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

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.03 Организационное и правовое обеспечение безопасности объектов

Направление подготовки (специальность) 27.03.04 Управление в технических системах

Профиль подготовки (специализация) Интеллектуальные системы обработки информации и управления

Квалификация выпускника бакалавр

Форма обучения заочная

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1 (2 часа)

Тема: «Вводная. Системная концепции обеспечения безопасности объектов охраны»

1.1.1 Вопросы лекции:

1. 1. Исходные положения для разработки системной концепции обеспечения безопасности объектов охраны

2.Основные составляющие информационной безопасности.

1.1.2 Краткое содержание вопросов:

1. Исходные положения для разработки системной концепции обеспечения безопасности объектов охраны

В данной работе излагаются основные направления деятельности по обеспечению безопасности объектов охраны, привлекательных для преступников с различных точек зрения. Преступные посягательства могут преследовать различные цели, например:

- кражи материальных и/или информационных ценностей;
- имеющие в своей основе террористические действия, направленные на решение политических или грабительских задач, как то: разрушение объекта; захват управления функционированием объекта; информационная разведка; ограбление; внедрение членов организованных преступных формирований или групп в управленческие структуры и т.д.

Актуальность системного решения проблем и задач охранной деятельности особенно возросла в последние годы, что диктуется многими факторами, например:

- в современных условиях становления новых общественных, экономических, политических, производственных и иных отношений при недостатке механизмов их правового регулирования происходит закономерный взрыв криминогенной обстановки. Резко активизируется деятельность организованных преступных структур, происходит их количественный рост, качественная техническая и методическая оснащенность, проникновение в коммерческие, государственные, в том числе и в правоохранительные органы. По информационно-аналитическим обзорам специалистов уровень преступности в ближайшие годы будет сохраняться;
- преступные действия организованных структур, направленные на захват и ограбление учреждений, на получение конфиденциальной информации о деятельности предприятий и т.д., все в большей степени подготавливаются как глубоко продуманные, технически хорошо оснащенные, смоделированные на достаточно высоком интеллектуальном и психологическом уровне акции;
- по данным экспертов подготовка и проведение преступных акций в большинстве случаев осуществляются на высоком профессиональном уровне, характеризуются системным решением и часто отличаются жестокостью исполнения.

Исходя из изложенного, разработчики системной концепции обеспечения безопасности объектов в максимальной степени должны учитывать мировой и отечественный опыт, касающийся всей многогранной деятельности, организуемой по защите объектов.

Практика охранной деятельности показывает, что необходим научно обоснованный подход к решению проблем и задач охраны объектов, в особенности, если это особо важные, особо опасные объекты, объекты особого риска или объекты, содержащие большие материальные ценности.

В связи с тем, что наиболее высоким уровнем разработки систем защиты характеризуются особо опасные, особо важные, особо режимные объекты и банки, и этот опыт, безусловно, полезен для объектов многих отраслей народного хозяйства, где

возможно придется работать сегодняшним студентам, в списке литературы приведены наименования соответствующих источников, опубликованных в открытой печати.

Очевидно, коль скоро действия преступников часто носят не просто ухищренный, а системно продуманный профессионалами характер, им следует противопоставить организацию и оснащение, выполненные на более высоком уровне профессионализма. Этим и объясняется необходимость разработки обобщенной системной концепции по обеспечению безопасности объектов, которая в каждом случае должна быть адаптирована к конкретному объекту, исходя из условий его функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды и обстановки и т.д. Таким образом, для каждого конкретного объекта должна разрабатываться на основе общей своя собственная концепция безопасности, исходя из положений которой разрабатывается проект оснащения объекта инженерно-техническими, специальными и программно-аппаратными средствами защиты.

Технические средства охраны, установленные на объектах охраны, должны в комплексе с силами физической охраны и системой инженерных сооружений удовлетворять современным требованиям по охране 00 от устремлений потенциального нарушителя.

Учитывая изложенное, разработчики технических средств охранной сигнализации и комплексов технических средств охраны при анализе исходных положений для определения "моделей нарушителей" должны рассматривать и такие факторы, характерные для современной жизни, как:

- наличие в свободной продаже зарубежных и отечественных изделий спецтехники;
- возможность приобретения современного вооружения;
- возможность рекрутирования организованными преступными формированиями подготовленных в силовых структурах людей;
- наличие значительных финансовых ресурсов в криминальных структурах и т.д., т.е. факторов, расширяющих возможность преступных формирований организовывать против объектов охраны преступные действия с высоким уровнем их предварительной подготовки.

Одной из центральных подсистем в системе обеспечения безопасности 00 является автоматизированная система охраны, с помощью которой реализуются практические меры по предупреждению недозволенного доступа к технике, оборудованию, материалам, документам и охране их от шпионажа в пользу конкурентов, диверсий, повреждений, хищений и других незаконных или преступных действий.

На практике действия АСО складываются из двух основных фаз: обнаружение нарушителя и его задержание.

Задачи обнаружения нарушителя и определения места его проникновения могут быть решены как с помощью патрулей из личного состава службы охраны, так и с помощью технических средств охраны. Задачи обнаружения нарушителя и контроля за состоянием безопасности охраняемых объектов решаются, главным образом, с помощью технических средств охраны и телевизионного наблюдения. Применение этих средств позволяет в разумных пределах снизить численность личного состава охраны, но при этом повысить надежность защиты объекта, увеличить оперативность в принятии мер к задержанию нарушителя.

2. Определение стратегии комплексной безопасности

Как показали результаты многих исследований, для выработки системного решения, удовлетворяющего необходимым и достаточным условиям обеспечения надежной защиты 00 от подготовленного и технически оснащенного нарушителя, требуется полный учет не только перечисленных выше факторов, но и многих других, как то: состояние инженерных сооружений объекта, состав и уровень подготовки сил

физической охраны объекта, окружение объекта, характер объекта, расположение и количество сил поддержки, состояние сетей электропитания объекта и т.д.

Многолетний опыт по созданию систем защиты объектов убеждает в безусловной необходимости разрабатывать в каждом случае системную концепцию обеспечения безопасности конкретного объекта, которая на практике предполагает комплексное взаимоувязанное решение руководством предприятия и службой безопасности ряда крупных блоков задач, как то:

1. Определение стратегии комплексной безопасности.

Здесь решаются проблемы классификации, систематизации и дифференциации угроз; определяются структура и задачи служб безопасности; разрабатываются нормативно-правовые документы, регламентирующие с позиций юриспруденции деятельность служб безопасности; на основе анализа ресурсов, технико-экономических показателей и социальных аспектов безопасности разрабатываются планы мероприятий по обеспечению безопасности объектов.

2. Обеспечение безопасности от физического проникновения на территорию и в помещения объекта. В этом блоке задач на основе анализа доступности объекта моделируются стратегия и тактика поведения потенциального нарушителя; дифференцируются зоны безопасности; на основе определения ключевых жизненно важных центров объектов разрабатываются принципы и схемы оборудования техническими средствами охранной сигнализации и телевизионного наблюдения, средствами инженерной, технической и специальной защиты рубежей охраны. Соответственно, на основе расчета тактико-технических требований выбирается состав и номенклатура технических средств.

3. Защита информации. Решение задач данного блока обеспечивается специальными методами защиты. На основе разработки принципов проверки, классификации источников информации и каналов ее утечки разрабатываются концептуальные модели защиты от утечки информации, проводятся их оценки на предмет эффективности предлагаемых этими моделями решений. Здесь решается широкая гамма задач разработки методов защиты по всем возможным каналам утечки. Разрабатывается нормативная база по защите от утечки информации. На основе моделирования возможных способов приема информации потенциальным нарушителем за пределами помещений посредством применения направленных микрофонов, лазерных средств и т.п. вырабатываются методы пассивной и активной защиты.

4. Защита от прогнозируемых к применению средств негласного контроля. Эти задачи ориентированы на модель нарушителя - сотрудника учреждения, либо на проведение контрразведывательных мероприятий, если по оперативным каналам получена информация о заинтересованности, которую проявили организованные преступные формирования к данному объекту. Здесь решается ряд специфических задач от выбора и установки средств негласного контроля до выбора организационно-режимных мер защиты от негласного контроля со стороны потенциального нарушителя. Большое внимание здесь уделяется техническим средствам дефектоскопии, автоматизации средств контроля трактов передачи информации, анализу системы демаскирующих признаков и ряду других.

5. Защита от диверсионно-террористических средств. Задачи данной предметной области также решаются специальными методами защиты. На основе исследования, классификации и моделирования вариантов активных действий террористов, прогнозирования возможных способов доставки ДТС на территорию объекта, изучения каналов управления диверсиями и технических способов их осуществления выбирается аппаратура обнаружения ДТС, разрабатываются организационно-технические мероприятия по созданию контрольных пунктов, постов проверки, использованию меточной техники и ряд других. Разрабатываются рекомендации по выбору техники обнаружения.

1. 2 Лекция № 2 (2 часа)

Тема: «Организация службы безопасности объекта**»**

1.2.1 Вопросы лекции:

1. Организация службы безопасности объекта
2. Функции, задачи и особенности службы безопасности объекта

1.2.2 Краткое содержание вопросов:

1. Организация службы безопасности объекта

В современных условиях перед предприятиями особо остро встает задача сохранения как материальных ценностей, так и информации, в том числе и сведений, составляющих коммерческую или государственную тайну. Беззастенчивая кража предприятиями и организациями интеллектуальной собственности друг друга стала почти массовым процессом. К этому следует добавить целенаправленные действия по сманиванию или подкупу рабочих и служащих предприятий конкурента с целью завладения секретами их коммерческой и производственной деятельности. Для защиты коммерческих секретов предприятия создают собственные службы безопасности, важной предпосылкой создания которых является разработка их структуры, состава, положений о подразделениях и должностных инструкций для руководящего состава и сотрудников

Служба безопасности (СБ) является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия. Такая структура управления системой безопасности, имеющая четкую вертикаль, характерна для области обеспечения безопасности, где требуется определенность, четкие границы, регламентация отношений на всех уровнях – от рядового сотрудника до менеджеров высшего звена. Как показывает практика, только на предприятиях, где проблемы безопасности находятся под постоянным контролем руководителя предприятия, достигаются наиболее высокие результаты.

Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности. При этом руководитель СБ должен обладать максимально возможным кругом полномочий, позволяющим ему влиять на другие подразделения и различные области деятельности предприятия, если этого требуют интересы безопасности.

Основными задачами службы безопасности предприятия являются:

- обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;
- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;
- организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
- предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
- выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
- обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;
- обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;

- обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
- оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

2. Функции, задачи и особенности службы безопасности объекта

Служба безопасности предприятия выполняет следующие общие функции:

- организует и обеспечивает пропускной и внутриобъектовый 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 обеспечения 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 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.
- Единой методики формирования структуры службы безопасности не существует. Предлагается следующий алгоритм построения СБ (рис. 1):
- определить жизненно важные интересы предприятия на момент создания службы безопасности;

- выявить угрозы безопасности для данного объекта;
- провести анализ угроз и выявить степень риска при их реализации;
- наметить пути локализации каждой из угроз и просчитать затраты на проведение соответствующих мероприятий;
- исходя из полученных данных, финансовых и трудовых возможностей, разработать структуру службы безопасности;
- поддерживать работоспособность СБ и корректировать ее структуру в зависимости от изменяющихся условий.

1. 3 Лекция № 3 (2 часа)
Тема: «Цели и задачи СБО»

1.3.1 Вопросы лекции:
1.Принципы построения службы безопасности
2.Основные задачи службы безопасности

1.3.2 Краткое содержание вопросов:

1. Принципы построения службы безопасности

1) Приоритет мер предупреждения. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе анализа которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

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

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

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

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

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

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

8) Плановая основа деятельности. Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам

(экономическая, научно-техническая, экологическая, технологическая и т.д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

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

2.Основные задачи службы безопасности

· обеспечение защиты информации и сведений, являющихся коммерческой тайной;

· организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите информации;

· организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся защищаемой информацией;

· предотвращение необоснованного допуска и доступа к сведениям и работам, являющихся защищаемой информацией;

· выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;

· обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;

· обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;

· обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;

· оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

1. 4 Лекция № 4 (2 часа)

Тема: «Функции и задачи СБ»

1.4.1 Вопросы лекции:

1.Функции службы безопасности

2.Задачи службы безопасности.

1.4.2 Краткое содержание вопросов:

1. Функции службы безопасности

· 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 информации;

· участвует в разработке основополагающих документов с целью закрепления в них требований обеспечение безопасности и защиты информации, 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 защищаемой информацией , при всех видах работ;

· 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;

· организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;
разрабатывает, ведет, обновляет и пополняет «Перечень сведений, подлежащих защите» и другие

· нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;

· обеспечивает строгое выполнение требований нормативных документов по защите информации;

· осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите информации;

· организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты информации;

· 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;

2.Задачи службы безопасности.

.

· обеспечение защиты информации и сведений, являющихся коммерческой тайной;

· организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите информации;

· организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся защищаемой информацией;

· предотвращение необоснованного допуска и доступа к сведениям и работам, являющихся защищаемой информацией;

· выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;

· обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;

· обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;

· обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;

· оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

1. 5 Лекция № 5 (2 часа)

Тема: «Законодательство об информации, информационных технологиях и защите информации»

1.15.1 Вопросы лекции:

1.Сфера действия настоящего Федерального закона

2.Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

1.15.2 Краткое содержание вопросов:

1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон определяет условия и порядок принудительного исполнения судебных актов, актов других органов и должностных лиц, которым при осуществлении установленных федеральным законом полномочий предоставлено право возлагать на иностранные государства, физических лиц (далее также - граждане), юридических лиц, Российскую Федерацию, субъекты Российской Федерации, муниципальные образования (далее также - организации) обязанности по передаче другим гражданам, организациям или в соответствующие бюджеты денежных средств и иного имущества либо совершению в их пользу определенных действий или воздержанию от совершения определенных действий.

2. Условия и порядок исполнения судебных актов по передаче гражданам, организациям денежных средств соответствующего бюджета бюджетной системы Российской Федерации устанавливаются бюджетным законодательством Российской Федерации.

3. Условия и порядок исполнения отдельных судебных актов, актов других органов и должностных лиц могут устанавливаться иными федеральными законами.

(часть 3 введена Федеральным законом от 05.04.2013 N 33-ФЗ)

2.Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:
1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2) установление ограничений доступа к информации только федеральными законами;
3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6) достоверность информации и своевременность ее предоставления;
7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Не предусмотрено РУП

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие №1 (2 часа)

.

Тема: «Организация службы безопасности объекта**»**

3.1.1 Задание для работы:

1. Организация службы безопасности объекта
2. Функции, задачи и особенности службы безопасности объекта

3.1.2 Краткое описание проводимого занятия:

1. Организация службы безопасности объекта

В современных условиях перед предприятиями особо остро встает задача сохранения как материальных ценностей, так и информации, в том числе и сведений, составляющих коммерческую или государственную тайну. Беззастенчивая кража предприятиями и организациями интеллектуальной собственности друг друга стала почти массовым процессом. К этому следует добавить целенаправленные действия по сманиванию или подкупу рабочих и служащих предприятий конкурента с целью завладения секретами их коммерческой и производственной деятельности. Для защиты коммерческих секретов предприятия создают собственные службы безопасности, важной предпосылкой создания которых является разработка их структуры, состава, положений о подразделениях и должностных инструкций для руководящего состава и сотрудников

Служба безопасности (СБ) является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия. Такая структура управления системой безопасности, имеющая четкую вертикаль, характерна для области обеспечения безопасности, где требуется определенность, четкие границы, регламентация отношений на всех уровнях – от рядового сотрудника до менеджеров высшего звена. Как показывает практика, только на предприятиях, где проблемы безопасности находятся под постоянным контролем руководителя предприятия, достигаются наиболее высокие результаты.

Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности. При этом руководитель СБ должен обладать максимально возможным кругом полномочий, позволяющим ему влиять на другие подразделения и различные области деятельности предприятия, если этого требуют интересы безопасности.

2. Функции, задачи и особенности службы безопасности объекта

Служба безопасности предприятия выполняет следующие общие функции:

- организует и обеспечивает пропускной и внутриобъектовый 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 обеспечения 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;

3.1.3 Результаты и выводы:

Студент знакомится с организацией службы безопасности объекта**, с** функциями, задачами и особенности службы безопасности объекта

3.2 Практическое занятие № 2 (2 часа).

Тема: «Цели и задачи СБО**»**

3.2.1 Задание для работы:

1.Принципы построения службы безопасности

2.Основные задачи службы безопасности

3.2.2 Краткое описание проводимого занятия:

1. Принципы построения службы безопасности

1) Приоритет мер предупреждения. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе анализа которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

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

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

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

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

2.Основные задачи службы безопасности

· обеспечение защиты информации и сведений, являющихся коммерческой тайной;

· организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите информации;

· организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся защищаемой информацией;

· предотвращение необоснованного допуска и доступа к сведениям и работам, являющихся защищаемой информацией;

· выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;

3.2.3 Результаты и выводы:

Студент знакомится с основными принципами построения и основными задачами службы безопасности

3.3 Практическое занятие № 3 (2 часа)

Тема: «Функции и задачи СБ**»**

3.3.1 Задание для работы:

1.Функции службы безопасности

2.Задачи службы безопасности

3.3.2 Краткое описание проводимого занятия:

1. Функции службы безопасности

· 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 информации;

· участвует в разработке основополагающих документов с целью закрепления в них требований обеспечение безопасности и защиты информации, 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 защищаемой информацией , при всех видах работ;

· 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;

· организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;
разрабатывает, ведет, обновляет и пополняет «Перечень сведений, подлежащих защите» и другие

Задачи службы безопасности.

· обеспечение защиты информации и сведений, являющихся коммерческой тайной;

· организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите информации;

· организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся защищаемой информацией;

· предотвращение необоснованного допуска и доступа к сведениям и работам, являющихся защищаемой информацией;

· выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;

· обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;

· обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;

3.3.3 Результаты и выводы:

Студент знакомится с функциями службы безопасности и задачами службы безопасности

3.4 Практическое занятие № 4 (2 часа).
Тема: «Изучение нормативно-правовых документов**»**

3.4.1 Задание для работы:
1.Защита информации при реализации информационных процессов.
2.Предотвращение и исправление неправильных действий пользователей

3.4.2 Краткое описание проводимого занятия:
Под защитой информации принято понимать использование различных средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения надежности передаваемой, хранимой и обрабатываемой информации. Защитить информацию - это значит: обеспечить физическую целостность информации, т.е. не допустить искажений или уничтожения элементов информации; не допустить подмены (модификации) элементов информации при сохранении ее целостности; не допустить несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий; быть уверенным в том, что передаваемые (продаваемые) владельцем информации ресурсы будут использоваться только в соответствии с обговоренными сторонами условиями. Способы несанкционированного доступа к информации: просмотр; копирование и подмена данных; ввод ложных программ и сообщений в результате связи; чтение остатков информации на ее носителях; прием сигналов электромагнитного излучения и волнового характера; использование специальных программных и аппаратных "заглушек" и т.п. Система защиты информации - это совокупность организационных, административных и технологических мер, программно - технических средств, правовых и морально-этических норм, направленных на противодействие угрозам нарушителей с целью сведения до минимума возможного ущерба пользователям владельцам системы. Архитектура безопасности: анализ возможных угроз разработка системы защиты; реализация системы защиты; сопровождение системы защиты. Программные средства и методы зашиты активнее и шире других применяются для защиты информации в персональных компьютерах и компьютерных сетях. Функции защиты: разграничение и контроль доступа к ресурсам; регистрация и анализ протекающих процессов, событий, пользователей; предотвращение возможных разрушительных воздействий на ресурсы

3.4.3 Результаты и выводы:
Студент знакомится с угрозой конфиденциальной информации