривать:

– обоснованность доступа, т.е. исполнитель (пользователь) должен иметь соответствующую форму допуска (информацией) определенного уровня конфиденциальности;

– персональную ответственность, заключающуюся в том, что исполнитель (пользователь) должен нести о доверенных ему документов (носителей информации, информационных массивов), а также за свои действия;

– надежность хранения, когда документы (носители информации, информационные массивы) хранятся в серверах, несанкционированное ознакомление с ними, их уничтожение, подделку или искажение;

– разграничение информации по уровню конфиденциальности, заключающееся в предупреждении размет конфиденциальности в документах (носителях информации, информационных массивах) с более низкими значениями, предупреждение передачи конфиденциальной информации по незащищенным линиям связи;

– контроль за действиями исполнителей (пользователей) с документацией и сведениями, а также в автоматизированном виде;

– чистку (обнуление, исключение информативности) оперативной памяти, буферов при освобождении ресурсов между другими пользователями;

– целостность технической и программной среды, обрабатываемой информации и средств защиты, средств информатизации, неизменности программной среды, определяемой предусмотренной технологий, средствами защиты предусмотренных функций, изолированности средств защиты от пользователей.

Требование обоснованности доступа реализуется в рамках разрешительной системы допуска к работам, для которой устанавливается:

– кто, кому, в соответствии с какими полномочиями, какие документы и сведения (носители информации, действий или для какого вида доступа может предоставить и при каких условиях;

– состав всех пользователей автоматизированных систем информационных и программных ресурсов, доступ (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно –технических систем.

Персональная ответственность достигается путем:

– росписи исполнителей в журналах, карточках учета, других разрешительных документах;

– индивидуальной идентификации пользователей и инициированных ими процессов в автоматизированных системах;

– проверки подлинности (аутентификации) исполнителей (пользователей) на основе использования паролей, подписи, а также биометрических характеристик личности при доступе как в автоматизированные системы (зоны).

Условие надежности хранения реализуется с помощью:

– хранилищ конфиденциальных документов, оборудованных техническими средствами охраны, доступ в которые ограничен и осуществляется в установленном порядке;

– выделения помещений, в которых разрешается работа с конфиденциальной документацией, оборудованными шкафами, а также ограничения доступа в эти помещения;

– использования криптографического преобразования информации в автоматизированных системах.

Правило разграничения информации по уровню конфиденциальности реализуется с помощью:

– предварительно учтенных тетрадей для ведения конфиденциальных записей или носителей информации определенного уровня секретности криптографического преобразования информации в автоматизированных системах;

Система контроля за действиями исполнителей реализуется посредством:

– организационных мер контроля при работе исполнителей с конфиденциальными документами и сведениями;

– регистрации (протоколирования) действий пользователей с информационными и программными ресурс указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимо-, запрещенные попытки доступа;

– сигнализации о несанкционированных действиях пользователей.

Очистка памяти осуществляется организационными и программными мерами, а целостность автоматизированных систем комплексом программно – технических средств и организационных мероприятий.

Защита информации от утечки за счет ПЭМИИ обеспечивается пу-

тем уменьшения отношения информационного уровня, при котором восстановление сообщений становится принципиально невозможным (данный уровень эффективности защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН). Решение этой задачи достигается путем снижения излучений информационных сигналов, так и увеличением уровня помех в соответствующих частотных диапазонах.

Первый способ реализуется выбором системно – технических и конструкторских решений при создании тех вычислительных средств в «защищенном исполнении», а также рациональным выбором места размещения относительно направлений возможного перехвата информативного сигнала.

Второй способ реализуется в основном за счет применения активных средств защиты в виде «генераторов антенн».

Защита информации в линиях связи. К основным видам линий связи, используемых для передачи информации (телефонные, телеграфные), радио- и радиорелейные, тропосферные и космические линии связи.

При необходимости передачи по ним конфиденциальной информации основным способом защиты ее от дезинформации является использование криптографического преобразования информации, а на небольшое использование защищенных волоконно – оптических линий связи.

Безопасное использование технических средств информатизации. Одним из методов технической разведки является внедрение в конструкцию различных технических средств закладных устройств перехвата, транспортирования, вывода технических средств из строя.

В целях противодействия такому методу воздействия на объекты технических средств информатизации, конфиденциальной информации, в обязательном порядке проводится проверка этих средств, осуществляющих ' организациями с помощью специального оборудования, как правило, в стационарных условиях в соответствии с требованиями.

Защита речевой информации при проведении конфиденциальных переговоров. Исходя из возможности проведения разговоров конфиденциального характера с помощью внедрения закладных устройств, акустически лазерных

технических средств разведки, противодействие этим угрозам должно осуществляться всеми доступными способами.

Необходимой составляющей системы информационной безопасности должно быть обеспечение качества мер защиты, нормативной базой которою является система стандартов и других руководящих нормативных документов по безопасности.

Данные документы утверждаются федеральными органами государственного управления в соответствии с нормы защищенности информации и требования к различным направлениям защиты информации.

В соответствии с этими требованиями должны проводиться:

– предпроектное обследование и проектирование информационных систем;

– заказ средств защиты информации и контроля, предполагаемых к использованию в этих системах;

– аттестация объектов информатики;

– контроль защищенности информационных ресурсов.

К основным стандартам и нормативно – техническим документам в области защиты информации от несанкционированного проникновения относятся:

– комплект руководящих документов Гостехкомиссии России (1992 г.), в том числе «Автоматизированные системы. Классификация АС и требования по защите информации»;

– «Положение по организации разработки, изготовления и эксплуатации программ и технических средств несанкционированного доступа в автоматизированные системы и электронную вычислительную технику.

В соответствии с данными требованиями право оказывать услуги сторонним организациям в области защиты разрешается только организациям, имеющим на этот вид деятельности разрешение (лицензию).

Подлежат обязательной сертификации по требованиям безопасности информации:

– средства и системы вычислительной техники и связи, предназначенные для обработки (передачи) секретных сведений;

– средства защиты и контроля эффективности защиты такой информации.

Обязательной аттестации по требованиям безопасности информации подлежат объекты информатики, представляющие следующие услуги:

– обработки секретной и иной конфиденциальной информации

– ведения секретных переговоров.

Глава 4. Комплексная система безопасности

Действующие и разрабатываемые законодательные и иные нормативные акты организации на выработку собственной концепции системы безопасности создание соответствующей службы (подразделений) для реализации этой концепции.

В концепции устанавливаются цели, задачи, принципы организации безопасности, а также основные угрозы безопасности предприятия, направления деятельности по комплексной безопасности предприятия, которые охватывают следующие объекты и аспекты:

– информационно-аналитические исследования и прогнозные оценки экономической, финансовой и экологической безопасности предприятия;

– обеспечение безопасности персонала и безопасности труда;

– обеспечение сохранности и физической защиты материальных и финансовых ценностей;

– обеспечение безопасности информационных ресурсов

– обеспечение экологической безопасности объектов предприятия (зданий, сооружений, помещений);

– обеспечение и контроль «надежности» и лояльности персонала управляющего предприятием.

Основными задачами направления информационно – аналитических и практических оценок безопасности являются:

– сбор и анализ информации о мировом и национальном рынках, открытых экономических программах и планах поддержки и развития технических и технологических программах, планах деятельности государственных органов исполнительной власти, представлять угрозы безопасности предприятия (например, налоговые);

– сбор и анализ экономической и научно – технической информации для недобросовестных конкурентов, а также эффективности деловых отношений с отечественными партнерами, выявление в их числе несостоятельных, ненадежных предпринимателей, структурами и т.п.;

– учет официальных претензий правоохранительных и контролирующих органов, возможным партнерам и т.п.

– изучение, анализ и оценка криминальной обстановки, в том числе состояния экономической преступной деятельности в регионе;

– выявление факторов и контроль показателей, определяющих несостоятельность (банкротство) предприятий;

– выявление факторов и контроль показателей, определяющих экологическую безопасность предприятия, возникновением аварийных (нештатных) ситуаций на предприятии на предприятии;

– организация работ по выявлению конфиденциальной информации, обоснованию уровня се конфиденциальности, оформлению в виде перечней сведений, подлежащих защите;

– мониторинг, выявление и оценка (прогнозирование) уязвимых мест в системе комплексной безопасности, предоставление руководству предложений по предупреждению и/или ослаблению, устранению (ликвидации внутренних опасностей и угроз, способных нанести неприемлемый (недопустимый в данный период, ущерб для предприятия;

– информационное обеспечение руководства в области безопасности предприятия;

– координация деятельности подразделений службы безопасности и обеспечения взаимодействия со всем предприятием в решении проблем комплексной безопасности.

***Основными задачами направления обеспечения безопасности персонала и безопасности труда являются*:**

– предупреждение, ослабление, устранение (ликвидация) и отражение опасностей и угроз жизни и здоровья в рабочее время (ключевых работников – при необходимости и во внерабочее время), их личным материальным средствам (имуществу), находящимся в рабочее время на территории предприятия, информации личного характера.

Основными задачами направления обеспечения сохранности и физической защиты материальных и финансовых ценностей являются:

– установление режима охраны производственных объектов и объектов жизнедеятельности;

– осуществление допускного и пропускного режимов па предприятии;

– обеспечение защищенного хранения ценностей и документов (носителей информаций), оснащение современными средствами охраны;

– организация физической защиты продукции в процессе ее внутриобъектовой транспортировки;

– осуществление контроля за сохранностью продукции на всех стадиях технологического процесса;

– взаимодействие всех структур, участвующих в обеспечении физической защиты.

Основными задачами направления обеспечения безопасности информационных ресурсов являются:

– организация и осуществление разрешительной системы допуска исполнителей к работе с документами;

– организация хранения и обращения с конфиденциальными документами (носителями информации);

– осуществление закрытой переписки и шифрованной связи (при необходимости);

– организация и координация работ по защите информации, обрабатываемой и передаваемой средствами связи;

– обеспечение безопасности в процессе проведения конфиденциальных совещаний, переговоров;

– осуществление контроля за сохранностью конфиденциальных документов (носителей информации), обрабатываемой и передаваемой средствами и системами вычислительной техники и связи.

Основными задачами направления по обеспечению экологической безопасности объектов предприятия (процессов) являются выявление (идентификация), предупреждение, ослабление, устранение (ликвидация), со стороны выпускаемой продукции и процессов ее производства, подготовки к поставке и поставе продукции предприятии в результате штатных и аварийных ситуаций на предприятии.

Основными задачами направления по обеспечению и контролю «надежности» и лояльности персонала, являются следующие:

1. **Набор персонала.** Как правило, набор осуществляется из внутренних (перемещение и продвижение по службе, (найм по объявлениям и по личным рекомендациям) источников. Основным требованием при этом является оценка (в том числе с точки зрения вопросов обеспечения безопасности) характеристик поступающего, по условиям и содержанию предлагаемой ему работы

2. **Отбор кандидатов.** При отборе кандидатов могут использоваться следующие основные группы: образовательные, организационные, личные. Основным требованием при отборе является тщательное рассмотрение этических данных каждого кандидата путем глубокого изучения его трудового прошлого. В процессе анализа целесообразно пользоваться услугами органов внутренних дел, оказываемыми ими в соответствии с приказом. Согласно данному приказу органы внутренних дел должны оказывать платные услуги о наличии (отсутствии) судимости, предоставлять сведения о лицах, находящихся в розыске.

3. Согласование заключения контракта с кандидатом при условии получения у него добровольного согласия условий регламентирующих режим безопасности и сохранения коммерческой тайны.

4. Организация и контроль обучения кандидатов перед допуском к работе, которое предусматривает введение установленным правилам выполнения должностных обязанностей; обучение установленным правилам труда, техники безопасности на рабочем месте, обеспечения безопасности и защиты информации.

5. Текущий контроль (мониторинг) за деятельностью сотрудника в части соблюдения им требований по технике безопасности, обеспечению безопасности и защиты информации, а также повышения его бдительности.

6. Своевременное выявление и устранение причин для возникновения внешних и внутренних конфликтных ситуаций, что предусматривает осуществление деятельности по правовому и психологическому обеспечению, по заключению контрактов и их реализации, а также всех мероприятий, направленных на совершенство деятельности предприятия.

Служба безопасности коммерческого предприятия, как правило, подчи-

няется непосредственно руководителю, руководитель службы безопасности должен быть заместителем руководителя и иметь полномочия по:

– административному управлению группой по информационно – аналитическим исследованиям и прогноз) обучению персонала

– оперативно – методическому руководству подразделениями (должностными лицами), отвечающими за сохранение ценностей и объектов, безопасность информационных ресурсов, экологическую безопасность;

– координации деятельности структурных подразделений предприятия, участвующих в выполнении конкретной концепцией системы комплексной безопасности предприятия, утвержденными программами и планами;

– разработке и предоставлению руководству предложений по предупреждению и/или ослаблению, устранению внешних и внутренних опасностей и угроз, способных нанести неприемлемый (недопустимый) в данный момент интересам предприятия.

Он отвечает за мониторинг, выявление и оценку (прогнозирование) уязвимых мест в системе комплексной безопасности, разработку, контроль и оценку эффективности реализации программ и планов проведения мероприятий по комплексной безопасности

Мерой комплексной безопасности организации, как критерия оценки деятельности предприятии в данном исполнении служит для удовлетворения установленных требований, запросов и/или предполагаемых потребностей всех заинтересованных лиц, состава и характеристик персонала, методов, технических средств, документации и процессов, используемой безопасности ключевых структурных элементов организации, по сравнению с соответствующими показателями среднепромышленном, среднеотраслевом, внутриотраслевом уровнях и/или конкретными конкурентами.

При оценке данного критерия используются подкритерии, характеризующие:

– число и масштабы ущерба от различных видов угроз для безопасности личности владельцев, клиентов их семей и близких родственников, заявленных правоохранительным органам и/или предотвращенных с усилиями организа-

ции (например, угроз убийства, похищений, разбойных нападений, шантажа, запугивания, вымогательств;

– число и масштабы ущерба от различных видов угроз материальным ценностям и нематериальным ценностям правоохранительным органам и/или предотвращенных с участием службы безопасности организации исключительного права организации на (результаты интеллектуальной деятельности, угоны, повреждения, преднамеренные аварии, поджоги, нападения, вторжения, захваты, пикетирования, блокирования, повреждения помещений, средств связи и другого недвижимого имущества организации);

– число и масштабы ущерба от различных видов угроз финансовым средствам организации, заявленных и предотвращенных с участием службы безопасности организации (например, хищения финансовых сред невозврат кредитных ссуд, мошенничества со счетами, фальсификации валюты, использование подложных пластиковых карт, взимания незаконных налогов, штрафов и пр.)

– число и масштабы ущерба от различных видов угроз информационным ресурсам организации, заявленных и предотвращенных с участием службы безопасности организации (например, разглашения конфиденциальной информации через технические средства обеспечения производственной деятельности, несанкционированного доступа к охраняемым сведениям со стороны конкурентных организаций и прессы, ознакомления с охраняемыми сведениями (составляющими коммерческую тайну), изменения информации, уничтожении информации с целью нанесения морального и материального ущерба предприятию и его членам.

Вопросы технической безопасности по направлениям деятельности службы безопасности должны решать подразделениями, отвечающими за соответствующее направление деятельности на предприятии.

Для решения основных вопросов: «Каков достаточный уровень безопасности, каким образом его достичь в дальнейшем?» необходимо в зависимости от состояния с комплексной безопасностью предприятия и его ресурсными возможностями определить наиболее рациональные соотношения между объемами и характером инвестиций разделить на: организационные, организационно-технические и иные виды мероприятий по:

– совершенствованию информационно – аналитических исследований и прогнозных оценок безопасности;

– совершенствованию технических систем и объектов, используемых для обеспечения безопасности предприятия;

– обучению, подготовке и поддержанию готовности персонала к выполнению служебных обязанностей, в безопасности предприятия;

– проведению контроля и внутреннего аудита уровня безопасности предприятия в целом и/или его отдельной деятельности) с целью выявления (идентификации), предупреждения, ослабления, устранения (ликвидации) и характера;

– ликвидации последствий, возникших на предприятии при реализации различных угроз.

Вывод: изучение научной литературы и практики позволяют прийти к выводу, что структурными элементами системы безопасности предприятия являются научная теория безопасности, политика и стратегия безопасности, средства и методы обеспечения безопасности и, наконец, концепция безопасности предприятия.

Список использованных источников и литературы

1. О безопасности. Закон РФ №2446-1 от 5 марта 1992 г. (ред. 25.07.2002).

2. О государственной стратегии экономической безопасности Российской Федерации (Основные положения). Указ Президента РФ от 29 апреля 1996 г. № 608 // Российская газета. 1996.14 мая.

3. Государственная экономическая политика: учеб, пособие для студентов вузов / под ред. Т.Г. Морозовой. М.: ЮНИТИ-ДАНА, 2006.

4. Грунин О., Грунин С. Экономическая безопасность организации. СПб.: Питер, 2002. 160 с.

5. Основы экономической безопасности / под ред. Е.А. Олейникова. М.: ЗАО "Бизнес-школа", 1997. 288 с.

6. Филин С.А. Информационная безопасность. 2006.

7. Громов В.И., Васильев Г.А. Энциклопедия безопасности.

8. Мак – Мак В.П. Служба безопасности предприятия (организационно – управленческие и правовые аспекты деятельности). М.: Мир безопасности, 1999.

Учебное издание

Сакович Наталия Евгениевна

Христофоров Евгений Николаевич

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

Учебное пособие

Редактор Осипова Е.Н.

Подписано к печати 26.07.2024 г. Формат 60х84 $^{1}/_{16.}$
Бумага офсетная. Усл. п. л. 4,30. Тираж 25 экз. Изд. № 7712.

Издательство Брянского государственного аграрного университета
243365 Брянская обл., Выгоничский район, с. Кокино, Брянский ГАУ