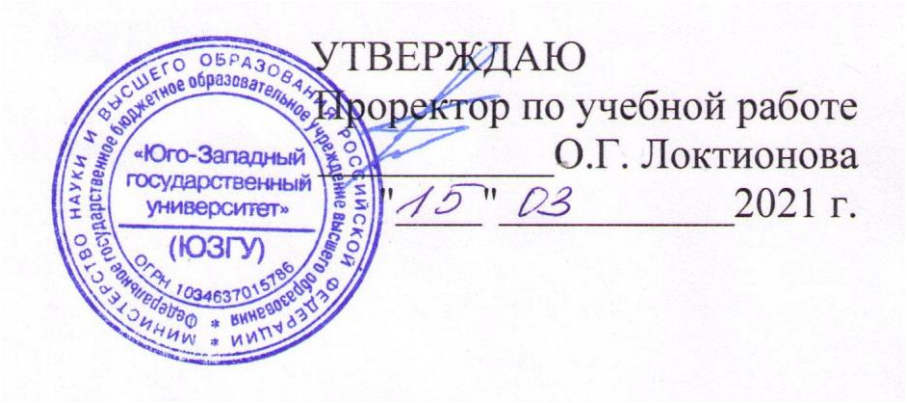
МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности



ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ

Методические указания по выполнению практических работ
для студентов направления подготовки (специальности)
10.03.01 информационная безопасность

Курск 2021

УДК 004
Составители: А.Л. Ханис

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности А.Г. Спеваков

Экономика защиты информации : методические указания по выполнению практических работ студентов всех форм обучения / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 26 с.:– Библиогр.: с. 26.

Содержат сведения по вопросам решения технико-экономических задач защиты информации в коммерческой организации. Указывается порядок выполнения практических работ, подходы к решению различных задач и правила оформления практических работ.

Методические указания составлены на основании учебного плана направления подготовки (специальности) 10.03.01 информационная безопасность и рабочей программы дисциплины «Экономика защиты информации».

Предназначены для студентов всех форм обучения специальности 10.03.01 и будут полезны для организации практических работ при подготовке к занятиям по дисциплинам «Экономика защиты информации», «Защита рисков и угроз».

Текст печатается в авторской редакции

Подписано в печать 15.03.2021. Формат 60х84 1/16.
Усл.печ. л. [кол-во стр. : 16 х 0,93] . Уч.-изд. л. [кол-во стр. : 19].
Тираж 100 экз. Заказ 520. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

ОГЛАВЛЕНИЕ

Введение

Важнейшей задачей коммерческой организации является обеспечение её эффективного функционирования, что предполагает ориентацию на инновацию и создание инновационной среды, умение привлекать и использовать для решения поставленных задач необходимые ресурсы из самых разнообразных источников.

Предпринимательская деятельность коммерческой организации охватывает самые различные сферы: производства, торговли, финансов, транспорта, образования, культуры, словом, практически всех направлений человеческой деятельности.

Конкуренция, направленная на повышение качества продукции и предоставляемых услуг с использованием достижений научно-технического прогресса, развитие послепродажного обслуживания и другие формы услуг без нанесения прямого ущерба конкурентам, считается добросовестной. К сожалению, на практике все чаще приходится сталкиваться с примерами недобросовестной конкуренции. В отличие от недавнего времени, когда конкурентоспособность продукта во многом определялась наличием путей сообщения и перевозок сырья, сегодня она в немалой степени зависит от умения защитить свою деловую, коммерческую и техническую информацию. В этом ряду особое место занимают новые идеи. Идеи участников предпринимательской деятельности составляют их интеллектуальную собственность, или, другими словами, информацию, которую можно использовать для производства товаров и услуг либо превратить в наличность, продав кому-нибудь. От умелого использования такого ценного товара, как информация, зависит успех предпринимательской деятельности [1].

Любой производитель, определяя возможности коммерческой деятельности, стремится держать в секрете свою конфиденциальную информацию, а его конкуренты, наоборот, стремятся ее получить в максимальном объеме и приемлемые сроки. Недобросовестная конкуренция осуществляется, прежде всего, в форме промышленного (информационного) шпионажа, роста коррупции, организованной преступности, фальсификации и подделки продукции конкурентов, манипулирования деловой отчетностью и нанесения материального и морального ущерба конкуренту.

В настоящее время государственные органы власти не в состоянии эффективно решать проблему защиты информации и обеспечить безопасность предпринимательской деятельности коммерческой организации. Поэтому руководители российских коммерческих фирм должны самостоятельно принимать решения о выборе критериев, норм и реальных механизмов защиты информации, являющейся их собственностью. В связи с этим в настоящее время первостепенное значение приобретают технико-экономические задачи защиты информации в организации.

Одной из центральных технико-экономических задач защиты информации является оптимизация этой деятельности по экономическим показателям. При этом под оптимизацией понимается достижение требуемых значений показателей системы защиты информации, при минимальном расходовании ресурсов. Более предметные постановки конкретных задач формулируются в одном из двух видов:

1. При заданном объеме расходуемых ресурсов обеспечить достижение максимально возможного результата.

2. Обеспечить достижение требуемого результата при минимальном расходовании необходимых ресурсов.

Решение этих задач возможно при взаимосвязи анализа, синтеза и управления.

При оценке возможного ущерба необходимо учитывать такие характеристики защищаемой информации, как ее важность, полнота и адекватность [1,2].

Синтез оптимальной системы защиты может быть реализован следующим подходом:

1. На основе опыта создания систем защиты информации составляются варианты наборов задач защиты.

2. Определяются наиболее подходящие наборы средств, использованием которых могут быть решены различные задачи защиты на различных рубежах.

3. На основе технико-экономических оценок средств защиты определяются размеры ресурсов, необходимых для практического использования различных средств.

1. Практическая работа №1. Система конфиденциальной информации коммерческой организации

1.1. Информация как товар

Товар – сложное, многоаспектное понятие, включающее совокупность многих свойств, главным из которых являются:

- потребительские свойства, т.е. способность товара удовлетворять потребности того, кто им владеет;
- цена, особенность которой состоит в том, что реальный процесс формирования цен здесь происходит не в среде производства, а в среде реализации продукции, т.е. на рынке под воздействием спроса и предложения;
- жизненный цикл товара (ЖЦТ) – время существования товара на рынке. Фазы ЖЦТ обычно делят на фазы внедрения, роста, зрелости, насыщения и спада.

Продолжительность жизненного цикла в целом и его отдельных фаз зависит как от самого товара, так и от конкретного рынка [1,2].

1.2. Информация коммерческой организации

Существуют различные подходы классификации информации, накапливаемой и циркулирующей в организации. С одной стороны, ее можно разделить на два больших блока:

- технологическую информацию, характеризующую научно-техническую сторону производства, «ноу-хау», часть которой представляет предмет пристального внимания конкурентов и промышленных шпионов;
- деловую информацию, связанную с управленческой, финансовой, маркетинговой и т.п. деятельностью, позволяющей успешно вести дела и заключать взаимовыгодные сделки.

С другой стороны, информация, необходимая для принятия решений и потребляемая организацией, может быть разделена на три группы:

- информация для стратегических решений;
- информация для тактических решений;
- информация для оперативных решений.

Для получения надлежащей информации необходимо выбрать базы для наблюдения, которые предопределяются насущными потребностями, те в свою очередь предопределяются поставленными целями.

Подготовка информации для принятия любого решения должна начинаться с определения целей, которые предопределяют потребности в информации, а затем и базы для наблюдения.

Стратегические цели (строительство новых предприятий, внедрение новой технологии, запуск в производство новой продукции) оказывают кардинальные изменения на функционирование фирмы. Эти цели предопределяют все последующие действия.

Стратегические потребности. Они включают в себя все, что может оказать долгосрочное влияние на деятельность предприятия.

На основании выявленных потребностей следует составить картотеку направлений для наблюдения. Примером могут служить следующие направления:

1. Тенденции по странам.
2. Технологический процесс: сырье, производственные технологии, окружающая среда.
3. Действующие лица: конкуренты (действительные и потенциальные), союзники и партнеры, кадры.
4. Диверсификация.

Тактическая цель заключается в выборе наилучшего средства достижения стратегической цели и в контроле неизменности условий, которые предопределили этот выбор.

Тактические потребности. Это может быть и выбор пути для достижения тактических целей. Здесь необходимо различать постоянную окружающую среду и переменную окружающую среду. При этом необходимо выбрать как первое, так и второе. Это различие связано с временной шкалой действий.

Потребности первого типа. Для правильного выбора необходимо знать общие характеристики каждой из сфер.

Потребности второго типа. Необходимо постоянно наблюдать

за состоянием окружающей среды для своевременного выявления препятствий, которые могут явиться причиной значительных отклонений от намеченного пути [1,2,3].

В первом случае базы создаются по запросу. Во втором случае ведется всеобъемлющее наблюдение за окружающей средой, т. к. неизвестно откуда будут исходить угрозы.

Прежде всего, речь идет об опасностях рынка и, в частности, об определенных действиях конкурентов. Таким образом, небольшой перечень баз наблюдения, учитываемых на стратегическом уровне, удлиняется на тактическом следующими направлениями:

- основные области деятельности и виды продукции (нынешние и будущие);
- зоны и территории деятельности;
- производственные мощности и способ производства;
- патентная и лицензионная активность.

На оперативном уровне стратегическая цель уже определена, путь ее достижения выбран. Теперь необходимо обеспечить продвижение вперед в наилучших условиях.

Оперативные потребности. Речь идет о благоприятных возможностях или об угрозах. Во всех случаях требуется свежая, точная, надежная и целенаправленная информация, т.к. речь идет о максимально быстром реагировании.

Оперативные базы. Речь идет о ближайшем окружении фирмы, за которым необходимо следить с повышенным вниманием (конкуренты, их коммерческая политика: ассортимент продукции, цены, рекламные компании, поставщики, клиенты, система торговли, субподрядчики).

Опыт показывает, что серьезная работа может начинаться со следующими базами:

- конкуренция (вся информация по действующим и потенциальным конкурентам);
- рынок (вся рыночная информация, вкусы и запросы потребителей, каналы сбыта и т.п.);
- технология (производство и использование продукции);
- законодательство (вся информация по законодательству, затрагивающему деятельность фирмы);
- ресурсы (информация по материально-техническим ресурсам

фирмы, по сырью, навыкам, рабочей силе и финансам);

- общие тенденции (политические, экономические, социальные, демографические);

- прочие факторы.

Система стратегической и перспективной информации (ССПИ) выполняет, главным образом, стратегическую роль, а ее деятельность ориентирована на перспективу.

Система тактической и оперативной информации (СТОИ) использует контакты сотрудников фирмы с внешним миром, а также возможности меж профессиональных встреч, таких как ярмарки, выставки и конференции (только узко специализированные).

Существуют два способа координации деятельности ССПИ и СТОИ: один – в рамках централизованной организационной структуры, другой – в рамках децентрализованной.

Информацию, необходимую для работы, предприятие получает из следующих источников.

Канал "Текст". (Общие публикации, специальные публикации и банки данных).

Канал "Фирма". Это контакты предприятия со всеми партнерами.

Канал "Консультант". (Общественные службы, консультанты, администрация).

Канал "Беседа". (Ярмарки, салоны и конференции).

Канал - неожиданный источник.

Для органов управления результатом является управленческое решение, и чем выше его эффективность, тем лучше работает служба информирования, способствующая его принятию.

Экономию времени руководителей и специалистов, занятых подготовкой решений за год, можно вычислить по формуле:

$$Э_t = 0{,}545 * \left(\Delta t_д * З_{ср.д} * N_д + \Delta t_и * З_{ср.и} * N_и\right), \qquad (1.1)$$

где 0,545 - отношение числа месяцев в году к среднему числу рабочих дней в месяце; $\Delta t_д$ - экономия времени руководителей за счет информационного обеспечения (дней в месяц); $З_{ср.д}$ - среднемесячная зарплата одного руководителя, обеспечиваемого информацией (руб.); $N_д$ - число руководителей, получивших

информацию и принявших ее к использованию; $\Delta t_{и}$, $З_{ср.и}$, $N_{и}$ - то же для специалистов, обеспечиваемых информацией и принимающих участие в подготовке решений [1,2,3].

1.3. Исходные данные для проведения работы

Для проведения ПР №1 используется следующая игровая ситуация:

Вы являетесь руководителем коммерческой организации (фирмы), действующей в условиях рынка нашего региона, которая обладает собственными коммерческими секретами и занимается, например, одним из следующих видов деятельности:

1. Производство электронных устройств.
2. Разработка программного обеспечения.
3. Производство программно-аппаратных средств.
4. Коммерческая деятельность.
5. Оказание услуг организациям и населению.

1.4. Задание

1. Определите название Вашей коммерческой организации (фирмы), вид ее деятельности, количество руководителей, емкость рынка фирмы, основных конкурентов, базы наблюдения и источники информации.
2. Составьте перечень информации, являющейся для Вашей организации (фирмы) оперативной, тактической и стратегической.
3. Укажите источники информации, которые могут обеспечить Вас сведениями о фирмах конкурентах (учитывать реально существующие источники и фирмы).
4. Оцените жизненный цикл Вашего информационного продукта (на примере конкретного документа, например, научно-технической документации, плана развития и т.п.).
5. Руководство Вашей фирмы получило научно-техническую информацию, ускоряющую разработку Ваших продуктов (прогноз развития рынка или отрасли). Оцените (по формуле 1.1) экономию (в руб.) рабочего времени работы руководителей и специалистов,

если получение этих сведений своими силами заняло бы 5 месяцев для 2-х ведущих специалистов.

Отчет о выполненной работе оформляется в соответствии с установленными требованиями.

Контрольные вопросы:

1. Какова роль информации в проведении конкурентной борьбы?
2. Почему информация также является товаром?
3. Какими основными свойствами обладает информация как товар?
4. Какими другими свойствами обладает информация как товар?
5. Что представляет собой рынок информации в России?
6. Системы классификации информации на предприятии.
7. Как выбрать базы для наблюдения?
8. Откуда брать необходимую для работы предприятия информацию?
9. Как классифицировать информацию, поступающую из внешней среды в организацию?
10. Система информации. Какой вклад вносит стратегическая, тактическая и оперативная информация в базы данных организации (фирмы)?
11. Какие существуют способы координации ССПИ и СТОИ?
12. Что необходимо сделать для создания системы стратегической информации?

2. Практическая работа №2. Коммерческая тайна организации

2.1. Коммерческая тайна и способы её добывания

Под коммерческой тайной (КТ) организации (фирмы) понимаются не относящиеся к государственным секретам сведения, связанные с производством, технологией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам.

Состав и объем сведений составляющих КТ, определяются руководством предприятия. Для того, чтобы иметь возможность контролировать деятельность предприятий, Правительство России выпустило 05.12.1991 г. Постановление № 35 (ред. от 03.10.2002) "О перечне сведений, которые не могут составлять коммерческую тайну, 29.07.2004 г. Федеральный закон от № 98-ФЗ (ред. от 09.03.2021) "О коммерческой тайне", статья 5.

Перечень сведений, относящихся к КТ и носящий рекомендательный характер, может быть сгруппирован по тематическому принципу.

Сведения о финансовой деятельности - прибыль, кредиты, товарооборот; финансовые отчеты и прогнозы; коммерческие замыслы; фонд заработной платы; стоимость основных и оборотных средств; кредитные условия платежа; банковские счета; плановые и отчетные калькуляции.

Информация о рынке - цены, скидки, условия договоров, спецификация продукции, объем, история, тенденции производства и прогноз для конкретного продукта; рыночная политика и планирование; маркетинг и стратегия цен; отношения с потребителем и репутация; численность и размещение торговых агентов; каналы и методы сбыта; политика сбыта; программа рекламы [4,5,6,7,8].

Сведения о производстве продукции - сведения о техническом уровне, технико-экономических характеристиках разрабатываемых изделий; сведения о планируемых сроках создания разрабатываемых изделий; сведения о применяемых и перспективных технологиях, технологических процессах и т.д.

Сведения о научных разработках - новые технологические методы, новые технические, технологические и физические принципы; программы НИР; новые алгоритмы; оригинальные программы.

Сведения о материально-техническом обеспечении - сведения о составе торговых клиентов, представителей и посредников; потребности в сырье, материалах, комплектующих узлах и деталях, источники удовлетворения этих потребностей; транспортные и энергетические потребности.

Сведения о персонале предприятия - численность персонала

предприятия; определение лиц, принимающих решения.

Сведения о принципах управления предприятием - сведения о применяемых и перспективных методах управления производством; сведения о фактах ведения переговоров, предметах и целях совещаний и заседаний органов управления; сведения о планах предприятия по расширению производства; условия продажи и слияния фирм.

Прочие сведения - важные элементы системы безопасности, кодов и процедур доступа, принципы организации защиты коммерческой тайны.

Органами, предназначенными для добывания коммерческой информации, являются органы коммерческой разведки. Разведка коммерческих структур (коммерческая разведка) добывает информацию в интересах их успешной деятельности фирмы на рынке в условиях острой конкурентной борьбы.

Органы добывания условно можно разделить на агентурные и технические.

Добывание информации производится путем проникновения агента к источнику информации на расстояние доступности его органов чувств или используемых им технических средств, копирования информации и передачи ее потребителю.

Развитие технической разведки связано, прежде всего, с повышением ее технических возможностей, обеспечивающих:

- снижение риска физического задержания агента службой безопасности организации (фирмы) за счет дистанционного контакта его с источником информации;

- добывание информации путем съема ее с носителей, не воздействующих на органы чувств человека.

Информационно-аналитическая работа должна предшествовать принятию решения. Основные направления действий информационно-аналитической службы организации (фирмы) – это анализ и прогнозирование.

В ходе видовой и комплексной обработки формируются первичные и вторичные сведения на основе методов синтеза информации и процедур идентификации и интерпретации данных и сведений.

Формирование первичных сведений производится путем сбора

и накопления данных и "привязки" их к тематическому вопросу, по которому добывается информация. Для включения данных в первичные сведения необходимо, чтобы эти данные содержали информационный признак о принадлежности данных к информации по конкретному вопросу. Если такой признак отсутствует, то имеет место простое накопление данных.

При формировании сведений применяются следующие методы синтеза информации: логические, структурные, статистические.

Логические методы используют для синтеза информации законы логики, учитывающие причинно-следственные связи в реальном мире. Причинно-следственные временные связи обеспечивают также выявление и прогнозирование действий объектов по признакам их деятельности в различные моменты времени.

Структурные методы учитывают объективно существующие связи между элементами объекта. Например, любой прибор имеет многоуровневую иерархическую структуру. Она включает блоки, узлы и детали, которые во время работы взаимодействуют друг с другом. Эти связи определяют конструкцию прибора и зафиксированы в конструкторской документации. При ее отсутствии специалисты восстанавливают конструкцию, назначение и функции по отдельным элементам и связям.

Статистические методы обеспечивают идентификацию и интерпретацию объектов и характера их деятельности по часто проявляющимся признакам, получаемым в результате статистической обработки добываемых данных. В качестве таких признаков выступают статистически устойчивые параметры случайных событий: средние значения, дисперсии, функции распределения. Например, частое появление возле территории организации (фирмы) одних и тех же людей и автомобилей, обнаружение в помещениях фирмы закладных устройств - служат признаками повышенного интереса конкурента или других субъектов к организации (фирме) или к отдельным ее сотрудникам [4,5,6,7,8].

2.2. Исходные данные для проведения работы

1. Условия работы организации (фирмы) аналогичные указанным в ПР №1.

2. Программа «Бизнес-план».

2.3. Задание

1. Ознакомиться с программой «Бизнес–план» и получить ответы на следующие вопросы:

- из каких составляющих складывается цена потребления?
- какие методы конкуренции рекомендуется использовать для товаров с эластичным и неэластичным спросом?
- при какой величине соотношения продажная цена/цена потребления снижение продажной цены не приводит к повышению конкурентоспособности товара?
- возможные стратегии фирмы при осуществлении нововведений?
- какие технические параметры используются для оценки конкурентоспособности выпускаемых изделий?

2. Определите цену потребления Вашего продукта.

3. Укажите диапазон продажной цены продукта Вашей организации (используемый для управления его конкурентоспособностью).

4. Какие методы конкуренции (ценовые или неценовые) Вы будите применять?

5. Какую ценовую политику выхода на рынок Вы будете использовать для своего товара?

6. По каким техническим параметрам и как Вы будите производить анализ конкурентоспособности изделий?

1. Контрольные вопросы:

1. Что такое коммерческая тайна организации (фирмы)?
2. Кто определяет состав и объем сведений, составляющих КТ?
3. Перечень сведений, которые не могут составлять КТ.
4. Какие сведения могут быть отнесены к КТ?
5. Какая информация используется для стратегического планирования?

6. Что такое бизнес-план? Основные разделы бизнес-плана.
7. Зачем проводится технико-экономическое обоснование проекта и для кого предназначен этот документ?
8. Откуда исходит угроза риска при реализации проекта?
9. Как уточнить исходную информацию и получить прогноз выполнения проекта?
10. Оценка предпринимательского риска и методы его снижения.
11. Органы добывания коммерческой информации.
12. Чем занимается коммерческая разведка?
13. Принципы деятельности информационно-аналитической службы организации (фирмы).

3. Практическая работа №3. Минимизация риска и защита информации при заключении договоров

3.1. Организация и порядок проведения совещаний и переговоров

Существует установившийся порядок проведения совещаний и переговоров по вопросам, составляющим коммерческую тайну.

Руководитель, давший разрешение на проведение таких совещаний (переговоров), назначает ответственного за их проведение. Последний составляет список его участников с указанием фамилии, имени и отчества, должности и предприятия.

На совещание пропускаются только те лица, фамилии которых указаны в списке.

Проводящий совещание (переговоры) обязан напомнить участникам встречи о необходимости сохранения коммерческой тайны и уточнить конкретно, какие сведения являются охраняемыми. Это напоминание фиксируется в протоколе совещания (переговоров).

Совещания проводятся в специально отведенных для этого аттестованных помещениях, исключающих возможность применения визуально-оптических, акустических и других технических средств, которые могут быть использованы

злоумышленниками, как в самом помещении, так и за его пределами [9,10,11,12].

На каждом совещании, связанном с вопросами, составляющими коммерческую тайну, ведется протокол (письменный или цифровая запись), в котором фиксируется доклад, информация, выступления, вопросы к докладчику.

Отдельные переговоры по вопросам коммерческих секретов оформляются в виде записи бесед.

Все материалы передаются в группу обеспечения безопасности внешней деятельности.

Под аттестацией помещения понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что помещение соответствует требованиям стандартов нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации в пределах его компетенции.

Сделки совершаются в различных формах. Однако, независимо от вида сделки, одним из важнейших требований являются:

-выбор делового партнера;

-обеспечение защиты конфиденциальных сведений в договорной документации;

-обеспечение достоверности договорной документации.

Работа над любой сделкой начинается с определения качества исходной информации. При получении разового коммерческого предложения или предложения об установлении долгосрочного делового партнерства от совершенно неизвестной коммерческой структуры, прежде всего, необходимо обратить внимание на способ уведомления заинтересованной в сотрудничестве с вами стороной, о своих намерениях и стиле их изложения.

Общепринятая деловая практика – предварительное уведомление о своих намерениях в виде сопроводительного письма-обращения на имя руководителя и краткого коммерческого предложения. Уже на этом этапе можно получить некоторое представление о потенциальном партнере и стиле его работы.

Основная его цель - вызвать у противоположной стороны заинтересованность в дальнейших деловых контактах, поэтому

коммерческое предложение должно содержать четкие и ясные формулировки. Объем коммерческого предложения зависит от конкретной ситуации.

В случае получения первой информации о предложении от конкретного представителя необходимо обратить внимание на следующее:

- каждый представитель обязан иметь на руках нотариально заверенную доверенность с общепринятыми реквизитами, в которой указывается, что и в каких пределах может совершать этот человек от лица организации ее выдавшей;

- представитель уважающей себя организации обязан иметь при себе максимум открытой информации о своем работодателе: рекламные проспекты, каталоги, прайс-листы, вплоть до типовых форм контрактов;

- поинтересоваться у представителя об источниках информации о существовании вашей организации. Так, если ответ на данный вопрос звучит убедительно и аргументировано, то это свидетельствует о деловой компетентности представителя. В противном случае следует отказаться от дальнейших контактов.

При вашей заинтересованности в предложениях представителя можно сделать телефонный звонок (естественно, в отсутствии последнего) в офис его организации. Если представитель имеет офис в вашем городе, то можно попросить своего сотрудника съездить по указанному адресу и выяснить, соответствует ли информация действительности.

Указанных рекомендаций достаточно, чтобы при минимальных затратах времени и средств составить общее представление о серьезности и чистоте намерений контрагента в отношении вашей организации.

Существенным фактором, влияющим на принятие решения, является наличие на встрече предложения в формате стандартной бизнес - справки, которая должна содержать следующие основные сведения:

- полное наименование организации;
- дата и место регистрации;
- регистрационный номер;
- юридическую форму собственности;

- наименования или имена учредителей;
- имена руководителей;
- сферу деятельности;
- годовой оборот;
- количество сотрудников;
- наименование банков, в которых обслуживается эта фирма;
- информацию о финансовом состоянии и деловых партнерах.

Если речь идет о долгосрочном сотрудничестве, желательно, чтобы потенциальный партнер предоставил также развернутый бизнес-план.

Заключительным, самым важным и ответственным этапом для принятия вами окончательного решения является проверка достоверности информации. Очень важно также выяснить такие дополнительные аспекты, как деловая репутация потенциального партнера, его отношения с властями, связи с криминалом, участие в судебных разбирательствах, учредительство или деловое участие руководства в других коммерческих структурах. Особенно внимательно, по понятным причинам, нужно отнестись к проверке посреднических структур. Перечень сведений, которые не могут составлять коммерческую тайну, можно получить в следующих организациях:

- регистрационные палаты предоставляют: регистрационный номер, юридический адрес, имя руководителя, код ОКПО, а иногда и Устав; регистрационный номер, юридический адрес, уставной капитал, вид деятельности, наименования и адреса учредителей, номинал акций или объемы делового участия инвесторов;
- лицензионные палаты (лицензия на право заниматься определенным видом деятельности);
- налоговые органы (сведения об уплате налогов и обязательных бюджетных платежей);
- органы внутренних дел (паспортные данные, судимости, сведения о нарушении правил противопожарной безопасности, правил дорожного движения и т.д.);
- судебные органы (уголовные, гражданские, арбитражные дела);
- кредитно-финансовые организации.

Кроме того, заслуживает внимания информация, которая может

быть представлена органами местной исполнительной власти (сведения о владельце недвижимости, арендаторе, субарендаторе, своевременности внесения арендной платы, коммунальных платежей), городскими и районными АТС (сведения о своевременности оплаты телефонных переговоров), городскими или районными электро-энергетическими службами (сведения о своевременности оплаты потребляемой электроэнергии, проводимых ремонтных и профилактических работах), адресными бюро, справочными и телефонными службами.

Организации или частные лица, заинтересованные в получении информации, должны направить в перечисленные ведомства письменный запрос и вправе рассчитывать на получение официального ответа по существу обращения [9,10,11,12].

3.2. Предпринимательский риск и методы его снижения

Под риском принято понимать вероятность (угрозу) потери предприятием части своих ресурсов, не до получения доходов или появления дополнительных расходов в результате осуществления определенной производственной и финансовой деятельности.

Эффективность организации управления риском во многом определяется знанием его разновидностей. С экономической точки зрения интересны не все виды рисков, а лишь те, которые влияют на экономическое положение предприятий.

Чистые риски - природно-естественные, экологические, политические, транспортные и часть коммерческих рисков (имущественные, производственные, торговые).

Особое значение приобретает анализ и оценка предпринимательского риска. Цель анализа риска заключается в том, чтобы предоставить необходимую информацию руководству для принятия решений о целесообразности инвестиций и предусмотреть меры по защите от возможных потерь.

Существуют следующие методы анализа риска:

- статистический;
- анализ целесообразности затрат;
- аналитический;
- экспертных оценок;

- аналогий.

Чтобы количественно определить величину риска, необходимо знать возможные последствия какого-нибудь отдельного действия и вероятность самих последствий [9,10,11,12].

Таким образом, математическое ожидание какого-либо события равно абсолютной величине этого события, умноженной на вероятность его наступления.

В связи с этим особый интерес представляет количественная оценка риска с помощью методов математической статистики. Главные инструменты данного метода оценки - дисперсия, стандартное отклонение, коэффициент вариации.

Соотношение максимально возможного убытка и собственных ресурсов представляют собой степень риска. Её можно выразить с помощью коэффициента риска.

$$К_р = \frac{У_{max}}{С}, \quad (1.2)$$

где Кр – коэффициент риска;

У*max* – максимально возможная сумма убытков, руб.;

С – объем собственных ресурсов.

Способы минимизации риска делятся на средства разрешения рисков и приемы снижения степени риска.

Средствами разрешения рисков являются избежание, передача или снижение их степени.

Избежание риска означает уклонение от мероприятий, связанных с риском.

Передача риска означает, что ответственность за риск передается кому-то другому, зачастую страховой компании. В данном случае, передача риска происходит путем страхования риска.

Снижение степени риска – это сокращение вероятности и объема потерь.

Для этого применяют различные приемы. Наиболее распространенными являются:

- диверсификация;
- хеджирование;
- самострахование;

- страхование.

Диверсификация производственной деятельности заключается в распределении усилий и капиталовложений между разнообразными видами деятельности, непосредственно не связанными друг с другом. В таком случае если в результате непредвиденных событий один вид деятельности будет убыточным, другой вид все же будет приносить прибыль.

Следует различать концентрическую и горизонтальную диверсификацию. Концентрическая диверсификация - это пополнение ассортимента изделиями, похожими на продукцию уже выпускаемую предприятием. Горизонтальная диверсификация представляет собой пополнение ассортимента изделиями, не похожими на товары предприятия, но интересными для потребителей. Метод диверсификации позволяет снижать производственные, коммерческие и инвестиционные риски.

В последнее время с развитием рыночных отношений появились новые формы торговых сделок. В связи с этим у предприятий появился новый способ компенсации возможных потерь от риска – хеджирование (от английского hedging – ограждать). Хеджирование, как правило, используется для минимизации рисков снабжения в условиях высоких инфляционных ожиданий и отсутствие надежных каналов закупок. В самом общем виде хеджирование можно определить, как страхование цены товара от риска, либо нежелательного для производителя падения, либо невыгодного потребителю увеличения путем создания встречных валютных, коммерческих, кредитных и иных требований и обязательств. Таким образом, хеджирование может использоваться предприятием с целью страхования прогнозируемого уровня доходов путем передачи риска другой стороне. Например, предприятие, желая оградиться от возможных потерь в связи с ростом цен на сырье, заключает срочный товарный контракт на бирже на покупку сырья по твердым ценам в определенный срок, тем самым, перекладывая возможный риск на поставщика. Поставщик же, в свою очередь, гарантирует себе сбыт определенного количества сырья и получения утвержденной цены на него даже в случае падения рыночной цены.

Приемлемым для предприятия вариантом минимизации риска

может стать самострахование некоторых видов рисков, т.е. есть создание специального резервного фонда (фонда риска) за счет отчисления от прибыли, на случай возникновения непредвиденной ситуации. Самострахование целесообразно в том случае, когда стоимость страхуемого имущества относительно невелика по сравнению с общим объем капитала предприятия. Например, крупному предприятию не выгодно через страховую компанию страховать не дорогое оборудование. Самострахование имеет также смысл, когда вероятность убытка достаточно мала.

Страхование представляет собой одну из экономических категорий производственных отношений. Его сущность заключается в распределении ущерба между всеми участниками страхования. Оно связано с возмещением материальных потерь, что служит основой для непрерывности и бесперебойности процесса воспроизводства.

Нанесенный предприятию в результате страхового случая материальный ущерб представляет собой страховой ущерб, который включает два вида убытков: прямые и косвенные.

Прямой убыток означает количественное уменьшение застрахованного имущества (гибель, повреждение, кража) или снижение стоимости (т.е. обесценивание его) вследствие страхового случая.

В сумму прямого убытка включаются также затраты, понесенные страхователем для уменьшения ущерба, спасения имущества и приведения его в надлежащий порядок после стихийного бедствия или другого страхового случая.

Прямой убыток выступает как первичный ущерб, т.е. как ущерб, который можно наблюдать реально.

Косвенный убыток указывает на ущерб, являющийся следствием гибели (повреждения) имущества или невозможности его использования после страхового случая. К нему относятся: неполученный из-за перерывов в производственном процессе доход, дополнительные затраты на ликвидацию последствий чрезвычайных ситуаций природного и техногенного характера [9,10,11,12].

3.3. Исходные данные для проведения работы

1. Условия работы организации, фирмы, аналогичные указанным в ПР №1.

2. Ваша организация, фирма собирается совершить коммерческую сделку (по выбору): купля; продажа; участие в совместной разработке или производстве продукции; вложение инвестиций в производство или ценные бумаги.

3. Процесс заключения сделки включает следующие этапы:

- проведение переговоров;
- анализ и оценку риска данной сделки;
- выбор партнера;
- минимизацию риска;
- документальное подтверждение сделки;
- обеспечение конфиденциальности переговоров (документооборота) и защиту своей коммерческой тайны в процессе совершения сделки.

3.4. Задание

1. Составьте план телефонного разговора с руководителем организации – предполагаемым партнером по сделке (цель, кому, когда, документация, использование технических средств).

2. Проведите анализ и дайте количественную оценку степени риска предстоящей сделки.

3. Укажите действия по минимизации риска.

4. Каковы будут Ваши действия на всех этапах совершения сделки по снижению предпринимательского риска, обеспечению конфиденциальности переговоров и защите Вашей КТ.

Контрольные вопросы

1. Каков порядок проведения секретных переговоров и совещаний?

2. Чем достигается соответствие помещений требованиям стандартов по безопасности информации?

3. Какие действия необходимо предпринять при выборе коммерческой организации - делового партнера?

4. Как осуществляется проверка достоверности информации о партнере?

5. Назовите виды рисков в предпринимательской деятельности.
6. Какие существуют методы анализа риска?
7. Как определить коэффициент риска?
8. На какие средства делятся способы минимизации рисков?
9. Какие основные приемы снижения степени риска вы знаете?
10. В чем заключается диверсификация и в чем различие концентрической и горизонтальной диверсификации?
11. В чем заключается хеджирование?
12. В чем заключается страхование и самострахование?
13. Что такое прямой и косвенный убыток?

4. Практическая работа №4. Организация работы при подборе кадров, контроль работы сотрудников организации

4.1. Персонал организации и его роль в утечке информации

Анализ угроз информации по возрастанию степени их опасности позволил выделить следующие виды угроз информационным ресурсам:

- некомпетентные служащие;
- хакеры;
- неудовлетворенные своим статусом служащие;
- нечестные служащие;
- инициативный шпионаж;
- организованная преступность;
- политические диссиденты;
- террористические группы.

В связи с этим в целях обеспечения информационной безопасности коммерческих структур необходимо уделять особое внимание подбору и изучению кадров, проверке любой информации, указывающей на их сомнительное поведение и компрометирующие связи.

Психологический профотбор преследует следующие основные цели:

- выявление ранее имевших место судимостей, преступных связей, криминальных наклонностей;

- выявление предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков;
- установлениефактов, свидетельствующих о морально психологической надежности, неустойчивости кандидата на работу.

В настоящее время ведущие коммерческие структуры имеют строго разработанные и утвержденные руководством организационные структуры и функции управления для каждого подразделения. Используются оргсхемы или организационные чертежи, на которых графически изображается каждое рабочее место, прописываются должностные обязанности и определяются информационные потоки для отдельного исполнителя.

Кроме того, для большей конкретизации этих процедур на каждое рабочее место составляются профессиограммы.

Профессиограмма – это перечень личностных качеств с оценочной шкалой, которыми в идеале должен обладать потенциальный сотрудник. Обязательными атрибутами подобных документов являются разделы, отражающие профессионально значимые качества (психические характеристики, свойства личности, без которых невозможно выполнение основных функциональных обязанностей), а также противопоказания (личностные качества, которые делают невозможным зачисление кандидата на конкретную должность) [13,14].

4.2. Основные рекомендации при организации проверки и отбора кандидатов на работу в коммерческие организации

Основными функциями по отбору кандидатов на работу в коммерческие структуры являются следующие:

- определение степени вероятности формирования у кандидата преступных наклонностей в случаях возникновения в его окружении определенных благоприятных обстоятельств (персональное распоряжение кредитно- финансовыми ресурсами, возможность контроля за движением наличных средств и ценных бумаг, доступ к материально-техническим ценностям, работа с конфиденциальной информацией и пр.);
- выявление имевших место ранее преступных наклонностей, судимостей, связей с криминальной средой (преступное прошлое,

наличие конкретных судимостей, случаи афер, махинаций, мошенничества, хищений на предыдущем месте работы кандидата и установление либо обоснованное суждение о его возможной причастности к этим преступным деяниям).

Для добывания подобной информации используются возможности различных подразделений коммерческих структур, в первую очередь службы безопасности, отдела кадров, юридического отдела, подразделений медицинского обеспечения, а также некоторых сторонних организаций, например, детективных агентств, бюро по занятости населения, диспансеров и пр. Для сбора сведений такого характера применяются следующие методы: опрос, анкетирование, целевые беседы с лицами по месту жительства кандидатов и на предыдущих местах их учебы или работы, наведение справок через медицинские учреждения, почерковедческая экспертиза и пр.

Используются тщательно подготовленные процедуры приема и увольнения персонала.

Часто имеют место случаи, когда сотрудник внутренне сам уверен в том, что увольняется по откровенно называемой им причине, хотя его решение сформировано и принято под влиянием совершенно иных, порой скрытых от него обстоятельств.

В этой связи принципиальная задача состоит в том, чтобы определить истинную причину увольнения сотрудника, попытаться правильно ее оценить и решить, целесообразно ли в данной ситуации предпринимать попытки к искусственному удержанию данного лица в коллективе либо отработать и реализовать процедуру его спокойного и бесконфликтного увольнения. Поэтому при поступлении устного или письменного заявления об увольнении рекомендуется провести с сотрудником беседу с участием представителей кадрового подразделения и кого-либо из руководителей коммерческой структуры. Однако до беседы целесообразно предпринять меры по сбору следующей информации об увольняемом сотруднике:

- характер его взаимоотношений с коллегами в коллективе;
- отношение к работе;
- уровень профессиональной подготовки;
- наличие конфликтов личного или служебного характера;

- ранее имевшие место высказывания или пожелания перейти на другое место работы;
- доступ к информации, в том числе составляющей коммерческую тайну;
- вероятный период устаревания сведений, составляющих коммерческую тайну для данного предприятия;
- предполагаемое в будущем место работы увольняющегося (увольняемого) сотрудника.

Беседа при увольнении проводиться лишь только после того, когда собраны все необходимые сведения.

В зависимости от предполагаемого результата беседа может проводиться в официальном тоне либо иметь форму доверительной беседы, задушевного разговора, обмене мнениями. Однако каковы бы ни были планы в отношении данного сотрудника, разговор с ним должен быть построен таким образом, чтобы последний ни в коей мере не испытывал чувства униженности, обиды, оскорбленного достоинства. Для этого следует сохранять тон беседы предельно корректным, тактичным и доброжелательным даже несмотря на любые критические и несправедливые замечания, которые могут быть высказаны сотрудником в адрес коммерческой структуры и ее конкретных руководителей.

Если руководством организации, отделом кадров и службой безопасности все же принято решение не препятствовать увольнению сотрудника, а по своему служебному положению он располагал доступом к конфиденциальной информации, то в этом случае отрабатывается несколько вариантов сохранения в тайне коммерческих сведений (оформление официальной подписи о неразглашении данных, составляющих коммерческую тайну, либо устная договоренность о сохранении увольняемым сотрудником лояльности к своей организации).

В этой связи необходимо подчеркнуть, что личное обращение к чувству чести и достоинства увольняемых лиц наиболее эффективно в отношении тех индивидуумов, которые обладают темпераментом сангвиника и флегматика, высоко оценивающих, как правило, доверие и доброжелательность.

Что касается лиц с темпераментом холерика, то с этой категорией сотрудников рекомендуется завершить беседу на

официальной ноте и тщательно оговаривать и обуславливать в документах возможности наступления для них юридических последствий раскрытия коммерческой тайны.

Несколько иначе рекомендуется действовать в тех случаях, когда увольнения сотрудников происходят по инициативе самих коммерческих структур. Если увольняемое лицо располагает какими-либо сведениями, составляющими коммерческую тайну, то целесообразно предварительно и под соответствующим предлогом перевести его на другой участок работы, например в такое подразделение, в котором отсутствует подобная информация.

Только лишь после реализации этих мер рекомендуется приглашать на собеседование подлежащего увольнению сотрудника и объявлять конкретные причины, по которым коммерческая организация отказывается от его услуг.

После объявления об увольнении рекомендуется внимательно выслушать контрдоводы, аргументы и замечания сотрудника в отношении характера работы, стиля руководства компанией и т.д. Обычно увольняемый персонал весьма критично, остро и правдиво освещает ситуации в коммерческих структурах, вскрывая уязвимые места, серьезные недоработки, кадровые просчеты, финансовые разногласия и т.п.

При окончательном расчете обычно рекомендуется независимо от личных характеристик увольняемых сотрудников брать у них подписку о неразглашении конфиденциальных сведений, ставших известными в процессе работы [12,13,14].

В любом случае после увольнения сотрудников, осведомленных о сведениях, составляющих коммерческую тайну, целесообразно через возможности службы безопасности организации проводить оперативную установку по их новому месту работы и моделировать возможности утечки конфиденциальных данных.

4.3. Исходные данные

1. Условия работы организации, аналогичные указанным в ПР №1.

2. Ваша организация собирается уволить (в соответствии с

интересами организации) трёх сотрудников – начальника производственного отдела, менеджера по продажам и рекламного агента и принять на их место новых работников.

3. Теоретический материал:

- организация и проведение профотбора в коммерческом предприятии;
- этапы и процедуры профотбора (методика проведения);
- процесс увольнения кадров;
- примеры программ тестов профориентации.

4.4. Задание

1. Составьте профили требований (профессиограммы) к данным сотрудникам.
2. Укажите основные мероприятия и процедуры профотбора, проводимые службами Вашей организации в каждом случае.
3. Сделайте выбор тестов (из предложенного набора), которые будут использоваться для проверки каждого из кандидатов.
4. Опишите процедуру увольнения прежних работников и связанные с ней действия администрации организации.

Контрольные вопросы:

1. Какие существуют виды угроз информационным ресурсам?
2. С какой целью проводится психологический профотбор?
3. Что включает в себя профессиограмма?
4. Какие структуры используются для сбора сведений о кандидатах?
5. Какие методы используются для сбора сведений о кандидатах?
6. Назовите тестовые приемы и другие научные методики проверки кандидатов.
7. Особенности проведения итоговой беседы с кандидатами.
8. Какие меры целесообразно предпринять до беседы с увольняемым сотрудником?
9. Какие формы может принимать беседа с увольняемым сотрудником, и каким образом должен быть построен разговор?
10. Какие существуют варианты сохранения в тайне

коммерческих сведений при увольнении сотрудников?

11. Как рекомендуется действовать в тех случаях, когда увольнения сотрудников происходят по инициативе самих коммерческих структур?

5. Практическая работа №5. Защита информации в условиях возникновения чрезвычайных ситуаций

5.1. Виды чрезвычайных ситуаций

Под чрезвычайной ситуацией природного и (или) техногенного характера понимается обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью или окружающей природной среде, значительные потери и нарушение условий жизнедеятельности людей [15,16]. К числу природных катастроф следует отнести:

- землетрясения и оползни;
- наводнения, обусловленные ливнями и прорывами плотин;
- разрушения, вызванные мощными ветровыми нагрузками;
- поражение информационных систем электрическими разрядами.

В последние годы резко возросли угрозы за счет техногенных угроз, обусловленных, прежде всего:

- отказами систем жизнеобеспечения;
- пожарами;
- взрывами за счет утечки бытового газа;
- отравлениями химическими веществами;
- взрывами криминогенного характера.

5.2. Защита информации в чрезвычайной ситуации

Как показывает опыт, наиболее рациональное решение в подобных условиях – это заблаговременное создание специального оперативного штаба по действиям и ликвидации последствий ЧС из

ответственных лиц организации. В его состав, как правило, входят следующие лица:

- генеральный директор (руководитель);
- заместитель генерального директора (руководителя);
- руководители соответствующих региональных или производственных отделов;
- руководители (ответственные представители) отдела кадров, отдела по установлению контактов с общественностью, финансового отдела, службы безопасности.

В соответствии с уже сложившейся практикой оперативный штаб не только предпринимает меры в случае возникновения кризисной ситуации, но также занимается разработкой превентивных мероприятий:

- разрабатывает предупредительные планы сохранения информации, возможной эвакуации персонала с объекта и вывоза материально-технических ценностей;
- осуществляет шаги по координации действий собственной службы безопасности с мероприятиями по линии государственных правоохранительных органов.

Формализованную оценку уровня имущества предприятия по частному функциональному критерию эффективности принимаемых мер защиты можно представить следующим образом:

$$\text{ЧФК} = \frac{\text{У}_{\text{пр}}}{\text{З} + \text{У}_{\text{по}}} \rightarrow max, \qquad (1.3)$$

где ЧФК – частный функциональный критерий уровня защиты имущества;

Упр – суммарный предотвращенный ущерб от реализации комплекса мер по защите имущества предприятия;

З – общая сумма затрат, понесенных предприятием при реализации указанного комплекса мер;

Упо – суммарный ущерб информационным ресурсам, понесенный предприятием в результате наступления чрезвычайных ситуаций [15,16].

5.3. Исходные данные

1. Условия работы организации, аналогичные, указанным в ПР №1.

2. В организации, фирме возникла чрезвычайная ситуация:

- произошел взрыв и пожар;

- нападение с целью хищения конфиденциальной информации и материальных ценностей.

5.4. Задание

1. Дайте количественную оценку возможному ущербу организации в результате данных событий (без принятия специальных мер).

2. Какими мерами, принятыми заблаговременно, можно снизить величину потерь. Оцените стоимость этих мероприятий.

3. Опишите мероприятия по управлению организацией в каждом случае.

4. Укажите перечень и последовательность действий персонала в данных ситуациях.

5. Оцените величину нанесенного организации ущерба и уровень защиты предприятия по частному функциональному критерию эффективности принимаемых мер.

Контрольные вопросы:

1. Что понимается под понятием чрезвычайная ситуация?
2. Какие виды ЧС имеют природный и техногенный характер?
3. Какие мероприятия по управлению организацией проводятся в условиях ЧС?
4. Кто входит в состав оперативного штаба?
5. Какие мероприятия разрабатывает оперативный штаб?
6. Какие условия обеспечивают успешную реализацию плана действий в ЧС?
7. Сведения, которые обязательно указываются в плане?
8. В чем заключается практическая подготовка персонала к действиям в ЧС?
9. Как оценить уровень затрат предприятия на проведение мер предосторожности?

10. Первоочередные действия службы безопасности при возникновении ЧС.

11. Какая информация для правоохранительных органов готовится службой безопасности после нападения на организацию?

Библиографический список

1. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2005. – 186 с.

2. Громов, Ю.Ю. Методы организации защиты информации / Ю.Ю. Громов, О.Г. Иванова, Ю.Ф. Мартемьянов [и др.] – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с.

3. Геннадиева, Е.Г. Технико-экономические задачи защиты информации // Безопасности информационных технологий, 1997. Вып. 3. С. 67-74.

4. Гасанов, Р.М. Промышленный шпионаж на службе монополий. - М.: - 1986.

5. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности / Г.П. Жигулин. – СПб: СПбНИУИТМО, 2014. – 173 с.

6. Зайцев, А.П. Технические средства и методы защиты информации: учебник для вузов / А. П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков [и др.] – М.: ООО Издательство «Машиностроение», 2009. – 508 с.

7. Котлер, Ф. Основы маркетинга. Пер. с англ. М.: Прогресс, 1990. - 736 с.

8. Климов, В.А. Методология формирования перечня сведений, относящихся к служебной или коммерческой тайне. // Конфидент, 1997, №4, с. 11-22.

9. Ларина, И.Е. Экономика защиты информации: учебное пособие / И.Е. Ларина – М.: МГИУ, 2007. – 92 с.

10. Лынник Н. Оценка стоимости объектов интеллектуальной собственности. // Интеллектуальная собственность, №5-6, 1996.

11. Основы экономической безопасности. Под ред. Олейникова Е.А. М.: ЗАО «Бизнес-школа Интел-Сервис», 1997.

12. Соловьев Э. Коммерческая тайна и ее защита. - М.: ЗАО «Бизнесшкола Интел-Синтез», 1997. 96 с.

13. Цуканова, О. А. Экономика защиты информации: учебное пособие / О.А. Цуканова, С. Б Смирнов, 2-е изд., изм. и доп. – СПб.: НИУ ИТМО, 2014. – 79 с.

14. Ярочкин, В.И. Безопасности информационных систем. М.: "Ось-89", 1996. - 320 с.

15. Шмыков, В.В. Безопасности предприятия в условиях рынка: Учебное пособие для студентов ВУЗов. Рязань: Горизонт. 1997. - 148 с.

16. Хозяйственный риск и методы его измерения. Пер. с венг. /Бачкаи Т., Месени Д. И др. / М.: Экономика, 1979. -184 с.