ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.1.33 Управление информационной безопасностью

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Форма обучения очная

СОДЕРЖАНИЕ

1. **Конспект лекций**

Лекция № 1 «Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах»

Лекция № 2 «Задачи и функции службы защиты информации»**.**

Лекция № 3 «Общая структурная система службы защиты информации»

Лекция № 4 «Порядок создания службы защиты информации»

Лекция № 5 «Подбор, расстановка и обучение сотрудников службы защиты информации»

Лекция № 6 «Структура и содержание должностных инструкций сотрудников службы защиты информации»

Лекция № 7 «Принципы управления службой защиты информации»

Лекция № 8 «Значение управленческих решений»

2. **Методические указания по проведению практических занятий**

Практическое занятие № ПЗ-1 Оценочные стандарты в информационной безопасности

Практическое занятие № ПЗ-2 Роль стандартов ИБ

Практическое занятие № ПЗ-3 Оценочные стандарты в информационной безопасности Международный стандарт ISO/IEC 15408

Практическое занятие № ПЗ-4 Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799

Практическое занятие № ПЗ-5 Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".

Практическое занятие № ПЗ-6 Создание СУИБ на предприятии

Практическое занятие № ПЗ-7 Основные процессы СУИБ

Практическое занятие № ПЗ-8 Процессы улучшения СУИБ

Практическое занятие № ПЗ-9 Процесс «Мониторинг эффективности

Практическое занятие № ПЗ-10 Основные процессы СУИБ

Практическое занятие № ПЗ-11 Подбор кадров службы защиты информации

Практическое занятие № ПЗ-12 Методика оценки рисков информационной безопасности предприятия

Практическое занятие № ПЗ-13 Метод оценки рисков на основе модели угроз и уязвимостей

Практическое занятие № ПЗ-14 Методика оценки рисков информационной организации на основе модели информационных потоков

Практическое занятие № ПЗ-15 Разработка корпоративной методики анализа рисков. Методы оценивания информационных рисков

Практическое занятие № ПЗ-16 Оценка рисков по факторам

3. Методические указания по проведению семинарских занятий

Не предусмотрено РУП

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1 (2 часа).
Тема: «Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах»
1.1.1 Вопросы лекции:

1. Место и роль службы защиты информации в системе защиты информации. Назначение службы защиты информации
2. Служба защиты информации координатор деятельности по обеспечению безопасности информации

1.1.2 Краткое содержание вопросов:
1. Место и роль службы защиты информации в системе защиты информации. Назначение службы защиты информации
В условиях формирования общего экономического пространства перед предприятиями особо остро встает задача сохранения коммерческой тайны. Можно сказать определенно: в период становления рынка недобросовестная конкуренция представляет собой серьезную угрозу этому процессу. Стало почти массовым процессом беззастенчивое заимствование интеллектуальной и промышленной собственности (методик, программ, знания и технологии) сотрудниками предприятий, работающими одновременно в кооперативах, малый предприятиях и других коммерческих структурах. К этому следует добавить целенаправленные действия по сманиванию или подкупу рабочих и служащих предприятий конкурента, чтобы завладеть секретами их коммерческой и производственной деятельности.
Современный промышленный шпионаж предполагает использование новейших достижений электроники, непосредственное тайное наблюдение, кражи со взломом, подкуп и шантаж. Речь идет о настоящей "тайной войне". Вот один из показательных примеров, приведенных в статье "Космический товар по минимальным ценам". Американское космическое ведомство весьма заинтересовано в приобретении у России целого ряда образцов космической техники и технологии по ее созданию, которые "в настоящее время предлагаются русскими по минимальным ценам". "Еще несколько лет назад мы намеревались выкрасть кое-что из этого", - заявило одно, пожелавшее остаться неизвестным, должностное лицо администрации США. Урон американскому бизнесу от краж торговых секретов превышает по их оценкам 4 млрд. долларов ежегодно. То, что в мировой практике именуется промышленным шпионажем, мы даже не можем юридически классифицировать. С переходом на рыночные отношения и условия самостоятельности предприятий перед нами встали серьезные проблемы по обеспечению сохранности своих коммерческих секретов и безопасности предприятия.
Отечественный и зарубежный опыт свидетельствует, что основную роль в обеспечении сохранности коммерческой тайны играют сами предприятия, а не государственные органы. Для защиты коммерческих секретов предприятия создают собственные службы

безопасности. Важной предпосылкой создания службы безопасности предприятия является разработка ее структуры, состава, положений о подразделениях, и должностных инструкций для руководящего состава и сотрудников. Состояние юридических, экономических и производственных отношений, материальных, интеллектуальных и информационных ресурсов, выражающее способность предприятия к стабильному функционированию (успешной финансово-коммерческой деятельности) составляет сущность его безопасности. Цели обеспечения безопасности предприятия определяют главные задачи основной деятельности службы безопасности, которые направляет на устранение внешних и внутренних угроз безопасности предприятия, преодоление негативных тенденций развития и обеспечение благоприятных условий его деятельности. Целями обеспечения безопасности предприятия являются:

- защита законных прав предприятия во взаимоотношениях с государственными органами, российскими и зарубежными партнерами и конкурентами; поддержание устойчивости порядка управления предприятием;
- сохранение собственности предприятия, ее рационального и эффективного использования в направлении удовлетворения общественных потребностей;
- повышение конкурентоспособности производимых товаров и услуг, создание благоприятной рыночной конъюнктуры для их реализации в условиях конкуренции на внутреннем и мировом рынке; рост прибылей предприятия;
- достижение внутренней и внешней организационной стабильности деятельности предприятия, надежности кооперированных связей и недопущение односторонней зависимости от случайных и недобросовестных партнеров;
- укрепление дисциплины труда и его производительности, формирование стимулов и условий повышения деловой активности сотрудников предприятия;
- максимально полное информационное обеспечение экономической, производственной и научно-технической деятельности предприятия, сохранение государственной и коммерческой тайны прав на интеллектуальную собственность, повышение эффективности использования имеющейся информации в мероприятиях по повышению деловой репутации предприятия среди российских и зарубежных партнеров.

2.Служба защиты информации координатор деятельности по обеспечению безопасности информации.

Средства и методы обеспечения безопасности

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 орг-структурных 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 ввиду 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 одновременное внедрение всех вышеуказанных 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:

технические - наблюдение, контроль, идентификация и т.д.;

Организационные - создание зон безопасности, режим, расследование, посты, патрули и т.д.;

информационные - составление детективами характеристик на сотрудников, аналитические материалы и учеты конфиденциального характера и т.д.;

финансовые – материальное стимулирование сотрудников, имеющих достижения в обеспечении безопасности, денежное поощрение информаторов и т.д.;

правовые - судебная защита законных прав и интересов, содействие правоохранительным органам и т.д.;

кадровые - подбор, расстановка и обучение кадров, обеспечивающих безопасность предприятия, их воспитание и т.д.;

интеллектуальные -патентование, ноу-хау и т.д.

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:

а) исходное состояние объекта, на преобразование которого направлена концепция;

б) состояние объекта, достигнутое в результате реализации концепции;

в) меры, необходимые для достижения сформулированных в концепции целей;

г) средства, необходимые и достаточные для достижения поставленных целей;

д) источники ресурсного обеспечения, используемые в ходе реализации концепции;

е) 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 реализации 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. 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:
I. 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.
II. 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 орг-структуры по управлению системой безопасности предприятия.
III. 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 ввиду, 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.

1. 2 Лекция № 2 (2 часа).
Тема: «Задачи и функции службы защиты информации»
1.2.1 Вопросы лекции:
1. Организационные задачи и функции службы защиты информации
2. Технологические задачи и функции службы защиты информации
3. Координационные задачи и функции службы защиты информации
1.2.2 Краткое содержание вопросов:
1. Организационные задачи и функции службы защиты информации
Обеспечивать и организовывать разработку перечней сведений конфиденциального характера.
Организовывать специальное делопроизводство исключающее несанкционированное получение конфиденциальной информации.
Обрабатывать и хранить конфиденциальные документы.
Своевременно выявлять угрозы защищаемой информации компании, причины и условия их возникновения и их реализации.

Анализировать возможности возможности возникновения новых каналов утечки информации, и разрабатывать методы и рекомендации по их пресечению.
Выявлять и максимально перекрывать потенциально возможные каналы и методы несанкционированного доступа к информации.
Предотвращать несанкционированный доступ к информации.
Разрабатывать и проводить мероприятия, предотвращающие вынос персоналом из помещения предприятия документов, дисков, дискет и др. носителей информации.
Для выполнения организационных задач, служба защиты информации выполняет следующие организационные задачи.

1. Организация и обеспечение режима ограничения доступа к источникам и носителям защищаемой информации;
2. Обеспечение организацией в ведение в делопроизводство конфиденциального характера;
3. Ограничение по режиму допуска к сведениям конфиденциального характера;
4. Организационно-правовое и методическое обеспечение работ по регулированию отношений, связанных с использованием сведений с ограниченным доступом;
5. Обследование производственной и административной деятельности, для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведения учета и анализ нарушения режима безопасности информации;
6. Организация и проведение служебных расследований по фактам разглашения конфиденциальных сведений, а также утраты документов содержащих такие сведения;
7. Обеспечение строгого выполнения требования нормативных документов по защите информации;
8. Регулярное проведение учебы сотрудников по всем направлениям защиты информации;
9. Ведение учета технических средств, в том числе спец хранилищ, средств вычислительной техники, используемых с данными ограниченного распространения;
10. Создание специального справочного фонда по вопросам защиты информации;
11. Сбор и анализ сведений по различным аспектам защиты информации в других предприятиях для использования в работе;
12. Обеспечение своевременного выявления недостатков и совершенствование комплекса мероприятий по реализации политики защиты информации;
13. Сбор, аналитическая обработка и оценка сведений о потенциальных и реальных конкурентах, в том числе и зарубежных, с целью выявления возможных противоправных действий по добыванию ими сведений и перекрытия каналов утечки информации.

2. Технологические задачи и функции службы защиты информации

Анализировать и оценивать реальную опасность перехвата информации технологическими средствами, негласного съема информации, предотвращать возможные несанкционированные действия по модификации, копированию, уничтожению и блокированию информации;
Предотвращать потерю и утечку информации, перехвата и вмешательство злоумышленников на всех уровнях обработки данных и для всех объектов;
Противодействовать средствам технической разведки активными и пассивными методами;
Обеспечивать целостность данных на всех этапах их преобразования и сохранность средств программного обеспечения.
Предотвращать утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).
Защищать информацию от компьютерных вирусов.
Защищать информацию от сбоев в системе питания.
Защищать информацию от копирования.
Защищать каналы передачи данных программными средствами.

Формировать рубежи охраны территории, зданий, помещений, оборудования с помощью комплексных технических средств.
Изучать и анализировать и оценивать состояние системы технической защиты информации и разрабатывать предложение и рекомендации по ее совершенствованию.
Для выполнения всех этих задач служба защиты информации заключается в следующем:
1. Обследовать объект с целью возможных каналов утечки информации.
2. Формирование перечней каналов утечки информации на основе анализа моделей технических разведок и угроз.
3. Разработка и внедрение средств инженерно-технической защиты информации и контроля их эффективности.
4. Анализ эффективности применения средств защиты и контрольно-измерительной аппаратуры.
5. Обеспечение юридической значимости электронных документов.
6. Оптимизация, использование информационных и вычислительных ресурсов путем контроля параметров надежности технических средств, а также выявление и прогнозирование критических ситуаций.
3. Координационные задачи и функции службы защиты информации
Деятельность СБ направлена на подержание выживания объекта путем сохранения или получения макс. прибыли за счет минимизации угроз. Это может достигаться только при активном противодействии внешним и внутренним угрозам.
Прежде чем приступать к созданию СБ, нужно определить объект защиты, чье уничтожение приведет к прекращению получения прибыли или нанесению ущерба.
Определить возможные угрозы следовательно выбрать адекватные средства защиты.
К координационным задачам службы безопасности относится:
- участие СБ в расстановке кадров, выявлением негативных тенденции в трудовых коллективах, возможных причин и условий соц. напряженности,
- оказание управленческих воздействий на создание/поддержку своевременной реорганизацию структуры управления без-ти предприятия,
- взаимодействия и координации между отдельными звеньями (отделами, группами) для достижения целей безопасности.

1. 3 Лекция № 3 (2 часа).
Тема: «Общая структурная система службы защиты информации»
1.3.1 Вопросы лекции:
1. Подразделения службы защиты информации
2. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ
3.Задачи, функции, права и ответственность заместителя (помощника) руководителя предприятия по безопасности в области защиты информации
1.3.2 Краткое содержание вопросов:

1. Подразделения службы защиты информации
В общем, структура службы безопасности и ее численность будут зависеть от формы собственности предприятия, вида его производственной деятельности, места предприятия на рынке товаров и услуг, числа сотрудников, наличия на предприятии крупных материальных ценностей, взрыво- и пожароопасных веществ, информации, составляющей гостайну, активности конкурентов и криминальных структур. Поэтому представить универсальную структуру службы безопасности невозможно, однако можно выделить основные структурные подразделения, которые должны присутствовать в большинстве

случаев при организации СБ на крупных промышленных государственных, акционерных предприятиях, в промышленно-финансовых группах, холдингах и т. п.
Организационно служба безопасности состоит из следующих структурных единиц:

- отдел режима и охраны, в составе сектора режима и сектора охраны;
- отдел защиты информации;
- инженерно-техническая группа;
- группа безопасности внешней деятельности.

2. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ

1. Состав и штатную численность отдела по защите информации утверждает директор предприятия исходя из условий и особенностей деятельности предприятия по представлению начальника отдела и по согласованию с _____ (отделом кадров; отделом организации и оплаты труда)
2. В состав отдела входят группы специалистов: инженеров по защите информации, инженеров-программистов, инженеров-электроников, техников-программистов, техников по защите информации, отвечающих за отдельные на-правления в работе (за анализ состояния информационных баз, определение требований к защищенности различных подсистем автоматизированной системы предприятия и выбор методов и средств обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам обеспечения информационной безопасности; за эффективное применение и администрирование штатных для операционных систем и систем управления базами данных и дополнительных специализированных средств защиты и анализа защищенности ресурсов автоматизированных систем).
Следует помнить, что применяемые на практике наименования "Администратор средств защиты, контроля и управления безопасностью", "Системный администратор", "Аналитик по вопросам технической защиты информации и компьютерной безопасности" вводить в положение об отделе, должностные инструкции и иные кадровые документы не следует. Дело в том, что Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов (ОКПДТР) не содержит таких наименований и, соответственно, их применение до внесения изменений в ОКПДТР недопустимо.
Начальник отдела по защите информации распределяет обязанности между сотрудниками отдела и утверждает их должностные инструкции.
Структура СБ иерархическая
1. руководитель предприятия
2. руководитель СБ
3. консультанты по различным вопросам
К консультантам по различным вопросам относятся:
1. Группа собственников безопасности. В их функции входит изучение и проверка сотрудников СБ, пожарной охраны, работа с персоналом, проведение регламентных работ.
2. Группа режима. В их функции входит работа с персоналом, контроль, проверка работа с клиентами, организация и контролирование конфиденциального делопроизводства и составление перечня конфиденциальных данных.
3. Служба охраны. В их функции входит: физ. охрана объекта, выделенная охрана, доставка грузов, проверка почтовых сообщений.
4. Аналитическая группа. В их функции входит сбор информации, анализ, подготовка рекомендации.
5. Детективная группа. В их функции входит работа с персоналом, клиентами, проверка окружения объекта, конкуренты, связь с правоохранительными органами.

6. Группа противодействия технической разведке. В их функции входит защита технических средств передачи информации, ВТ, проведение спец. исследований, обеспечение связи.
7. Группа ЗИ от НСД. В их функции входит защита ЭВМ и ЛВС, разработка защищенных технологий обработки информации
8. Криптографическая группа. В их функции входит ЗИ в компьютерах, сетях.
Начальник службы безопасности должен:
1. Требовать от всех сотрудников неукоснительного выполнения внутриобъектовых правил режима нормативно-правовых обязательств, действующих на предприятии.
2. Требовать от руководителей подразделений и исполнителей правильного и своевременного выполнения нормативных документов по организации и ведению специального делопроизводства.
3. Вводить тотальную проверку эффективности защиты обработки информации внутри объекта.
4. Запретить использование технических и программных средств, не соответствующих требованиям безопасности.
5. Требовать от функциональных подразделений необходимых сведений для анализа информационной безопасности.
6. Вносить предложения по совершенствованию организационных, технических мероприятий по повышению безопасности.
7. Планировать деятельность СБ, подтверждая ее у руководителя
8. Требовать гарантированного финансирования мероприятий запланированных деятельности СБ.

3. Задачи, функции, права и ответственность заместителя (помощника) руководителя предприятия по безопасности в области защиты информации
Обязанности сотрудников СБ.
- разрабатывать организационные, организационно-технические и технические мероприятия по обеспечению надежности деятельности предприятия
- осуществлять постоянный контроль за соблюдением безопасности
- постоянно контролировать СЗ
- обеспечивать организацию специальных исследований технических и программных средств и аттестацию выделенных помещений
- осуществлять сбор и анализ информации для выявления угроз и злоумышленных действий
- докладывать руководителю о фактах нарушений требований нормативных документов и др. действий, которые могут привести к нарушению безопасности
- отчитываться перед руководством СБ о состоянии СЗ и планах своей деятельности
- организовывать, проводить обучение сотрудников предприятия по требованиям безопасности
- в случае возникновения ЧС принимать все возможные меры для ее локализации, устранению последствий, восстановлению норм работы СЗ
Сотрудники СБ несут персональную ответственность за личные нарушения мер безопасности, неудовлетворительное выполнение служебных обязанностей и не исполнения своих прав при функциональных задач.
Функции директора по безопасности
1.1. Директор по безопасности относится к категории руководителей.
1.2. Директор по безопасности назначается на должность и освобождается от нее приказом генерального директора.
1.3. Директор по безопасности подчиняется непосредственно генеральному директору.
1.4. На время отсутствия директора по безопасности его права и обязанности переходят к другому должностному лицу, о чем объявляется в приказе по организации.

1.5. На должность директора по безопасности назначается лицо, отвечающее следующим требованиям: высшее образование и стаж управленческой работы в соответствующей области не менее 3 лет.
1.6. Директор по безопасности должен знать:
- законы и иные нормативно-правовые акты Российской Федерации, регламентирующие вопросы безопасности, частной охранной деятельности, защиты информации, оперативно-розыскной деятельности;
- принципы организации охраны объектов организации;
- технические средства защиты объектов от несанкционированного доступа к ним;
- технические средства защиты информации;
- требования к разработкам внутренних документов по режиму на объектах, инструкций по допуску к ресурсам предприятия (финансовым, товарно-материальным, информационным, пр.);
- правила сопровождения особо ценных товарно-материальных, финансовых и иных ресурсов;
- методы проведения инструктажа по безопасности, проведения контрольных мероприятий.
1.7. Директор по безопасности руководствуется в своей деятельности:
- законодательными актами РФ;
- Уставом организации, Положением о службе безопасности, Правилами внутреннего трудового распорядка, другими нормативными актами компании;
- приказами и распоряжениями руководства;
- настоящей должностной инструкцией.
Директор по безопасности выполняет следующие должностные обязанности:
2.1. Организует и возглавляет работу по правовой и организационной защите предприятия.
2.2. Разрабатывает и руководит мероприятиями по обеспечению безопасности охраняемых объектов.
2.3. Вырабатывает адекватные угрозе средства защиты и виды режимов охраны.
2.4. Осуществляет проверку и оценку лояльности сотрудником компании.
2.5. Обеспечивает неприкосновенность перевозимых материальных ценностей компании.
2.6. Обеспечивает соблюдение контрольно-пропускного режима.
2.7. Взаимодействует с правоохранительными органами в расследовании случаев преступных посягательств на охраняемые объекты.
2.8. Проводит обучение и тренинги персонала по вопросам безопасности.
2.9. Организует специальный режим делопроизводства, исключающий несанкционированное получение сведений, находящихся под режимом особого доступа.
2.10. Предотвращает необоснованный допуск и доступ к сведениям и работам, составляющим коммерческую тайну предприятия.
2.11. Оценивает необходимость привлечения для несения охраны объекта службы безопасности МВД, коммерческих охранных структур на договорной основе.
2.12. Контролирует соблюдение требований режима безопасности сотрудниками и посетителями.
2.13. Организует и проводит служебные расследования по фактам разглашения сведений, утрате документов, ценностей и других нарушений безопасности предприятия.
2.14. Возглавляет разработку основополагающих документов с целью закрепления в них требований по обеспечению безопасности предприятия (инструкции, положения, правила).
2.15. Вносит предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите безопасности предприятия.
2.16. Организует учет и анализ нарушений режима.

1. 4 Лекция № 4 (2 часа).
Тема: «Порядок создания службы защиты информации»
1.4.1 Вопросы лекции:
1.Структура и содержание положения о службе защиты информации
2.Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации
1.4.2 Краткое содержание вопросов:
1. Структура и содержание положения о службе защиты информации
В положение содержится :
- основные задачи и цели по ЗИ
- на основании каких нормативных документов создаётся
- какими нормативными актами руководствуется отдел в своей работе
- запись о штатной численности и структуре
- основные понятия и определения
- кто руководит отделом, кто его замещает на период отсутствия
- порядок приёма на работу специалистов отдела
В разделе описывается регламентация поддержания взаимодействия с другими отделами или предприятиями. А также то, что отдел защиты информации свою работу проводит в тесном контакте и взаимодействии с научными, производственными организациями и территориальными органами ФСБ, ФСО, ФСТЭК России
В разделе ИМУЩЕСТВО И СРЕДСТВА описывается:
- что составляет материально-техническую основу отдела
- ответственность за сохранность имущества
В разделе ТРУДОВЫЕ ОТНОШЕНИЯ описывается:
- на каких нормативных актах строятся трудовые отношения
- на какой основе работают сотрудники (на контрактной)
- регламентируется приём на работу, увольнение, перемещение внутри организации
- чем руководствуются сотрудники в своей работе
- как оплачивается работа сотрудников
- виды поощрения и взыскания
- как решаются трудовые споры
В разделе ОРГАНИЗАЦИЯ РАБОТ описывается:
- плановый порядок
- кто составляет и утверждает планы работы отдела
- внеплановая работа и командировки
- обеспечение конфиденциальности
- регламентация реорганизации и ликвидации отдела
В разделе ФИНАНСИРОВАНИЕ РАБОТ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ описывается:
Изменения существенного характера в настоящее Положение вносятся на основании распоряжения руководителя предприятия и отражаются в приказе.
2. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации
В своей деятельности служба безопасности предприятия руководствуется целым рядом нормативно-законодательных документов, постановлений правительства, которые представляются в виде набора практических инструкций, таких как инструкции:
- по организации режима и охраны (для соответствующих структурных подразделений);
- защите коммерческой тайны;

- работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;
- организации хранения дел, содержащих конфиденциальную информацию и по работе архивов, хранящих эту информацию;
- инженерно-технической защите информации (для соответствующих структурных подразделений);
- порядке работы с иностранными представителями и представительствами и другие,

а также

- перечня сведений, составляющих коммерческую тайну.

Наиболее важным документом, регламентирующим деятельность службы безопасности предприятия, является закон РФ «О частной детективной и охранной деятельности в РФ». Этим законом регламентируется, что учредителями службы безопасности не могут быть физические лица, даже имеющие соответствующие лицензии. В соответствии с законом учредителем службы безопасности может быть только одно предприятие.

В законе четко определено, что служба безопасности создается в интересах собственной безопасности учредителя, однако роль службы безопасности в ее обеспечении не определена. Представляется, что служба безопасности предназначена прежде всего для организации защиты от всех видов угроз.

Детализация различных угроз, устранение, пресечение или их нейтрализация входит в компетенцию службы безопасности, должна быть отражена в ее уставе применительно к основным видам безопасности. Приведем краткий перечень возможных действий службы безопасности по пресечению, устранению или нейтрализации угроз в рамках основных видов безопасности .

1. Физическая безопасность – охрана персонала от насильственных преступлений, предупреждение таких преступлений и т.д.
2. Информационная безопасность – сохранение коммерческой тайны, борьба с хакерами и т.д.
3. Экономическая безопасность – охрана имущества предприятия, борьба с экономическим шпионажем и т.д.
4. Экологическая безопасность – документирование экологических правонарушений, выставление экологических постов и т.д.
5. Пожарная безопасность – проектирование, монтаж и эксплуатационное обслуживание пожарной сигнализации, выставление постов в местах загорания и пожаров и т.д.
6. Техногенная безопасность – охрана наиболее опасных участков предприятия от террористов, участие в расследовании техногенных катастроф и т.д.
7. Психологическая безопасность – информирование персонала предприятия об отсутствии реальных угроз, адекватное реагирование на дезинформационные мероприятия и т.д.
8. Научно-техническая безопасность – охрана ноу-хау, организация охраны научных лабораторий и т.д.

Саму же службу безопасности, призванную обеспечить безопасность предприятия, можно определить как его структурное формирование, осуществляющее в рамках законодательства и собственного устава меры по предотвращению и пресечению угроз интересам своего учредителя.

Правовое обеспечение службы защиты информации на конкретном предприятии (фирме, организации) отражается в совокупности учредительных, организационных и функциональных документов.

Требования обеспечения безопасности и защиты информации отражаются в уставе (учредительном договоре) в виде следующих положений:

предприятие имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз;

предприятие обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации предприятия:

- создавать организационные структуры по защите конфиденциальной информации;
- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- включать требования по защите информации в договоры по всем видам хозяйственной деятельности;
- требовать защиты интересов предприятия со стороны государственных и судебных инстанций;
- распоряжаться информацией, являющейся собственностью предприятия, с целью извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства;
- разработать «Перечень сведений конфиденциальной информации».

Требования правовой обеспеченности защиты информации предусматриваются в коллективном договоре, который должен содержать следующие требования:

В разделе «Предмет договора».

Администрация предприятия (в том числе и администрация самостоятельных подразделений) ОБЯЗУЕТСЯ обеспечить разработку и осуществление мероприятий по определению и защите конфиденциальной информации.

Трудовой коллектив принимает на себя обязательства по соблюдению установленных на предприятии требований по защите конфиденциальной информации.

Администрация обязана учесть требования защиты конфиденциальной информации в правилах внутреннего распорядка.

В разделе «Кадры. Обеспечение дисциплины труда».

Администрация обязуется:

нарушителей требований по защите коммерческой тайны привлекать к административной и уголовной ответственности в соответствии с действующим законодательством.

В разделе «Порядок приема и увольнения рабочих и служащих».

при поступлении рабочего или служащего на работу или переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией предприятия, а также при увольнении администрация обязана проинструктировать работника или служащего по правилам сохранения коммерческой тайны с оформлением письменного обязательства о ее неразглашении;

администрация предприятия вправе принимать решение об отстранении от работ лиц, которые нарушают установленные требования по защите конфиденциальной информации.

В разделе «Основные обязанности рабочих и служащих».

Рабочие и служащие обязаны соблюдать требования нормативных документов по защите конфиденциальной информации предприятия.

В разделе «Основные обязанности администрации».

Администрация предприятия, руководители подразделений обязаны:

обеспечить строгое сохранение конфиденциальной информации, постоянно осуществлять организаторскую и воспитательно-профилактическую работу, направленную на защиту секретов предприятия;

включить в должностные инструкции и положения обязанности по сохранению конфиденциальной информации;

неуклонно выполнять требования устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других организационных и

хозяйственных документов по обеспечению экономической и информационной безопасности.
Обязательства конкретного сотрудника, рабочего или служащего по защите информации обязательно должны быть оговорены в трудовом договоре (контракте), при заключении которого трудящийся обязуется выполнять определенные требования, действующие на данном предприятии. Независимо от формы заключения договора (устного или письменного) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора.
Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, вытекающие из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспечения информационной безопасности.
Использование договоров о неразглашении тайны - вовсе не самостоятельная мера по ее защите. Не следует думать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по защите информации, и правовая основа к тому, чтобы пресечь его неверные или противоправные действия. Далее следует задача не допустить утраты коммерческих секретов.
Реализация правовых норм и актов, ориентированных на защиту информации на организационном уровне, опирается на те или иные организационно-правовые формы, к числу которых относятся соблюдение конфиденциальности работ и действий, договоры (соглашения) и различные формы обязательного права. Для понимания этих важных организационно-правовых форм приведем их определения.
Конфиденциальность – это форма обращения со сведениями, составляющими коммерческую тайну, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями.
Договоры – это соглашения сторон (двух и более лиц) об установлении, изменении или прекращении взаимных обязательств.
Обязательство – гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия.

1. 5 Лекция № 5 (2 часа).
Тема: «Подбор, расстановка и обучение сотрудников службы защиты информации»

1.5.1 Вопросы лекции:
1. Особенности подбора кадров
2. Социально-психологические факторы, влияющие на расстановку кадров
3.Специфика деятельности сотрудников службы защиты информации.
4. Распределение обязанностей между сотрудниками службы защиты информации
1.5.2 Краткое содержание вопросов:
1. Особенности подбора кадров
Эффективность управления в решающей степени зависит от качественного подбора и расстановки кадров руководителей и специалистов.
В современных условиях важное значение имеют не только высокие деловые качества, но и широта экономического мышления, предприимчивость, умение видеть перспективу развития предприятия, обладать необходимыми личными качествами.
Подбор кадров управления – это процесс их поиска и изучения с целью установления пригодности работников для выполнения обязанностей по определенной должности.

Отбор кадров управления – это выявление возможностей претендентов для определения их на соответствие условиям и особенностям работы.
Расстановка кадров управления предполагает обоснованное и экономически целесообразное распределение работников по структурным подразделениям и должностям в соответствии с требуемым уровнем и профилем подготовки, опытом работы, деловыми и личными качествами.
Таким образом, подбор, отбор и расстановка кадров решают две задачи: назначение на должность наиболее подходящих работников и нахождение для каждого из них наиболее соответствующей его данным сферы трудовой деятельности.
За подбор, отбор и расстановку кадров на предприятии ответственность несет его руководитель, а непосредственно осуществляет эти функции кадровая служба совместно с руководителями подразделений, для которых подбираются кадры.
Подбор, отбор и расстановка кадров состоят из ряда принципов:
1) Формирование требований к исполнителям по каждой должности
2) Сбор данных о возможных кандидатах
3) Оценка качеств кандидатов и составление характеристик по каждому из них
4) Сопоставление качеств кандидатов и требований к работнику
5) Сравнение данных различных кандидатов и выбор наиболее подходящего кандидата
6) Назначение кандидата на должность.
Определить требования к работникам – сложная задача, так как они должны касаться не только знаний и практических навыков, но и определенных способностей, особенностей мышления, черт характера, типа нервной высшей деятельности.
Требования к знаниям и навыкам изложены в квалификационном справочнике должностей служащих. А остальные требования определяются конкретно на предприятии.
Общих требований к специалистам, техническим исполнителям сформулировать невозможно, а к руководителям общие требования сформулированы:
1. Профессиональная компетентность в вопросах деятельности своего предприятия или подразделения и эрудиция по более широкому кругу вопросов, касающихся производства.
2. Высокие организаторские и деловые качества. Он должен быстро ориентироваться в обстановке, не бояться принимать ответственные решения, уметь настоять на своем, проявлять требовательность, быть энергичным и оперативным в действиях, видеть перспективу и определять главные звенья.
3. Знание основ психологии личности и социальной психологии.
4. Наличие высоких морально-этических качеств.
2. Социально-психологические факторы, влияющие на расстановку кадров
Под расстановкой персонала в организации понимается целесообразное распределение наличных работников по подразделениям и рабочим местам в соответствии с принятой в организации системой разделения и кооперации труда, с одной стороны, и способностями работников - с другой.
Расстановка персонала должна обеспечивать слаженную деятельность коллектива с учетом объема, характера и сложности выполняемых работ на основе соблюдения следующих условий:
равномерная и полная загрузка работников всех служб и подразделений;
использование персонала в соответствии с его профессией и квалификацией (конкретизация (функций исполнителей, с тем чтобы каждый рабочий ясно представлял круг своих обязанностей, хорошо знал, как выполнять порученную ему работу);
обеспечение необходимой взаимозаменяемости работников на основе овладения ими смежными профессиями;
обеспечение полной ответственности каждого за выполнение своей работы, т.е. точный учет ее количественных и качественных результатов. Закрепление за исполнителем работы, которая соответствует уровню его знаний и практических навыков.
При расстановке кадров необходимо соблюдение следующих принципов:

- соответствия;
- перспективности;
- сменяемости.

Принцип соответствия означает соответствие нравственных и деловых качеств претендентов требованиям замещаемых должностей.

Принцип перспективности основывается на учете следующих условий:

установление возрастного ценза для различных категорий должностей;

определение продолжительности периода работы в одной должности, на одном и том же участке работы;

возможность изменения профессии или специальности, организация систематического повышения квалификации; состояние здоровья.

Принцип сменяемости заключается в том, что лучшему использованию персонала должны способствовать внутриорганизационные трудовые перемещения, под которыми понимаются процессы изменения места работников в системе разделения труда, а также смены места приложения труда в рамках организации, так как застой (старение) кадров, связанный с длительным пребыванием в одной и той же должности, имеет негативные последствия для деятельности организации. Например, начальники цехов сами заявляют, что очень трудно работать в этой должности более б-7 лет на одном месте.

Расстановка персонала в организации прежде всего предполагает правильное распределение работников по категориям промышленно-производственного персонала (рабочие, ученики, ИТР, служащие, МОП). При этом следует добиваться наиболее оптимального соотношения между численностью данных категорий путем установления нормативов численности рабочих, ИТР и других категорий персонала. На базе научно обоснованных норм затрат труда решается в каждом конкретном случае, сколько требуется рабочих для выполнения того или иного объема работ.

Рациональная расстановка персонала подразумевает соблюдение определенных для данных условий пропорций по квалификации, социальной активности, возрасту, полу. В инструкциях по расстановке кадров должны быть зафиксированы также и социально-психологические аспекты совместимости сотрудников.

Все более характерным становится использование прогностических методов определения должностной пригодности претендента, построенных на основе гипотезы о его будущей деятельности. Вместе с тем успешно используются также и практические методы установления степени соответствия кандидата месту - отдельные поручения, временное замещение должности, стажировка и пр.

Расстановка персонала по рабочим местам (должностям) должна осуществляться не только в соответствии с количественными, качественными, временными и территориальными требованиями процесса производства, но и с учетом интересов и склонностей работников.

Социально-психологическая адаптация - приспособление работника к первичному трудовому коллективу, во взаимодействии с которым проходит его общественная и профессиональная деятельность,

3. Специфика деятельности сотрудников службы защиты информации

Служба безопасности предприятия выполняет следующие общие функции и задачи:

• организует и обеспечивает пропускной и внутри объектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;

• руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;

• участвует в разработке основополагающих документов с целью закрепления в них требований обеспечение безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений

о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
• разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организует и контролирует выполнение требований «ИНСТРУКЦИИ по защите коммерческой тайны";
• изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций о деятельности предприятия и его клиентов, партнеров, смежников;
• организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;
разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие
• нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
• обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;
• осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны;
• организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был глубоко осознанный подход;
• ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;
• ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
• поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).
4. Распределение обязанностей между сотрудниками службы защиты информации
Распределение обязанностей по обеспечению информационной безопасности состоит в четком определении обязанностей персонала по защите информации.
В соответствии с Политикой ИБ в организации должна быть разработана схема управления информационной безопасностью, определяющая подход к распределению и контролю выполнения обязанностей по реализации мер обеспечения информационной безопасности.
Схема управления ИБ описывает распределение соответствующих обязанностей между подразделениями и лицами, обеспечивающим создание и эксплуатацию СОИБ, высшим руководством организации, владельцами деловых процессов и информационных активов, руководителями подразделений и рядовыми сотрудниками организации.
В качестве «главного исполнителя» по обеспечению ИБ в зависимости от выбранной схемы или создаются отдельное подразделение/ штатная единица, отвечающие за обеспечение информационной безопасности, или функции обеспечения ИБ являются «дополнительной нагрузкой» для сотрудников организации, выполняющих другие функции. Или что-то среднее.
Согласно многим стандартам ИБ подразделение или сотрудник, ответственные за ИБ, должны соответствовать следующим принципам:

самостоятельность в рамках полномочий – наделение ответственных за ИБ правами определять, планировать, реализовывать и контролировать те средства управления, что им поручены, используя те ресурсы, что им для этих задач выделены;
независимость от тех, чьи процессы находятся под контролем – ответственный за ИБ не должен быть подчиненным того, кто также управляет процессами, являющимися предметом контроля со стороны ИБ – это прямой конфликт интересов; в идеале, службы ИБ и ИТ должны иметь разных кураторов в высшем руководстве организации;
невмешательство в ход деловых процессов – сотрудник ИБ не должен иметь возможность самостоятельно совершать или прекращать тот или иной деловой процесс или операцию, дабы не являться самим источником таких же рисков, как и те источники, что находятся под его контролем;
находится под контролем независимых средств – сотрудник ИБ не должен обладать привилегированными правами в системе обеспечения ИБ, любые его критические действия должны контролироваться (например, подтверждаться) независимыми службами, например ИТ, деятельность самой службы должна быть включена в область мониторинга системы внутреннего контроля организации.
Рассмотрим варианты организации «главного исполнителя» по ИБ.
Отдельное подразделение – служба информационной безопасности (СИБ). Как правило, СИБ является подразделением службы экономической безопасности. Не зависит от руководителя ИТ. Имеет возможность осуществлять независимый мониторинг и управление средствами обеспечения ИБ. Обычно ИТ передает им все контрольные функции ИБ, оставляя за собой только исполнение. Если таких функций много, а подразделение небольшое (например – один человек), то возможны проблемы с взаимозаменяемостью сотрудников, поэтому при создании СИБ в такой конфигурации надо озаботиться обучением и распределением обязанностей.
Сотрудник ИТ, ответственный за информационную безопасность. Подчиняется, а значит зависим от руководителя ИТ. Попытка реализовать вариант «двойного подчинения» является вариантом «засланного казачка» или «своего человека в Гаване», что вносит сумятицу и дисбаланс в работу, поэтому лучше даже не пробовать его реализовывать. Функции управления ИБ ограничены исключительно «необходимым минимумом». В основном, сотрудников, которые могут выполнять эти функции, несколько, они частично взаимозаменяемы. Как правило, является переходным вариантом от следующего варианта к предыдущему (для растущей организации) или «стабильным середняком» (по оценкам зрелости процессов), но действующим вариантом обеспечения СОИБ для средней или небольшой организации.
Сотрудник ИТ, «нагруженный» дополнительно функциями ИБ. Самый слабый вариант, но часто единственный в небольших организациях, стоящих на самой начальной фазе создания СОИБ или имеющих очень ограниченный бюджет. Его основные функции естественно превалируют над «дополнительными». Практически, не взаимозаменяем. Очень часто в качестве его «заместителя» выступает начальник ИТ. Естественно, говорить о независимости, взаимном мониторинге и т.п. очень сложно. Оценки при аудите ИБ в основном невысокие. Реализовать взаимный контроль в технологических процессах обеспечения ИБ не просто, но можно. При этом, такой сотрудник может провести анализ существующей системы и выработать предложения по созданию СОИБ, чем «подготовить почву» для перехода к ее более «активной» конфигурации.
В любом случае хорошей практикой при развитии СОИБ считается определение функциональных ролей (в виде набора необходимых действий, а также прав, необходимых для их исполнения) для выполнения тех или иных функции обеспечения информационной безопасности. Примером таких ролей могут быть:

- администратор безопасности системы управления предприятием или автоматизированной банковской системы (АБС);
- администратор антивирусной защиты;

- администратор сетевой системы;
- оператор системы резервного копирования;
- оператор системы мониторинга системы обеспечения ИБ;
- и т.п.

Выполнение определенной функциональной роли требует от ее исполнителя определенных (и достаточно конкретных знаний), он должен быть наделен соответствующими правами.

Одним из основных принципов как создания роли, так и назначения исполнителей ролей является правило, что никакая роль и никакой исполнитель ролей не должен в совокупности предоставленных прав обладать возможностью совершить действия, критические для деятельности организации. По крайней мере – бесконтрольно. Например, администратор АБС может зарегистрировать пользователя, но присвоением пользователю профиля доступа (т.е. прав на функции и данные в информационной системе) занимается администратор безопасности АБС и т.п. Один сотрудник, в принципе, может отвечать за выполнение нескольких ролей, если этого требуют обстоятельства и это не нарушает обозначенный и другие принципы информационной безопасности.

После анализа имеющихся ресурсов и проведения при необходимости их (пере-)подготовки назначаются конкретные исполнители функциональных ролей, например – в виде матрицы «роль-исполнитель», с определение в ее ячейках основных и дублирующих исполнителей. Полноценно назначенной и выполняемой ролью можно считать только ту, по которой есть как минимум одио основной и один дублирующий исполнитель.

Ролевой подход обладает большой гибкостью в управлении исполнением функций. В нем управление идет не от конкретного человека и его текущих знаний, а от необходимых для выполнения функций знаний и прав и «подтягивания» к ним исполнителя.

В правильно организованной системе управления у каждого делового процесса и/или информационной системы есть владелец, т.е. (согласно определениям Стандарта 27001) «лицо или организация (подразделение), имеющие утвержденные руководством обязательства по контролю за производством, разработкой, поддержкой, использованием и безопасностью активов». Т.е., в том числе, отвечает за обеспечение информационной безопасности.

Лица, являющиеся ответственными за обеспечение ИБ (в частности, владельцы информационных активов) могут передавать задания по выполнению конкретных действий другим, но, тем не менее, они все равно остаются ответственными, в том числе, и за приемку результатов задания.

При распределении обязанностей должны быть выполнено следующее:

- идентифицированы все информационные активы и процессы защиты, связанные с каждой информационной системой;
- определены и документально назначены владельцы активов, ответственные за актив или процесс обеспечения ИБ;
- уровни полномочий четко определены и закреплены документально.

Как уже отмечалось выше, сотрудник службы информационной безопасности не должен быть исполнителем в процедурах настройки технических средств, участвующих в деловых процессах. Его задача – контроль процессов и формирование «управляющих заданий» для исполнителей.

1. 6 Лекция № 6 (2 часа).

Тема: «Структура и содержание должностных инструкций сотрудников службы защиты информации»

1.6.1 Вопросы лекции:

1.Организация рабочих мест сотрудников службы защиты информации (рациональное размещение, оснащение оборудованием, техническими средствами).

2. Обеспечение необходимых условий труда
1.6.2 Краткое содержание вопросов:
1 Организация рабочих мест сотрудников службы защиты информации (рациональное размещение, оснащение оборудованием, техническими средствами).
Организация трудового процесса включает: разработку технологии выполнения работ, рациональное размещение рабочих мест сотрудников, установление правильного режима труда и отдыха, обеспечение техники безопасности.
Технология выполнения работ складывается из описания содержания работ в последовательности их выполнения. Она может закрепляться в инструкции по конфиденциальному делопроизводству, технологических картах, картах организации трудового процесса или других документах.
Рациональное размещение рабочих мест сотрудников предполагает соответствие технологии выполнения работ, последовательности происхождения документов, взаимосвязям между сотрудниками. Оно должно способствовать и обеспечению персональной ответственности за сохранность документов.
Правильный режим труда и отдыха требует рационального распределения нагрузки в течение рабочего дня, чередования труда и отдыха, проведения, при необходимости, психофизической разгрузки.
Установление и поддержание здорового микроклимата в коллективе также способствует повышению производительности труда и сохранению здоровья сотрудников.
Микроклимат зависит не только от взаимоотношений сотрудников, но и от отношения руководителя к сотрудникам Непредвзятость со стороны руководителя, равномерная загрузка сотрудников, оказание им помощи, внимание к их бытовым проблемам, своевременное устранение конфликтных ситуаций создают благоприятную почву для хорошего настроения сотрудников и нормальных, доброжелательных взаимоотношений.
Каждый сотрудник подразделения конфиденциального делопроизводства должен быть обеспечен нормативно-методическими документами регулирующими процесс его деятельности и технологию выполнения работ. К ним относятся нормативные документ по защите информации, а также методическая литература: книги, брошюры, журналы, которые позволяют найти ответы на вопросы, не отраженные в нормативных документах.
На рабочих местах следует иметь и необходимые справочники, включая телефонные.
Система защиты информации — это комплекс организационных и технических мер, направленных на обеспечение информационной безопасности предприятия. Главным объектом защиты являются данные, которые обрабатываются в автоматизированной системе управления и задействованы при выполнении бизнес-процессов.
Основные угрозы для информационной безопасности любой компании связаны с кражей данных (например, промышленный шпионаж), использованием непроверенного программного обеспечения (например, содержащего вирусы), хакерскими атаками, получением спама (также может содержать вирусы), халатностью сотрудников. Реже утрата данных вызвана такими причинами, как сбой в работе аппаратно-программного обеспечения или кража оборудования. В результате компании несут значительные потери.
Процесс создания системы защиты информации можно разделить на три этапа:
- формирование политики предприятия в области информационной безопасности;
- выбор и внедрение технических и программных средств защиты;
- разработка и проведение ряда организационных мероприятий.

2. Обеспечение необходимых условий труда.
Человек значительную часть своей жизни тратит на труд и потому от условий труда, уровня ее безопасности, зависит работоспособность и производительность труда, качество работы, состояние здоровья. По данным Всемирной организации здравоохранения на состояние здоровья нации на 50 процентов влияют социальные факторы (условия жизни, условия труда).

Благоприятные условия обеспечивают как социальную гармонию лица человека, так и отношение ее, к труду и удовлетворение трудом. Актуальность вопроса улучшения условий труда обусловливается и тем, что уровень образования работников выдвигает на первое место необходимость удовлетворения потребностей в содержательном труде в опасных условиях. Поэтому создание благоприятных условий труда должно быть одним из главных заданий общества, неотъемлемой частью государственной социальной и экономической политики, важной составляющей менеджмента персонала.

На государственных предприятиях трудовым коллективам предоставлены большие полномочия относительно улучшения условий труда. Они имеют право принимать участие в обсуждении и утвержденные комплексных планов инженерный – технических мероприятий по достижению установленных нормативов безопасности, гигиены труда и производственной среды; контролировать использование средств на выполнение планов, ставить вопрос о привлечении к ответственности за нарушение норм из охраны труда и тому подобное.

В условиях развития рыночных отношений улучшению условий труда способствует и необходимость использовать в конкурентной борьбе новейшие технологии, которые базируются на достижениях научно-технического прогресса, стремления достичь снижения расходов на производство продукции и соответствующего роста прибыли на предприятиях, будь, – какой формы собственности.

Условия труда разделяются на социально экономические, которые рассматриваются в широком контексте и характеризуют отношение к ним общества, и производственные, то есть условия труда непосредственно на рабочих местах.

ГОСТ 19605 – 74 “Организация труда. Основные понятия, сроки и определения”, трактует условия труда как “совокупность факторов производственной среды, которые влияют на здоровье та работоспособность человека в процессе труда”.

Гигиеническая классификация труда определяет условия труда как совокупность факторов трудовой и производственной среды, в которой осуществляется деятельность человека.

На формирование условий труда влияют факторы, которые разделяются на три группы.

- Первая группа - социально-экономические факторы, действие которых обусловливает характер условий труда. Среди них выделяются подгруппы:
- нормативно правовые (законы, нормы, стандарты а также формы административного и общественного контроля, за их выполнением);
- экономические (материальное и экономическое стимулирование, моральное поощрение, система льгот и компенсаций, за неблагоприятные условия труда);)
- социально психологические (отношение работников к труду, психологический климат);
- общественно-политические (формы движения работников за создание благоприятных условий, изобретательство и рационализация).

Вторая группа - технико-организационные факторы. Они влияют на формирование условий труда на рабочих местах, участках, цехах. Среди них выделяются такие подгруппы:

- предметы труда и их продукты (сырье, материалы, готовые изделия);
- технологические процессы;
- средства труда;

организационные формы производства, труда и управления.

Третья группа – естественные факторы, действие которых не только обусловливается особенностями естественной среды, но и выдвигает дополнительные требования к оборудованию, технологии, организации производства и труду. Среди них выделяются такие подгруппы:

- географические (климатические зоны);

- биологические (особенности растительного и животного мира в сельском хозяйстве);
- геологические (характер добывания полезных ископаемых).

Все эти факторы выливают на формирование условий труда одновременно и в неразрывном единстве, обусловливая рядом с другими параметрами производственную среду.

Классификация факторов помогает на уровне отрасли, объединения, отдельного производства:

формировать и улучшать условия труда, анализировать их состояние;

планировать мероприятия по улучшению условий труда;

разрабатывать проекты оборудования, сооружений, технологических процессов, направленных на улучшение условий труда;

сосредоточивать ресурсы (финансовые, материальные, трудовые) на улучшение условий труда;

прогнозировать изменения в условиях труда в связи с изменениями технологии, оборудования, внедрения новых материалов и технологий.

Свое влияние на человека система факторов влечет опосредствовано через совокупность системы элементов, которые непосредственно определяют условия труда на рабочих местах.

Выделяются такие элементы условий труда: санитарно-гигиенические, что характеризуют производственную среду, на которую влияют предметы и средства труда, а также технологические процессы (промышленный шум, вибрация, токсичные вещества, промышленная пыль, температура воздуха и другие).

Все они количественно оцениваются с помощью методов санитарно-гигиенических исследований и нормируются путем установления стандартов, санитарных норм и требований.

Психофизиологические элементы обусловлены содержанием труда и ее организацией (физическая нагрузка, нервно – психологическое напряжение, монотонность трудового процесса и тому подобное). Элементы этой группы, за исключением физических усилий и монотонности, не имеют утвержденных нормативов.

Эстетичные элементы способствуют формированию позитивных эмоций у работника (художественно конструктивное решение рабочего места, освещения, функциональная музыка и тому подобное).

Количественных оценок элементы этой группы не имеют. Определение эстетичного уровня условий труда осуществляется с помощью методов экспертного оценивания.

Социально психологические элементы характеризуют взаимоотношения в трудовом коллективе, создавая соответствующее психологическое настроение работающих (социальный климат).

Они не имеют единиц измерения, норм и стандартов. Но социологические исследования в виде устного опроса, анкетирования, способствуют их объективному оцениванию.

Технические элементы определяются уровнем механизации труда.

Труд, а соответственно условия и охрана труда, является реалиями разных систем, с одной стороны, ”человек – машина(технологический процесс)”, “человек – производственная среда”, “человек – машина (технологический процесс) – производственная среда”, а из другого “человек - коллектив – общество”, - “человек – общество - природа”.

Для первых трех систем условия труда рассматриваются в пределах рабочего места, участка, цеха, производства, а для последних двух – в пределах предприятия, отрасли, региона.

Обеспечение необходимых условий трудовой деятельности осуществляется за тремя направлениями;

формирование благоприятных условий труда, обогащения ее содержания;

улучшение условий труда в связи с наличием неблагоприятных факторов или растущими потребностями общества, а при невозможности улучшения условий труда поддержания их на достигнутом уровне;
защита работников от имеющихся и возможных опасностей, то есть охрана труда.
Наиболее эффективными являются мероприятия, направленные на формирование благоприятных условий, на новых предприятиях или в порядке реконструкции на действующих.
Для большинства предприятий характерным является планомерное улучшение условий труда и защита работников от опасных и вредных производственных факторов.

1. 7 Лекция № 7 (2 часа).
Тема: «Принципы управления службой защиты информации»

1.7.1 Вопросы лекции:
1. Понятие и сущность методов управления
2. Система методов управления. Административно-правовые методы управления. Экономические методы управления. Социально-психологические методы управления
3. Взаимосвязь методов управления
4. Технология управления службой защиты информации
1.7.2 Краткое содержание вопросов:
1. Понятие и сущность методов управления
Методы управления — это совокупность приемов и способов воздействия на управляемый объект для достижения поставленных организацией целей.
Через методы управления реализуется основное содержание управленческой деятельности.
В практике управления, как правило, одновременно применяют различные методы и их сочетания. Существует 3 вида методов управления:
1) Метод командный. Используемые механизмы: Административные: приказ, распоряжение, указание. Нормативные: закон, положение, инструкция, план, спущенный сверху и обязательный для выполнения. Экономические: процент выплачиваемой прибыли, цена продукта (назначенная), зарплата (назначенная), материальные санкции, установленные сверху. Социально-психологические: выговор, объявленный в приказе, награждение грамотой по распоряжению руководства, благодарность в приказе, план социального развития коллектива и мероприятий по его реализации.
При командном методе управления - отношения субъекта и объекта - власти и подчинения. Основные достоинства метода: 1)обеспечивается единство воли руководства в достижении цели; 2)не требует крупных материальных затрат; 3)в малых организациях оперативно достигаются цели и обеспечивается быстрая реакция на изменение внешней среды. Недостатки метода следующие: 1)подавляется инициатива, творческая работа; 2)отсутствуют действенные стимулы труда и могут возникать антистимулы; 3)в крупных организациях: а)менеджеры не заинтересованы в повышении компетентности, поэтому она в дефиците; б)обюрокрачивается аппарат управления; в)требуется громоздкая система контроля.
2) Метод экономический. Механизмы: договорной процент отчисляемой прибыли, договорная цена продукта, договорная зарплата, материальные санкции, предусмотренные договором.
Экономические методы управления - отношения субъекта и объекта - договорные - товарно-денежные. Характеризуются: 1)свободой субъекта и объекта, достаточной для реализации их интересов в договорном процессе; 2)выполнение договорных обязательств. Достоинства метода: стимулируется проявление инициативы, реализуется творческий потенциал работников на основе удовлетворения материальных потребностей.

Недостатки: остаются неудовлетворенными многие потребности, лежащие вне сферы материального интереса, что снижает мотивацию.
3) Социально-психологический метод. Механизмы также договорные: убеждение, критика, информирование, выступление руководителя перед людьми. Социально-психологические методы - управленческие отношения субъекта и объекта договорные без материальной основы. Условия реализации: одна из сторон инициирует договорной процесс, вторая не отвергает его. Достоинства метода: 1)включаются механизмы трудовой мотивации, не связанные с удовлетворением материальных потребностей; 2)практически не требуются материальные затраты. Недостатки: 1)не используются стимулы, опирающиеся на материальные потребности людей; 2)трудно прогнозировать результаты.
2. Система методов управления. Административно-правовые методы управления. Экономические методы управления. Социально-психологические методы управления
Административно-правовые методы — это способы реализации задач и функций исполнительной власти, средства непосредственного воздейст-вия органов исполнительной власти на управляемые объекты (отрасли, сферы, органы управления различных организаций, коллективы работ-ников, граждан). Эти методы показывают, как, каким образом государ-ство решает задачи в области управления. Для методов управления характерно то, что они используются органами исполнительной власти для решения стоящих перед ними конкретных задач; применяются по-вседневно и выборочно; обнаруживаются во взаимодействии субъекта и объекта управления; выражают компетенцию органов исполнитель-ной власти по принятию правовых актов, а также осуществлению иных государственно-властных полномочий. Отсюда следует немаловажный вывод о том, что методы управления производны от политического режима государства.
Методы целенаправленного управленческого воздействия органов исполнительной власти (должностных лиц) на свои объекты весьма разнообразны, так как не только субъекты, но и объекты управления имеют свои особенности, касающиеся их назначения, организацион-но-правового статуса. В сфере исполнительной власти имеются раз-личные группы общественных отношений, требующих различного подхода для их урегулирования с учетом формы собственности, ведом-ственной принадлежности и т.д. Ясно, что например, по отношению к государственным предприятиям применяются иные методы управле-ния, чем к негосударственным.
Методы воздействия, как и формы реализации исполнительной власти, закрепляются в правовых актах управления. Например, в по-становлении Правительства обычно указываются цель его издания и конкретные способы (приемы) внешнего воздействия на объект управ-ления, чтобы достичь поставленной цели. При этом могут быть указаны конкретные виды контроля, учета, проверок, оформляемых докумен-тов, материального и морального стимулирования, меры администра-тивного принуждения и т.д.
Среди разнообразных методов, используемых в процессе реализа-ции исполнительной власти, выделяют прежде всего методы убежде-ния и принуждения, которые применяются в любом виде государствен-ной и общественной деятельности.
Метод убеждения должен быть основным методом деятельности ор-ганов исполнительной власти, что предполагает систематическую ра-боту по убеждению масс, формированию общественного сознания в необходимости должного поведения участников управленческих об-щественных отношений, строгого соблюдения ими установленных го-сударством правил. Разъяснение целей государства, проектов законов, правительственных программ, проводимых властью мероприятий и т.п. необходимо потому, что они затрагивают интересы большинства граждан и должны быть им понятны. Убеждение выступает и как сред-ство профилактики правонарушений и укрепления государственной дисциплины. Среди мер убеждения — разъяснение, обоснование, об-суждение, внушение, поощрение, показ положительных объектов уп-равления и

многое другое, описываемое и реализуемое в понятиях и процедурах социальной психологии и педагогики.

Стремительное качественное изменение нашего общества, станов-ление рыночной экономики, движение к демократии и правовому го-сударству выдвигают на первый план решение масштабнейшей зада-чи — формирование в России единого информационно-правового пространства, обеспечивающего правовую информированность всех структур общества и граждан. Это — основная цель Указа Президента от 28 июня 1993 г. «О концепции правовой информатизации России»*. Указом Президента от 29 марта 1994 г. объявлена Программа взаимо-действия федеральных органов государственной власти Российской Федерации в области информационно-правового сотрудничества с ор-ганами власти СНГ**.

По характеру воздействия (прямой или косвенный) на сознание и волю людей различаются экономические и административные методы.

Экономические — это методы косвенного воздействия на объект управления. Чаще всего используются такие экономические рычаги, как цены, налоги, проценты, премии, имущественные льготы, эко-номические санкции и др. С их помощью орган исполнительной власти (должностное лицо) достигает желаемого поведения объекта управления, воздействуя на его материальные (имущественные) ин-тересы. Поэтому они и именуются экономическими методами управ-ления.

К административным относятся методы прямого или внеэкономи-ческого воздействия со стороны субъектов управления на сознательно-волевое поведение управляемых. Наименование этих методов опреде-ляется тем, что они наиболее характерны для органов исполнительной власти. Орган исполнительной власти (должностное лицо) в пределах своей компетенции принимает управленческое решение (правовой акт управления), юридически обязательное для объекта управления. Кон-кретное содержание административно-правовых методов весьма раз-нообразно: предписание об обязательном совершении определенных действий; ограничение или запрещение совершения определенных действий; разрешение споров между участниками управленческих от-ношений; применение иных методов, направленных на быстрое и эф-фективное решение проблем, возникающих при осуществлении госу-дарственно-управленческой деятельности.

Экономические и административные методы управления, несмотря на их различия, взаимосвязаны, и их противопоставление недопусти-мо, так как они используются с единой конечной целью — реализация управляющего воздействия субъекта на объект управления. С учетом расширения оперативной самостоятельности государственных пред-приятий, их разгосударствления на первый план выдвигается задача разумного сочетания средств управляющего воздействия.

В условиях прежней директивно-плановой экономики методы ад-министративного воздействия были основными. По мере продвиже-ния России к рыночной экономике все более широкое применение приобретают экономические методы. Но неверны представления, согласно которым в рыночной экономике обязательные предписания органов исполнительной власти вообще неуместны. Рыночная эко-номика вовсе не должна быть стихией, никак не регулируемой госу-дарством, — должны быть изменены формы и методы такого регули-рования. Хотя основным методом и становится реализация творчес-кой инициативы и самостоятельности управляемых, это не исключает применения и метода обязательных предписаний. Например, в Указе Президента от 28 февраля 1995 г. «О мерах по упорядочению государ-ственного регулирования цен (тарифов)»* содержится предписание о допущении государственного регулирования цен (тарифов) на про-дукцию естественных монополий. О повышении роли государства в регулировании рыночной экономики свидетельствуют также норма-тивные правовые акты, принятые в последние годы, например, по вопросам лицензирования деятельности физических и юридических лиц, управления федеральной собственностью, стабилизации

потре-бительского рынка, совершенствования государственной ценовой (та-рифной) политики.
Поскольку участниками процесса управления являются люди, то социальные отношения и отражающие их соответствующие методы управления важны и тесно связаны с другими методами управления.
К ним относятся:
- моральное поощрение,
- социальное планирование,
- убеждение,
- внушение,
- личный пример,
- регулирование межличностных и межгрупповых отношений,
- создание и поддержание морального климата в коллективе.

3. Взаимосвязь методов управления

Эффективное управление возможно лишь на основе сочетания, единстве всех трех групп методов: экономических, административных и социально-психологических, так как применение экономических методов становится успешным тогда, когда умело поставлена организаторская, административная деятельность, обеспечивающая создание четкого распорядка работы, установление ответственности каждого исполнителя за возложенные на него обязанности. Там, где есть уважение к дисциплине, там эффективнее действуют и экономические методы. Нормальное функционирование экономического управления настоятельно требует, чтобы все виды административного воздействия были строго регламентированы и введены в правовые рамки. Речь идет о необходимости разработки административного кодекса — своеобразного дисциплинарного устава. Экономическое управление требует ясности и полноты не только в чисто экономической, но и во всех других областях деятельности предприятия. Экономические и административные методы управления неразрывны, образуют единую систему рычагов, направляющих предприятие к его конечной цели, позволяющих прийти к ней кратчайшим и наиболее экономным путем. К сожалению, этих двух методов оказывается недостаточно. На пути их реализации появляется весьма серьезное препятствие. К примеру, созданы экономические стимулы и проведены соответствующие административные мероприятия, но это не означает, что предприятие станет успешно решать свои задачи. Все это произойдет, если не будет учтен главный элемент производства — человек. Тут нужны методы особого рода.
В свою очередь административные методы связаны с социально-психологическими. Исходя из принципа единоначалия, руководитель имеет право издавать приказы и распоряжения. Но должен учитывать в каждый момент общее состояние «социально-психологического» климата, а также индивидуальные способности каждого исполнителя, от которых во многом зависит успешность выполнения издаваемого приказа или распоряжения.
Опыт работ по управлению персоналом показал, что роль социально-психологических методов постоянно возрастает. Это обусловлено тремя моментами:
а) повышением образовательного и культурного уровня работников, что вызывает с их стороны ожидание в применении методов управления их деятельностью, основанных на учете интересов их и коллективов, в которых они работают, методов, которые не подавляют их как личность, вызывают рост их творческой активности;
б) развитием демократических начал в управлении;
в) значительная часть коллективов является не только наемными работниками, но и акционерами предприятия, что вызывает необходимость некоторого насыщения организационных (административно-правовых) и экономических методов — методами социально-психологического воздействия. Речь идет не об усилении одного метода за счет ослабления другого, а о подкреплении одного метода другим. Это означает, например, что

экономические методы, связанные с разработкой систем материального стимулирования труда работников, должны максимально учитывать социально-психологические факторы, которые сложились в коллективе.
В практике управления, как правило, одновременно применяют различные методы и их комбинации. Для эффективного управления необходимо использовать в управлении предприятием все три группы методов. Так, использование только властных и материальных методов не позволяет мобилизовать творческую активность персонала на достижение целей организации. Для достижения максимальной эффективности необходимо применение духовных методов.
Отмечаемый рядом авторов рост роли экономических методов управления в России связан прежде всего с формированием и совершенствованием рыночной экономической системы. В условиях рынка экономические методы управления неизбежно получат дальнейшее развитие, повысятся действенность и результативность экономических стимулов, что позволит поставить каждого работника и коллектив в такие экономические условия, при которых появится возможность наиболее полно сочетать личные интересы с рабочими целями. Однако акцентирование внимания на экономических методах стимулирования зачастую приводит к снижению внимания к социально-психологическим аспектам, определяющим внутреннюю мотивацию персонала.
В современном менеджменте применяются и иные группировки методов стимулирования. Укрупненно все методы стимулирования можно также сгруппировать в следующие четыре вида:
1. Экономические стимулы всех типов (зарплата во всех ее разновидностях, включая контрактную, премии, льготы, страховки, беспроцентные кредиты и т.п.).
Успешность их воздействия определяется тем, насколько коллектив понимает принципы системы, признает их справедливыми, в какой мере соблюдается неотвратимость поощрения (наказания) и результатов работы, их тесная связь во времени.
2. Управление по целям. Эта система широко используется в США и предусматривает установление для личности или группы цепи целей, способствующих решению главной задачи организации (достижение определенных количественных или качественных уровней, повышение квалификации персонала и т.п.). Достижение каждой цели автоматически означает повышение уровня зарплаты или другую форму поощрения.
3. Обогащение труда — эта система в большей степени относится к неэкономическим методам и означает предоставление людям более содержательной, перспективной работы, значительной самостоятельности в определении режима труда, использовании ресурсов. Во многих случаях к этому добавляется и рост оплаты труда, не говоря уже о социальном статусе.
4. Система участия в настоящее время существует в многообразных формах: от широкого привлечения коллектива к принятию решений по важнейшим проблемам производства и управления (Япония) до соучастия в собственности путем приобретения акций собственного предприятия на льготных условиях (США, Англия).
Лишь совместное, взаимосвязанное применение методов способно сделать труд рациональным и привлекательным, а его результаты — эффективными, полезными обществу и каждому из нас. В центре этих методов, как уже отмечалось, экономические и социально-психологические методы.
4. Технология управления службой защиты информации
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.
Необходимость комплексного и системного применения методов управления службой защиты информации

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;
- сохранение и 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.
Выделяются следующие типы стратегий безопасности:
1) ориентированные на устранение существующих или предотвращение возникновения возможных угроз;
2) нацеленные на предотвращение воздействия существующих или возможных угроз на предмет безопасности;
3) 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.
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 компетенции). Другую часть субъектов этой группы условно можно назвать полу специализированной, 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.

1. 8 Лекция № 8 (2 часа).
Тема: «Значение управленческих решений»

1.8.1 Вопросы лекции:
1. Цели планирования. Виды планирования, их назначение
2. Содержание и структура планов
3. Критерии эффективности службы защиты информации. Методы оценки качества службы защиты информации
1.8.2 Краткое содержание вопросов:

1. Цели планирования. Виды планирования, их назначение

Планирование - это определение системы целей функционирования и развития организации, а также путей и средств их достижения. Любая организация не может обходиться без планирования, так как необходимо принимать управленческие решения относительно:

- распределения ресурсов;
- координации деятельности между отдельными подразделениями;
- координации с внешней средой (рынком);
- создания эффективной внутренней структуры;
- контроля за деятельностью;

- развития организации в будущем. Планирование обеспечивает своевременность решений, позволяет избегать поспешности в решениях, устанавливает четкую цель и ясный способ ее реализации, а также даст возможность контролировать ситуацию.

В общем, в процессе планирования можно выделить:

- процесс целеполагания (определение системы целей);
- процесс сочетания (координации) целей и средств их достижения;
- процесс развития или единство существующей системы работы организации с ее будущим развитием.

Целеполагание - это процесс разработки системы целей, начиная от общих целей организации и заканчивая целями отдельных ее подразделений. В результате получается дерево целей, которое лежит в основе всего процесса планирования.

Само по себе наличие цели еще не означает, что она будет достигнута, необходимо наличие соответствующих материальных, финансовых и людских ресурсов. При этом часто от количества этих ресурсов зависит уровень достижения цели. Так, например, для создания предприятия в определенной отрасли необходимы первоначальные вложения не менее № млн рублей. Этот финансовый ресурс обязательно должен быть в наличии, и тогда будет обеспечено сочетание цели и средства ее достижения. Как результат координации появляются планы, в которых сочетаются мероприятия по достижению целей, сроки, средства и исполнители.

Для реализации процесса планирования также необходимо иметь налаженную организационную систему. Работа организации направлена на достижение планового показателя, и от того, как построена и скоординирована эта работа, зависит результат. Даже самые идеальные планы не будут реализованы без соответствующей организации. Должна существовать исполнительская структура. Кроме того, у организации должна существовать возможность будущего развития, так как без этого организация будет разрушаться (если мы не развиваемся, значит, мы умираем). Будущее организации зависит от условий среды, в которой она работает, от навыков и знаний персонала, от того места, которое организация занимает в отрасли (регионе, стране).

Весь процесс планирования в организации разделяется на два уровня: стратегический и оперативный. Стратегическое планирование - это определение целей и процедур организации в долгосрочной перспективе, оперативное планирование - это система управления организацией на текущий период времени. Эти два вида планирования соединяют организацию в целом с каждым конкретным подразделением и являются залогом успешной координации действий. Если брать организацию в целом, то планирование осуществляется в следующем порядке:

1. Разрабатывается миссия организации.
2. Исходя из миссии, разрабатываются стратегические ориентиры или направления деятельности (эти ориентиры часто называют качественными целями).
3. Производится оценка и анализ внешней и внутренней среды организации.
4. Определяются стратегические альтернативы.
5. Выбор конкретной стратегии или пути достижения цели. Ответ на вопрос "что делать?".
6. После установления цели и выбора альтернативных путей ее достижения (стратегии) основными компонентами формального планирования являются:

- тактика, или как добиться того или иного результата (ответ на вопрос "как делать?"). Тактические планы разрабатываются на основе выбранной стратегии, они рассчитаны на более короткий период времени (текущий момент), разрабатываются менеджерами среднего звена, результат такого планирования появляется быстро, и его легко соотнести с конкретными действиями работников;
- политика, или обще руководство для действий и принятия решений, которое облегчает достижение целей;
- процедуры, или описание действий, которые следует предпринимать в конкретной ситуации;
- правила, или что должно быть сделано в каждой конкретной ситуации.

Существует несколько методов планирования: балансовый, расчетно-аналитический, экономико-математические, графоаналитический и программно-целевые (рис. 2). Балансовый метод планирования обеспечивает установление связей между потребностями в ресурсах и источниками их покрытия, а также между разделами плана. Например, балансовый метод увязывает производственную программу с производственной мощностью предприятия, трудоемкость производственной программы — с численностью работающих. На предприятии составляются балансы производственной мощности, рабочего времени, материальный, энергетический, финансовый и др.

Расчетно-аналитическии метод используется для расчета показателей плана, анализа их динамики и факторов, обеспечивающих необходимый количественный уровень. В рамках этого метода определяется базисный уровень основных показателей плана и их изменения в плановом периоде за счет количественного влияния основных факторов, рассчитываются индексы изменения плановых показателей по сравнению с базисным уровнем.

Экономико-математические методы позволяют разработать экономические модели зависимости показателей на основе выявления изменения их количественных параметров по сравнению с основными факторами, подготовить несколько вариантов плана и выбрать оптимальный.

Графоаналитический метод дает возможность представить результаты экономического анализа графическими средствами. С помощью графиков выявляется количественная зависимость между сопряженными показателями, например, между темпами изменения фондоотдачи, фондовооруженности и производительности труда. Сетевой метод является разновидностью графоаналитического. С помощью сетевых графиков моделируется параллельное выполнение работ в пространстве и времени по сложным объектам (например, реконструкция цеха, разработка и освоение новой техники и др.).

Программно-целевые методы позволяют составлять план в виде программы, т. е. комплекса задач и мероприятий, объединенных одной целью и приуроченных к определенным срокам. Характерная черта программы — ее нацеленность на достижение конечных результатов. Стержнем программы является генеральная цель, конкретизируемая в ряде подцелей и задач. Цели достигаются конкретными исполнителями, которые наделяются необходимыми ресурсами. На основе ранжирования целей (генеральная цель — стратегические и тактические цели — программы работ) составляется граф типа «дерево целей» — исходная база для формирования системы показателей программы и организационной структуры управления ею.

По срокам различают следующие виды планирования: перспективное, текущее и оперативно-производственное (рис. 3). Перспективное планирование основывается на прогнозировании. С его помощью прогнозируются перспективная потребность в новых видах продукции, товарная и сбытовая стратегия предприятия но различным рынкам сбыта и т. д. Перспективное планирование традиционно подразделяется на долгосрочное (10-15 лет) и среднесрочное (3-5 лет) планирование.

Долгосрочный план имеет программно-целевой характер. В нем формулируется экономическая стратегия деятельности предприятия на длительный период с учетом расширения границ действующих рынков сбыта и освоения новых. Число показателей в плане ограниченно. Цели и задачи перспективного долгосрочного плана конкретизируются в среднесрочном плане. Объектами среднесрочного планирования являются организационная структура, производственные мощности, капитальные вложения, потребности в финансовых средствах, исследования и разработки, доля рынка и т. п. В настоящее время сроки исполнения (разработки) планов не имеют обязательного характера, и ряд предприятий разрабатывают долгосрочные планы сроком на 5 лет, среднесрочные — на 2-3 года.

Текущее (годовое) планирование разрабатывается в разрезе среднесрочного плана и уточняет его показатели. Структура и показатели годового планирования различаются в зависимости от объекта и подразделяются на заводские, цеховые и бригадные.

Оперативно-производственное планирование уточняет задания текущего годового плана на более короткие отрезки времени (месяц, декада, смена, час) и по отдельным производственным подразделениям (цех, участок, бригада, рабочее место). Такой план служит средством обеспечения ритмичного выпуска продукции и равномерной работы предприятия и доводит плановые задания до непосредственных исполнителей (рабочих). Оперативно-производственное планирование подразделяется на межцеховое, внутрицеховое и диспетчирование. Завершающим этапом заводского оперативно-производственного планирования является сменно-суточное планирование.

В целом перспективное, текущее и оперативно-производственное планирование взаимосвязаны и образуют единую систему. Упрощенная процедура разработки комплексного плана фирмы включает следующие основные элементы.

Имеются различные признаки классификации планирования по видам, срокам, формам и другим признакам. С точки зрения обязательности принятия и выполнения плановых заданий оно подразделяется на директивное и индикативное планирование. Директивное планирование характеризуется обязательным принятием и выполнением плановых заданий, установленных вышестоящей организацией для подчиненных ей предприятий. Директивное планирование пронизывало все уровни системы социалистического централизованного планирования (предприятия, отрасли, регионы, экономику в целом), сковывало инициативу предприятий. В рыночной экономике директивное планирование используется на уровне предприятий при разработке их текущих планов.

Индикативное планирование - это форма государственного регулирования производства через регулирование цен и тарифов, ставок налогов, банковских процентных ставок за кредит, минимального уровня заработной платы и других показателей. Задания индикативного плана называются индикаторами. Индикаторы — это параметры, характеризующие состояние и направления развития экономики, выработанные органами государственного управления. В составе индикативного плана могут быть и обязательные

задания, но их число весьма ограничено. Поэтому в целом план носит направляющий, рекомендательный характер. Применительно к предприятиям (организациям) индикативное планирование чаще применяется при разработке перспективных планов.

Необходимо различать перспективное планирование, прогнозирование, стратегическое планирование, тактическое планирование и бизнес-планирование, которые взаимосвязаны, образуют единую систему и в то же время выполняют различные функции и могут применяться самостоятельно. Как уже отмечалось выше, перспективное планирование основано на прогнозировании. Прогнозирование является базисом, фундаментом перспективного планирования и в отличие от него основано на предвидении, построенном на экономико-математическом, вероятностном и в то же время научно обоснованном анализе перспектив развития предприятия в обозримом будущем.

Стратегическое планирование ставит перспективные цели и вырабатывает средства их достижения, определяет основные направления развития предприятия (организации) и, что особенно важно, формирует миссию предприятия, направленную на реализацию его общей цели. Миссия детализирует статус предприятия (организации) и обеспечивает направления и ориентиры для определения целей и стратегий на различных уровнях развития. Тактическое планирование в отличие от перспективного и стратегического планирования охватывает краткосрочный и среднесрочный периоды и направлено на реализацию выполнения этих планов, которые конкретизируются в комплексных планов социально-экономического развития предприятия.

Битее-минирование является разновидностью технико-экономического планирования, однако в условиях рыночной экономики его функции значительно расширились и оно стало самостоятельным видом планирования. Существуют и другие классификации форм и видов планирования. Так, по классификации Р.Л. Акоффа, широко используемой в зарубежной науке и практике, планирование бывает:

реактивным - базируется на анализе и экстраполяции прошлого опыта снизу вверх;

инактивным - ориентируется на существующее положение предприятия для выживания и стабилизации бизнеса;

преактивным (упреждающим) - основано на прогнозах с учетом будущих изменений и осуществляется на предприятиях сверху вниз путем оптимизации решений;

интерактивным - заключается в проектировании будущего с учетом взаимодействия прошлого, настоящего и будущего, направленном на повышение эффективности развития предприятия и качества жизни людей.

Отметим, что планирование на предприятии (фирме) является важнейшим элементом рыночной системы, ее базисом и регулятором.

2. Содержание и структура планов

План позволяет очертить круг проблем, с которыми сталкивается предприятие при реализации своих целей в изменчивой, неопределенной, конкурентной хозяйственной среде. Поможет определить и обеспечить пути решения этих проблем. Он ориентирован на достижение успеха, главным образом, в финансово-экономической деятельности.

План является основой предложения при переговорах с будущими партнерами и возможными инвесторами. Это определяет некоторые требования к его оформлению, форме, содержанию и структуре. Он должен быть представлен в форме, позволяющей заинтересованному лицу получить четкое представление о существе дела и перспективах своего участия в нем.

Структура и содержание плана строго не регламентированы, но можно предложить следующий макет бизнес-плана: резюме (краткое содержание бизнес-плана); место нахождение предприятия; цель деятельности; описание вида деятельности, характеристика продукции (услуг); оценка рынка сбыта; конкуренция и конкурентное преимущество предприятия; внешнеэкономическая деятельность; стратегия маркетинга; прогнозирование продаж; план технической доработки продукта; план производства; управление предприятием; характеристика персонала; материально-техническое обеспечение; оценка риска; финансовый план; эффективность проекта.

Несколько иная структура бизнес-плана принята при получении кредитов в банке. Следует заручиться объективной оценкой плана. По возможности, заключение по бизнес-плану должен сделать аудитор.

В международной практике для обоснования проектов (бизнес-планов) применяется несколько обобщающих показателей: чистая текущая стоимость; рентабельность; внутренний коэффициент эффективности (пороговое значение рентабельности); период возврата капитальных вложений (срок окупаемости); максимальный денежный отток (отражает необходимые размеры финансирования проекта и должен быть увязан с источником покрытия всех затрат); норма безубыточности (минимальный размер партии выпускаемой продукции, при котором обеспечивается "нулевая прибыль", доход от продажи равен издержкам производства).

3. Критерии эффективности службы защиты информации. Методы оценки качества службы защиты информации

Организационно-штатная работа включает в себя:

•обобщение и анализ изменений в деятельности службы безопасности и подготовку предложений по приведению его организационно-штатной структуры в соответствие с объемом выполняемых задач;

•разработку структуры и формирование штатов службы безопасности и подчиненных ему подразделений;

•учет и анализ штатной численности службы безопасности по категориям и подразделениям;

•выработку предложений по наиболее рациональному и эффективному использованию имеющихся сил и средств, распределению и перераспределению имеющейся и дополнительно выделенной штатной численности;

•расчет нагрузки на сотрудников всех подразделений службы безопасности.

Организация эффективного использования связи

В целях эффективного использования системы связи штаб:

разрабатывает основополагающие документы (планы связи, распоряжения по связи, схемы организации радио- и проводной связи, таблицы позывных должностных лиц, наставления, инструкции и методические пособия) по вопросам организации и эксплуатации средств связи;

•организует стационарные и передвижные узлы связи;

•определяет лиц, имеющих в использовании средства связи, а также порядок пользования этими средствами;

•создает резерв средств связи;

•разрабатывает и реализует мероприятия по организации контроля за использованием средств связи. Цели, задачи, функции и другие вопросы деятельности штаба обычно отражаются в положении о штабе, примерный образец которого приведен в

приложении 6. После утверждения руководством службы безопасности и предприятия целей, задач и функций штаба необходимо сформировать его структуру.

В составе штаба целесообразно создать следующие подразделения: анализа и планирования, связей с общественностью, ресурсного обеспечения, дежурной части, справочно-информационного фонда, кабинета передового опыта, организационно-инспекторского, юридической и криптофафической защиты.' Все подразделения штаба условно можно разделить на 4 группы:

26. аналитические (отделение анализа и планирования, справочно-информационный фонд, кабинет передового опыта);

27. организационно- управленческие (дежурная часть и организационно-инспекторское отделение);

28. вспомогательные (отделение по связям с общественностью и отделение по ресурсному обеспечению);

29. внешней и внутренней защиты (юридическое отделение, криптографическая группа).

Силы и средства штаба и методы деятельности его сотрудников носят специфический характер. К силам относятся сотрудники, имеющие лицензию частных охранников или детективов и не имеющие ее (юристы, специалисты по шифросистемам, сотрудники подразделения по связи с общественностью и т.д.). Особые требования предъявляются к сотрудникам первой группы, которые должны иметь некоторый опыт работы в аналитических, штабных подразделениях или в дежурных частях правоохранительных органов.

В то же время каждый сотрудник штаба должен знать основы деятельности службы безопасности и ее подразделений, их .задачи и возможности; четко выполнять свои должностные обязанности; уметь анализировать, оценивать и кратко докладывать криминогенную обстановку; быстро и точно производить необходимые расчеты; качественно готовить штабные документы; знать и строго соблюдать требования по обеспечению коммерческой тайны; постоянно повышать уровень профессиональных и специальных знаний, совершенствовать практические навыки в штабной работе; объективно оценивать результаты деятельности подразделений службы безопасности.

Среди средств штабной работы в первую очередь следует выделить материально-технические и информационные средства. К материально-техническим средствам относится оборудование для пультов дежурных частей, компьютерные системы, вычислительная техника и т.д. В число информационных средств входят различного рода учеты,

справочники, сборники правовых актов, печатные публикации, сводки, аналитические материалы и т.д.

Особенностью финансового обеспечения штаба является относительно высокая, по отношению к другим подразделениям, оплата труда сотрудников, что вполне объяснимо, т.к. почти все они должны быть набраны из числа высококлассных специалистов.

Сотрудники штаба с учетом специфики своей работы могут применять методы деятельности, среди которых прежде всего упомянутые в ст. 5 Закона РФ «О частной детективной и охранной деятельности в Российской Федерации», если они не противоречат требованиям, изложенным в этом Законе. Например, опрос граждан и должностных лиц (с их согласия) производится только с целью получения сведений о работе сотрудников других подразделений службы безопасности.

Аналогичным образом применяются и другие методы (наведение справок, внешний осмотр строений, помещений и других объектов, наблюдение, в т.ч. электронное). Однако основным методом следует, видимо, признать изучение документов. В то же время надо подчеркнуть, что только комплексное применение вышеупомянутых методов может дать положительные результаты. Параллельно с методами, применение которых законом разрешено, штабные работники широко используют и такие общенаучные методы, как системный подход, моделирование, эксперимент и т.д.

Для объективной оценки деятельности штаба необходимо разработать соответствующие критерии и показатели его деятельности.

Критерием эффективной деятельности штабного подразделения можно признать качество его управленческого воздействия на подразделения службы безопасности в целом и его подразделений в отдельности. Показателями, раскрывающими этот критерий, являются: степень достижения цели планов; своевременное и полное обеспечение ресурсами подразделений службы безопасности по установленным нормам; оперативное и качественное выявление недостатков и положительного передового опыта, выявленного в процессе контроля и комплексного инспектирования; достаточное и своевременное предоставление сотрудникам службы безопасности установленных видов информационных документов.

Анализ практики функционирования служб безопасности позволяет утверждать, что слабая эффективность их деятельности в значительной степени является следствием существования различных проблем. Все эти проблемы настолько переплетены друг с другом, что разграничение их между собой на практике невозможно. Тем не менее автор посчитал необходимым сделать это, так как разграничение этих проблем позволяет в самом общем виде сформулировать способы их решения. Проблемы эти можно свести в четыре группы: правовые, организационные, кадровые и экономические. Рассмотрим эти проблемы и краткие предложения по их решению.

20. Отсутствие типового устава службы безопасности. Разработку, утверждение и официальное опубликование типового устава службы безопасности можно поручить Министерству юстиции РФ.

21. Неэффективное взаимодействие служб безопасности с право-охранительными и контрольно-надзирающими органами.

Правила и процедуры такого взаимодействия для каждого органа отдельно в рамках его компетенции могут быть определены в специальном постановлении Правительства России.

22. Запрет на ношение и применение оружия при охране жизни и здоровья физических лиц. Такой бессмысленный и необоснованный запрет легко отменить путем внесения соответствующих поправок в действующее законодательство.

23. Отсутствие закрепленного в законе перечня основных функций службы безопасности.

Необходимо в соответствующий раздел Закона «О частной детек-тивной и охранной деятельности в Российской Федерации» внести в качестве поправки исчерпывающий перечень этих функций.

24. Сдерживание развития службы безопасности в связи с высокими налоговыми платежами.

В законодательном порядке установить перечень налогов, сборов и т.д. для служб безопасности и льготного режима налогообложения в начале их деятельности (на год, три и т.д.).

25. Отсутствие самостоятельного статуса службы безопасности.

Внести необходимые поправки в Закон «О частной детективной и охранной деятельности в Российской Федерации» для признания службы безопасности как самостоятельной коммерческой негосударственной правоохранительной организации, т.е. юридическим лицом.

26. Запрет об оказании службой безопасности предприятия услуг другим физическим и юридическим лицам. Внести необходимые поправки в Закон «О частной детективной и охранной деятельности в Российской Федерации» с оговоркой, что такие услуги служба безопасности может осуществлять с согласия руководства предприятия-учредителя.

27. Отсутствие методики определения необходимого количества сотрудников службы безопасности для данного предприятия. Какая-либо общественная организация (фонд), занимающаяся проблемами безопасности в сфере предпринимательства, могла бы объявить конкурс на разработку такой методики.

28. Совмещение функций выдачи лицензии, регистрации и контроля за деятельностью служб безопасности у одного органа. Представляется, что выдача лицензий, регистрация сотрудников и самой службы безопасности должны быть закреплены за органами Министерства юстиции, функцию же контроля оставить за органами внутренних дел.

29. Отсутствие у руководителей служб безопасности необходимых правовых и организационно-управленческих знаний, умений и навыков. Разработка для этой категории руководителей силами преподавателей негосударственных образовательных учреждений программ спецкурсов.

30. Запрещение выдачи лицензий гражданам, имеющим судимость за совершение только умышленного преступления. Целесообразно дополнить ст. 6 Закона «О частной детективной и охранной деятельности в Российской Федерации» запретом на выдачу лицензий также гражданам, имеющим непогашенную судимость и совершивших неумышленные преступления.

31. Отсутствие нормативных оснований для одностороннего рас-торжения договора с предприятием-учредителем. Необходимо в законодательном порядке зафиксировать такие основания, как противоправные действия руководства предприятия-учредителя, задержки с выдачей зарплаты, незаконные указания, так как существующий в законодательстве порядок расторжения договора не содержит ясного и исчерпывающего перечня таких оснований.

32. Несовершенство статистического учета результатов деятельности службы безопасности. Целесообразно создание в органах Министерства юстиции единого и детального учета результатов деятельности служб безопасности по муниципальным территориальным образованиям, регионам и стране в целом.

33. Запрет на выдачу лицензии бывшим работникам правоохранительных органов, осуществляющим контроль за частной детективной и охранной деятельностью, если со дня их увольнения не прошел год. Практика показала, что такой запрет необходимо отменить путем внесения поправок в Закон «О частной детективной и охранной деятельности в Российской Федерации». Привлечение этой категории законопослушных и

профессионально грамотных сотрудников к работе в службах безопасности (например, в штабных подразделениях) только укрепит в них состояние законности и дисциплины.

34. Невозможность действий сотрудников службы безопасности вне государственной территории Российской Федерации. Решение этой проблемы видится в подписании межправительственнных соглашений, регламентирующих порядок действий сотрудников службы безопасности на территории другой страны.

35. Запрет на создание службы безопасности для группы предприятий и коммерческих организаций.

Такой запрет нелогичен, поскольку толкает их руководителей к обеспечению собственной безопасности неправовыми средствами. Устранить этот запрет можно внесением соответствующей поправки к Закону «О частной детективной и охранной деятельности в Российской Федерации».

36. Необходимость письменного согласия предпринимателя при заключении им коммерческого контракта на выяснение биографических и других характеризующих личность контрагента данных. Общеизвестно, что на практике такое согласие никогда не дается. Следует внести соответствующие коррективы в действующее законодательство, т.к. предпринимательская деятельность в условиях риска требует, среди прочего, информацию о личности делового партнера.

37. Несоответствие между декларируемой в Законе «О частной детективной и охранной деятельности в Российской Федерации» общей позицией законодателя о признании частных охранно-детективных структур коммерческими организациями и закреплением в этом же Законе статуса служб безопасности как структурных подразделений предприятия. Целесообразно внести поправку к Закону о признании службы безопасности коммерческой организацией, имеющей право заключать договора на обслуживание многих предприятий.

В процессе работы службы безопасности регулярно возникает необходимость контроля за выполнением как плановых мероприятий, так и эффективностью деятельности подразделений. Эту работу организует начальник штаба в рамках своей компетенции или по указанию своего непосредственного начальника. Надо сказать, что контроль этот не является всеобъемлющим (в силу малочисленности со-трудников штаба), а выборочным. Объектами контроля становятся те «болевые точки», изучение которых позволит сделать вывод об эффективности деятельности либо подразделения, либо службы безопасности в целом. Например, контроль за обеспечением пропускного режи-ма необходим для объективной оценки степени защищенности всего охраняемого объекта.

Для повышения эффективности контроля необходимо в обязательном порядке проверять фактическое устранение недостатков, выявленных в процессе первичного контроля («контроль за контролем»). Регулярные проверки осуществляются с применением досье контроля на определенный объект. Фиксируются не только недостатки, но и положительный опыт в работе.

Комплексное инспектирование подчиненных подразделений.

Отдельные контрольные проверки не позволяют оценить деятельность подчиненных подразделений в целом. Оценка возможна только по итогам комплексного инспектирования. В ходе инспектирования обследованию подлежит как деятельность всего подразделения в це-лом, так и его групп (секторов) и каждого сотрудника. Системный анализ позволяет выявлять недостатки и положительные результаты, тенденции развития, профессиональный уровень сотрудников и т.д.

Поскольку в ходе комплексного инспектирования требуется произвести глубокий и качественный анализ, то необходимо предоставить инспекторской группе значительное время, в связи с чем не рекомен-дуется проводить такое инспектирование чаще, чем один раз в год.

По итогам инспектирования составляется акт, который представляется руководителю службы безопасности (второй экземпляр вручается начальнику инспектируемого подразделения). Представляется, что этот акт, видимо, должен быть формализованным, поскольку это позволит проследить динамику изменений в инспектируемом подразде-лении за несколько лет.

Организация взаимодействия и координации между подразделениями.

Организация взаимодействия условно подразделяется на два вида. Во-первых, постоянное взаимодействие между подразделениями, которое требует организующего воздействия со стороны штаба. Например, при проведении длительных по времени и крупных по масштабу привлекаемых сил и средств комплексных операций (борьба с кражами, обеспечение порядка во время ярмарок, специализированных выставок и т.д.).

Во-вторых, временное взаимодействие для решения повседневных конкретных задач. Примером может служить контроль за несением службы охранниками на своих постах и маршрутах; своевременное введение в действие сил и средств при возникновении чрезвычайных ситуаций (119;201) доведение до сведения сотрудников подразделений необходимой информации и т.д. При организации взаимодействия между подразделениями возникает опасность вторжения штаба в их компетенцию. Избежать этого можно путем четкого разграничения функций.

Такое взаимодействие можно квалифицировать как вертикальное (участники разных ступеней иерархии), информационное (обмен информацией), консультационное (методическое), организационное (установление регламентов, нормативов и пр.) и формальное. В отличие от организации взаимодействия, координировать может только штаб, наделенный соответствующими полномочиями по отношению к остальным подразделениям службы безопасности. Координация заключается в согласовании и упорядочении действий этих подразделений.

По своему характеру координационная деятельность штаба может быть превентивной (направленной на сохранение существующей схемы работы) и стимулирующей (направленной на улучшение деятельности системы даже при отсутствии конкретных проблем).

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

2.1 Практическое занятие № 1 (2 часа).

Тема: «Оценочные стандарты в информационной безопасности**»**

2.1.1 Задание для работы:

1. Мероприятия и обеспечение ИБ

2.1.2 Краткое описание проводимого занятия:

Желая помочь своим коллегам, программист Сальников и адвокат Сабуров - работники нотариальной конторы «ОКС» - внесли изменения в программу «Акты и

документы о недвижимости». В результате этих действий была уничтожена информация, касающаяся опыта работы конторы в области регистрации недвижимости за последний год и нарушена работа ПК.
Руководитель нотариальной конторы обратился к прокурору с заявлением о возбуждении уголовного дела против Сальникова и Сабурова.
Есть ли в действиях Сальникова и Сабурова состав преступления?
Решение:
Согласно норме п. 1 ст. 273 УК РФ, создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.
Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок до семи лет (п. 2 ст. 273 УК РФ).

3.1.3 Результаты и выводы:

Студент знакомится с оценочными стандартами в информационной безопасности.

2.2 Практическое занятие № 2 (2 часа).

Тема: «Роль стандартов ИБ**»**

2.2.1 Задание для работы:

1. Конституция РФ
2. Доктрина информационной безопасности РФ

3.2.2 Краткое описание проводимого занятия:

Главный редактор журнала «Нефтяник» Щукин отказался публиковать решение Ступинского народного суда по гражданскому делу своего племянника - Антона Коробкина. Однако, когда председатель народного суда Рябинина потребовала, чтобы Щукин выполнил решение суда, содержащее прямое указание об опубликовании названного документа, главный редактор нехотя ответил: «Хорошо, мы опубликуем это решение, но за плату. Нашему журналу не на что жить».
Рябинина возмутилась и пожаловалась на Щукина в Государственный комитет РФ по печати.
Нарушен ли в этой ситуации закон?
Решение:
Да, в этой ситуации закон нарушен
Согласно положению ст.35 Закона «О средствах массовой информации», редакция обязана опубликовать бесплатно и в предписанный срок:
- вступившее в законную силу решение суда, содержащее требование об опубликовании такого решения через данное средство массовой информации;
- поступившее от органа, зарегистрировавшего данное средство массовой информации, сообщение, касающееся деятельности редакции.
Редакции средств массовой информации, учредителями (соучредителями) которых являются государственные органы, обязаны публиковать по требованию этих органов их официальные сообщения в порядке, регулируемом уставом редакции или заменяющим его договором, а равно иные материалы, публикация которых в

данных средствах массовой информации предусмотрена законодательством Российской Федерации

2.2.3 Результаты и выводы:

Студент знакомится со стандартами ИБ.

2.3 Практическое занятие № 3 (2 часа).

Тема: «Оценочные стандарты в информационной безопасности Международный стандарт ISO/IEC 15408**»**

2.3.1Задание для работы:

1.Федеральные законы о безопасности.

2.Основные принципы обеспечения безопасности

3.3.1 Краткое описание проводимого занятия:

Директор сельской школы Сорокоумова, историк по образованию, купила по безналичному расчёту для своих учеников 10 ПК IBM. При этом она, слабо разбираясь в технике, не осмотрела компьютеры, а поверила на слово продавцу, который расхваливал товар и не предоставил ей возможность получить соответствующую информацию о нём. При установке техники в школе специалисты выявили, что две машины разукомплектованы и в двух компьютерах разбиты экраны мониторов.

Сорокоумова обратилась в магазин с просьбой заменить бракованные компьютеры, но там с ней отказались разговаривать. Она собрала необходимые документы и обратилась с иском в суд, утверждая, что при покупке компьютеров продавец не предоставил ей всю информацию о товаре.

Правомерны ли действия Сорокоумовой и продавца компьютерной техники?

Решение:

Согласно норме ст. 495 ГК РФ, продавец обязан предоставить покупателю необходимую и достоверную информацию о товаре, предлагаемом к продаже, соответствующую установленным законом, иными правовыми актами и обычно предъявляемым в розничной торговле требованиям к содержанию и способам предоставления такой информации.

Покупатель вправе до заключения договора розничной купли-продажи осмотреть товар, потребовать проведения в его присутствии проверки свойств или демонстрации использования товара, если это не исключено ввиду характера товара и не противоречит правилам, принятым в розничной торговле.

Если покупателю не предоставлена возможность незамедлительно получить в месте продажи информацию о товаре, указанную в пунктах 1 и 2 ст. 495 ГК РФ, он вправе потребовать от продавца возмещения убытков, вызванных необоснованным уклонением от заключения договора розничной купли-продажи (пункт 4 статьи 445), а если договор заключен, в разумный срок отказаться от исполнения договора, потребовать возврата уплаченной за товар суммы и возмещения других убытков.

Продавец, не предоставивший покупателю возможность получить соответствующую информацию о товаре, несет ответственность и за недостатки товара, возникшие после его передачи покупателю, в отношении которых покупатель докажет, что они возникли в связи с отсутствием у него такой информации.

2.3.3 Результаты и выводы:

Студент знакомится с оценочными стандартами в информационной безопасности Международный стандарт ISO/IEC 15408

2.4 Практическое занятие №__4___ (_2_ часа).

Тема: «Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799**»**

2.4.1 Задание для работы:

1. Права субъекта персональных данных
2. Обязанности оператора
3. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований настоящего Федерального закона

2.4.2 Краткое описание проводимого занятия:

Программист Голанов поступая в фирму «Сокол», формально отнесся к заполнению документов по типовым формам , предложенным руководством фирмы. В течение двух лет Голанов создал ряд программных продуктов, реализация которых принесла фирме «Сокол» значительную прибыль и известность в республике. Видя это, Голанов обратился к руководству фирмы с просьбой выплатить ему денежное вознаграждение как автору программ, обеспечивших заметный успех коллективу. Однако генеральный директор фирмы Валентинов, ссылаясь на регулярную выплату заявителю высокого должностного оклада, отказался удовлетворить его просьбу. При этом он заявил, что свои программы Голанов создал в служебное время и, кроме того, программист не осуществил регистрацию программ в установленном законом порядке.
Прав Голанов или Валентинов?
Решение:
Прав Валентинов.
Согласно ст. 1296 ГК РФ, в случае, когда программа для ЭВМ или база данных создана по договору, предметом которого было ее создание (по заказу), исключительное право на такую программу или такую базу данных принадлежит заказчику, если договором между подрядчиком (исполнителем) и заказчиком не предусмотрено иное. Автор созданных по заказу программы для ЭВМ или базы данных, которому не принадлежит исключительное право на такую программу или такую базу данных, имеет право на вознаграждение в соответствии с абзацем третьим пункта 2 статьи 1295 ГК РФ.

3.4.2 Результаты и выводы:

Студент знакомится со стандартами управления информационной безопасностью BS 7799 и ISO/IEC 17799

2.5 Практическое занятие №__5___ (_2_ часа).

Тема: «Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования”**»**

2.5.1 Задание для работы:

1. Лицензирование права деятельности.
2. Сертификация услуг (работ)

2.5.2 Краткое описание проводимого занятия:

Администрация фирмы «Свет» поручила своему программисту Алексееву, работавшему по трудовому договору, создать базу данных для учета материальных ценностей предприятия. В целях быстрейшего выполнения поставленной задачи программист использовал некоторые типовые разработки своих знакомых коллег, работавших в других организациях. В результате установки данных программ на ПК в компьютер был внесен вирус. Помимо этого, по истечении некоторого времени на ПК был установлен факт уничтожения базы данных в результате действия вируса. В итоге фирме «Свет» пришлось закупать новую базу данных, в результате чего она понесла убытки. Администрация предприятия, рассмотрев сложившуюся ситуацию, наложила на Алексеева штраф в размере трёх месячных окладов и лишила его премии. Программист написал жалобу в прокуратуру, требуя отмены решения руководства фирмы и снятия с него всех обвинений.
Имеются ли здесь нарушения законодательства об информации, информационных технологиях и защите информации?
Решение:
Да, нарушения законодательства об информации, информационных технологиях и защите информации имеются. Администрация фирмы «Свет» права.
Непосредственным объектом преступления, предусмотренного ст. 274 УК РФ, признаются общественные отношения, обеспечивающие правильную и безопасную эксплуатации ЭВМ, системы ЭВМ или их сети. Предмет преступления - охраняемая законом компьютерная информация. Объективная сторона характеризуется нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшим уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.
Под правилами эксплуатации ЭВМ, системы ЭВМ или их сети (компьютерной системы) понимаются правила, установленные компетентным государственным органом, или технические правила, установленные соответствующими лицами, которыми могут быть изготовители ЭВМ, разработчиками компьютерных программ, их законные владельцы и др., определяющие порядок работы с ЭВМ (нормативные акты, инструкции, правила, техническое описание, положение, приказы и т.д.).

2.5.3 Результаты и выводы:

Студент знакомится с международным стандартом ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования”

2.6 Практическое занятие № 6 (2 часа).

Тема: «Создание СУИБ на предприятии**»**

2.6.1 Задание для работы:

1. Режимные объекты
2. Меры защиты информации

2.6.2 Краткое описание проводимого занятия:

В правительственном обзоре средств массовой информации от 24 апреля 2001г. со ссылкой на радио «Эхо Москвы» и газету «Русский телеграф» сообщалось, что в США произошел самый серьёзный за всю историю случай проникновения в компьютерные сети Пентагона. Группа хакеров взломала все защитные схемы и похитила секретное программное обеспечение, которое использовалось с военной спутниковой системой. При этом взломщики, требуя выкуп, пригрозили продать

программу террористам. С похитителями долго беседовали через интернет представители Пентагона, уговаривали их отказаться от преступных замыслов, но бесполезно. Группа хакеров - люди от 19 до 28 лет, восемь из которых находились в США, пятеро в Великобритании и двое в Российской Федерации - настаивали на своём. Однако через сутки, чувствуя неотвратимость наказания, взломщики заявили журналистам, что они отказываются от своих намерений, но взамен требуют от руководителей США, Великобритании и России немедленно прекратить гонку вооружений, ибо эти государства своей военной политикой ведут мир к неминуемой катастрофе.
Оцените эту ситуацию с точки зрения норм информационного права.
Квалифицируйте действия двух российских граждан, участвовавших в указанной выше акции.
Решение:
Преступность в сфере высоких технологий (киберпреступность) является серьезной угрозой национальной безопасности РФ. Она приобрела характер транснациональной организованной преступности, о чем отмечено в Бангкокской декларации по результатам XI Конгресса ООН 2005 г. В Конвенции о преступности в сфере компьютерной информации (Будапешт, 2001 г.с Дополнительным протоколом, в котором Россия не участвует), не только государства - члены Совета Европы, но и другие признали необходимость проведения в приоритетном порядке общей политики в сфере уголовного права, нацеленной на защиту общества от преступности в сфере компьютерной информации.
В целях обеспечения эффективной борьбы с рассматриваемыми преступлениями было принято Соглашение о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере компьютерной информации (Минск, 2001 г.). В Соглашении определены основные термины:
а) преступление в сфере компьютерной информации - уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация;
б) компьютерная информация - информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи;
в) вредоносная программа - созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;
г) неправомерный доступ - несанкционированное обращение к компьютерной информации.

2.6.3 Результаты и выводы:

Студент знакомится с создание СУИБ на предприятии

2.7 Практическое занятие №__7___ (_2_ часа).

Тема: «Основные процессы СУИБ»

2.7.1 Задание для работы:

1. Изучение документов по лицензированию и сертификации продукции

2.7.2 Краткое описание проводимого занятия:

Используя электронную сеть «Межсвязь», главный специалист коммерческого банка «Кубыш» Кусочкин в течение двух недель передавал с магнитных носителей информацию в департамент ценных бумаг ЦБ РФ. При этом он однажды рассказал

о содержании направленных в ЦБ сообщений своему другу – юристу Министерства связи Савенко. Савенко, зная, что его товарищи из адвокатской фирмы «Прокруст» готовят иск против «Кубыш», немедленно переправил им полученную информацию. Адвокаты по достоинству оценили полученные сведения, использовали их при подготовке иска и в итоге – выиграли дело у банка. Узнав об этом, председатель правления коммерческого банка «Кубыш» Пупкин уволил Кусочкина с работы за разглашение коммерческой тайны. Кусочкин не согласился с решением Пупкина и обжаловал его действия в суде.
Проанализируйте ситуацию с точки зрения норм информационного права и квалифицируйте действия Кусочкина, Савенко и Пупкина.

2.7.3 Результаты и выводы:

Студент знакомится с основными процессами СУИБ

2.8 Практическое занятие №__8___ (_2_ часа).

Тема: «Процессы улучшения СУИБ**»**

2.8.1 Задание для работы:

1. Защита интеллектуальной собственности в интернете

2.8.2 Краткое описание проводимого занятия:

Инженер-программист Кархунен был принят на работу в акционерное общество «Кентавр», где на него возлагались функции оператора ПЭВМ по вводу законодательства в информационные базы, которые «Кентавр» продавал на коммерческой основе предприятиям легкой промышленности. В свободное от ввода информации время Кархунену удалось разработать и внедрить более совершенный алгоритм обработки правовой информации в информационной базе, что заметно повысило ее ценность и привело к получению значительной прибыли. На собрании учредителей акционерного общества «Кентавр» было предложено премировать Кархунена, а его разработку использовать в ходе реализации модернизированной программы на выгодных коммерческих условиях. Однако Кархунен заявил руководству общества, что оно нарушает его авторские права, и потребовал отчисления ему всей прибыли за использование его программного продукта.
Как разрешитъ этот спор с позиции норм информационного права?

2.8.3 Результаты и выводы:

Студент знакомится с процессами улучшения СУИБ

2.9 Практическое занятие №__9___ (_2_ часа).

Тема: «Процесс «Мониторинг эффективности**»**

2.9.1 Задание для работы:

1. Разработка политики безопасности

2.9.2 Краткое описание проводимого занятия:

Журналист областной газеты Журавлев, проанализировав состояние работы по обеспечению техники безопасности на машиностроительном заводе «Подшипник», подготовил разгромную статью о нарушениях правил безопасности на указанном предприятии и передал ее для публикации главному редактору газеты Лапушкину. Однако под давлением директора завода Скатова, не заинтересованного в распространении объективной информации, Лапушкин отклонил критическую статью журналиста, и она не была опубликована. Кроме того, главный редактор газеты рекомендовал Журавлеву в дальнейшем сосредоточиться на другой тематике. Обиженный журналист обратился с жалобой в Судебную палату по информационным спорам при Президенте РФ.
Оцените эту ситуацию с точки зрения законодательства о средствах массовой информации.
Какие меры здесь необходимо принять к нарушителям?

2.9.3 Результаты и выводы:

Студент знакомится с процессом «Мониторинг эффективности»

2.10 Практическое занятие №__10___ (_2_ часа).

Тема: «Основные процессы СУИБ**»**

2.10.1 Задание для работы:

1. Активы организации
2. Расчет риска

2.10.2 Краткое описание проводимого занятия:

В телевизионной передаче «Властелины вкуса» ведущий Нямкин, демонстрируя приготовление блюд, целенаправленно обращал внимание телезрителей на несколько продуктов, представляемых по сюжету передачи. При этом он постоянно упоминал пищевой концентрат «То-то» – одно из вкуснейших современных добавок.
Просмотр этой передачи вызвал у фирмы «Странник» живой интерес к продукту «То-то», который она закупила для продовольственного снабжения туристической компании. Однако после употребления пищевого продукта клиентами и его анализа независимыми экспертами было отмечено, что рекламируемые по телевидению вкусовые качества «То-то» явно не соответствуют тем характеристикам, о которых говорил ведущий Нямкин в передаче. Некоторые клиенты фирмы, получая продукт «То-то» в качестве приправы, получили аллергические расстройства и эти неприятные факты были зафиксированы врачами.
В результате руководство фирмы «Странник» охарактеризовало действия Нямкина как скрытую и недостоверную рекламу и обратилось с иском в суд к телевизионной компании, потребовав от нее компенсацию морального ущерба и возмещения вреда, причиненного здоровью своих клиентов.
Как необходимо квалифицировать действия Нямкина и правомерны ли требования фирмы «Странник»?

2.10.3 Результаты и выводы:

Студент знакомится с основными процессами СУИБ

2.11 Практическое занятие №__11___ (_2_ часа).

Тема: «Подбор кадров службы защиты информации**»**

2.11.1 Задание для работы:

1. Модель нарушителя

2.11.2 Краткое описание проводимого занятия:

Региональное информационное агентство, используя возможности контроля телефонных каналов связи, препятствовало негосударственному предприятию «Связник» в реализации его функций международного информационного обмена и предлагало ему заключить договор на оказание услуг в области эксплуатации каналов связи. Однако условия, на которых предлагалось заключить этот договор, были для предприятия «Связник» невыгодны: согласно условиям договора, оно должно было передать региональному информационному агентству за услуги свои имущественные права на 25% акций.

Правомерны ли действия регионального агентства с точки зрения законодательства о международном информационном обмене?

2.11.3 Результаты и выводы:

Студент знакомится с подбором кадров службы защиты информации

2.12 Практическое занятие №__12___ (_2_ часа).

Тема: «Методика оценки рисков информационной безопасности предприятия**»**

2.12.1 Задание для работы:

1. Функциональные обязанности СБО

2.12.2 Краткое описание проводимого занятия:

Фирма «КомпасЮр» оказывала различного рода правовые услуги гражданам с использованием правовых информационно-поисковых систем «Правовик» и «Юрисконсульт», являвшихся ее собственностью.

Через год эта фирма открыла свое дочернее предприятие «Юркон» и передала ему часть технических средств со всем программным обеспечением, которое ранее было установлено на них. Прошел год и предприятие «Юркон» объявило себя самостоятельным и независимым от фирмы «КомпасЮр», выкупив у нее ПЭВМ, на которых оставались правовые системы, принадлежавшие «КомпасЮр». Однако в своей деятельности сотрудники дочернего предприятия продолжали использовать эти информационно-поисковые системы.

Имеются ли нарушения законодательства при использовании фирмой «КомпасЮр» и ее дочерними предприятиями технических средств и программ?

2.12.3 Результаты и выводы:

Студент знакомится с методикой оценки рисков информационной безопасности предприятия

2.13 Практическое занятие № 13 (2 часа).

Тема: « Метод оценки рисков на основе модели угроз и уязвимостей**»**

2.13.1 Задание для работы:

1. Анализ ИБ предприятия

2.13.2 Краткое описание проводимого занятия:

Оператор ЭВМ Мячев, работавший в локальной сети редакции газеты, в соответствии с должностной инструкцией обязан был перед вводом в ЭВМ информации, поступающей от корреспондентов на дискетах, проводить антивирусный контроль машинных носителей. Стремясь завершить работу досрочно, Мячев однажды пренебрег требованиями инструкции и в результате допущенных им нарушений информация подготовленного к печати 8-полосного номера газеты была разрушена; выпуск номера был задержан и в результате редакции причинен материальный ущерб.

Квалифицируйте действия оператора Мячева в соответствии с действующим законодательством о компьютерной информации.

2.13.3 Результаты и выводы:

Студент знакомится с метод оценки рисков на основе модели угроз и уязвимостей

2.14 Практическое занятие № 14 (2 часа).

Тема: «Методика оценки рисков информационной организации на основе модели информационных потоков**»**

2.14.1 Задание для работы:

1. Угрозы конфиденциальной информации

2.14.2 Краткое описание проводимого занятия:

Российский научно-исследовательский институт «Квант» являлся разработчиком и создателем информационной базы данных об испытаниях авиационно-космической техники. Институт получил разрешение Правительства РФ и соответственно своего министерства о направлении соответствующей информации о характеристиках авиационной аппаратуры в аналогичную научную организацию, находящуюся на территории Белоруссии.

Однако представитель ФАПСИ, через которого предполагалось обеспечить передачу этой информации, обратил внимание дирекции института на конфиденциальный характер передаваемых сведений и, ссылаясь на этот факт, отказал НИИ в выделении каналов и средств для передачи информации. Институт «Квант» обжаловал решение представителя ФАПСИ в Правительство РФ.

Как решить эту ситуацию с точки зрения норм информационного права?

2.14.3 Результаты и выводы:

Студент знакомится с методикой оценки рисков информационной организации на основе модели информационных потоков

2.15 Практическое занятие № 15 (2 часа).

Тема: «Разработка корпоративной методики анализа рисков. Методы оценивания информационных рисков**»**

2.15.1 Задание для работы:

1. Принципы создания систем ИБ

2.15.2 Краткое описание проводимого занятия:

Программист Содеев несколько лет работал в акционерном обществе «Сторм». Однако при приеме его на работу явным образом не оговаривались и не были записаны в трудовом договоре его имущественные права на создаваемые программы.

За время трудовой деятельности Содеев разработал эффективную систему автоматизации учета товаров на предприятии. Но, не удовлетворенный своей заработной платой, он уволился, предложив руководству общества «Сторм» свои платные услуги по сопровождению и модернизации программного обеспечения созданной им системы. Руководство сочло запрошенную Содеевым оплату слишком высокой и отвергло его предложение.

Впоследствии в акционерное общество «Сторм» был принят на работу программист Ковекс, на которого тоже были возложены обязанности по развитию и сопровождению системы автоматизированного учета товаров на предприятии.

Содеев, предвидя, что ему не удастся добиться желаемого соглашения с администрацией общества, модифицировал свою программу, в результате чего она перестала нормально функционировать, а это практически парализовало всю систему учета в «Сторме».

Оцените сложившуюся ситуацию с информационно-правовых позиций.

2.15.3 Результаты и выводы:

Студент знакомится с разработкой корпоративной методики анализа рисков. Методы оценивания информационных рисков

2.16 Практическое занятие № 16 (2 часа).

Тема: «Оценка рисков по факторам**»**

2.16.1 Задание для работы:

1. Процесс построения КСЗИ

2.16.2 Краткое описание проводимого занятия:

Юрист Букашко, работая в юридической фирме «НормаЛик» помощником генерального директора, в свободное от работы время несанкционированно получал доступ к чужим программам и постоянно пользовался ими.

Информацию, полученную в чужих базах данных, Букашко часто использовал не по назначению, продавал ее своим клиентам. При этом из-за несанкционированного проникновения помощника генерального директора в названные программы в них стали появляться сбои. Впоследствии собственники информационных ресурсов установили причины сбоев программных продуктов и потребовали строгого наказания Букашко.

Дайте правовую оценку действиям Букашко

2.16.3 Результаты и выводы:

Студент знакомится с оценкой рисков по факторам