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 очная

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)

Тема: «Функции и задачи IT-отдела СБ»

1.5.1 Вопросы лекции:

1. Функции IT-отдела
2. Задачи IT-отдела

1.5.2 Краткое содержание вопросов

1. Функции IT-отдела

В процессе производственной деятельности организации ИТ-отдел осуществляет следующие функции:

1. Приобретение: - активного сетевого оборудования; - серверов; - средств резервного копирования и восстановления данных; - средств защиты информации; - средств контроля и управления сетевой инфраструктурой; - периферийного оборудования; - вычислительной техники и комплектующих; - программного обеспечения; - расходных материалов и запасных частей к устройствам печати и офисной технике.

2. Установка, настройка, техническое сопровождение и обслуживание: - серверов; - активного сетевого оборудования; - аппаратных и программных средств защиты информации; - аппаратных и программных средств контроля и управления сетевой инфраструктурой; - средств резервного копирования и восстановления данных; - рабочих станций; - периферийного оборудования; - программного обеспечения; - офисной техники.

3. Организация автоматизированных рабочих мест.

4. Диагностика и устранение неисправностей вычислительной и офисной техники.

5. Диагностика и устранение неполадок программного обеспечения.

6. Координация работ с поставщиками и производителями вычислительной и офисной техники по вопросам гарантийного обслуживания и ремонта.

7. Координация работ с подрядчиками и субподрядчиками - производителями программного обеспечения по вопросам приобретения, обновления и модификации.

8. Разработка, внедрение и организация контроля исполнения руководящих документов по обеспечению информационной безопасности.

9. Разработка плана обеспечения непрерывной работы и восстановления работоспособности подсистем автоматизированных систем.

10. Анализ потребностей организации в дополнительных средствах вычислительной техники и обработки информации.

2.Задачи ИТ-отдела

Задачами ИТ-отдела являются:

1. реализация работ по обеспечению бесперебойного функционирования и развития программно-аппаратных комплексов;

2. обеспечение защиты сведений, составляющих коммерческую тайну, в процессе деятельности организации;

3. осуществление в соответствии с законодательством Российской Федерации работы по комплектованию, хранению, учету и использованию архивных документов, образовавшихся в процессе деятельности организации. 1. реализация концепции развития информационных систем;

4. обеспечение требуемого уровня информационной безопасности;

5. разработка стандартов на использование вычислительной техники и программного обеспечения;

6. обеспечение информационной и технической поддержки средств вычислительной техники и программного обеспечения;

7. проведение работ по оптимизации использования информационно-технических ресурсов.

1.6 Лекция № 6 (2)

Тема: «Организационная структура системы ОИБ**»**

1.6.1 Вопросы лекции

1. Цели создания системы ОИБ
2. Основные понятия по ИБ

1.6.2 Краткое содержание вопросов:

1. Цели создания системы ОИБ

2. Технологии создания системы ОИБ

Конечной *целью создания системы обеспечения безопасности информационных технологий* является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), наносимого субъектам информационных отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Основной задачей системы защиты является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) АС соответствующими множеству значимых угроз методами и средствами.

Обеспечение информационной безопасности - это непрерывный процесс, основное содержание которого составляет управление, - управление людьми, рисками, ресурсами, средствами защиты и т.п. Люди - обслуживающий персонал и конечные пользователи АС, - являются неотъемлемой частью автоматизированной (то есть *«человеко-машинной»)* системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и ее безопасность.

2. Технологии обеспечения информационной безопасности

Под *технологией обеспечения информационной безопасности в АС* понимается определенное распределение функций и регламентация порядка их исполнения, а также порядка взаимодействия подразделений и сотрудников (должностных лиц) организации по обеспечению комплексной защиты ресурсов АС в процессе ее эксплуатации.

Требования к технологии управления безопасностью:

• соответствие современному уровню развития информационных 4; технологий;

• учет особенностей построения и функционирования различных подсистем АС;

• точная и своевременная реализация политики безопасности организации;

• минимизация затрат на реализацию самой технологии обеспечения безопасности.

Для реализации технологии обеспечения безопасности в АС необходимо:

• наличие полной и непротиворечивой правовой базы (системы взаимоувязанных нормативно - методических и организационно -распорядительных документов) по вопросам ОИБ;

• распределение функций и определение порядка взаимодействия подразделений и должностных лиц организации по вопросам ОИБ на всех этапах жизненного цикла подсистем АС, обеспечивающее четкое разделение их полномочий и ответственности;

• наличие специального органа (подразделения защиты информации, обеспечения информационной безопасности), наделенного необходимыми полномочиями и непосредственно отвечающего за формирование и реализацию единой политики информационной безопасности организации и осуществляющего контроль и координацию действий всех подразделений и сотрудников организации по вопросам ОИБ.

Реализация технологии ОИБ предполагает:

• назначение и подготовку должностных лиц (сотрудников), ответственных за организацию, реализацию функций и осуществление конкретных практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

• строгий учет всех подлежащих защите ресурсов системы (информации, ее носителей, процессов обработки) и определение требований к организационно-техническим мерам и средствам их защиты;

• разработку реально выполнимых и непротиворечивых организационно-распорядительных документов по вопросам обеспечения безопасности информации;

• реализацию (реорганизацию) технологических процессов обработки информации в АС с учетом требований по информационной безопасности;

• принятие эффективных мер сохранности и обеспечения физической целостности технических средств и поддержку необходимого уровня защищенности компонентов АС;

• применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывную административную поддержку их использования;

• регламентацию всех процессов обработки подлежащей защите информации, с применением средств автоматизации и действий сотрудников структурных подразделений, использующих АС, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств АС, на основе утвержденных организационно-распорядительных документов по вопросам обеспечения безопасности информации;

• четкое знание и строгое соблюдение всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

• персональную ответственностью за свои действия каждого сотрудника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС;

• эффективный контроль за соблюдением сотрудниками подразделений - пользователями и обслуживающим АС персоналом, - требований по обеспечению безопасности информации;

• проведение постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработку и реализацию предложений по совершенствованию системы защиты информации в АС.

Организационные (административные) меры регламентируют процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

1.7 Лекция №7 (2 часа)

Тема: «Работа с персоналом**»**

1.7.1 Вопросы лекции:

1. Проблемы безопасности коммерческих структур в работе с кадрам
2. Методы сбора информации

1.29.2 Краткое содержание вопросов:

1. Проблемы безопасности коммерческих структур в работе с кадрам

Анализ сообщений средств массовой информации и оперативных сводок правоохранительных органов о последних диверсионно-террористических актах против коммерческих структур в Москве и других городах России позволяет сделать однозначный вывод о высокой степени осведомленности преступников относительно режима дня и динамики деятельности предпринимателей: жертв, как правило, неизменно встречали в районе проживания или места работы либо с предельной точностью по времени и месту перехватывали на трассе. Заблаговременно были изучены основные и запасные маршруты перемещения коммерсантов. Преступники располагали подробными сведениями о составе семьи и родственниках будущих жертв, марках и номерных знаках

личных и служебных автомашин, соседях и т.п. Таким образом очевидно, что любые противоправные деяния, связанные с силовым воздействием на коммерческие структуры, тщательно планируются и, следовательно, состоят из нескольких последовательных этапов, среди которых вторжения, хищения, вооруженные нападения являются фактически финальными акциями преступников.

В этой связи современная система мер безопасности должна быть ориентирована на то, чтобы прогнозировать и выявлять признаки вероятных правонарушений, а тем более преступлений на ранних стадиях, на этапе формирования умысла и разработки криминальными сообществами планов преступных действий, что позволяет предупредить и предотвратить подобного рода деяния.

Неотъемлемым составляющим элементом любой планируемой преступной акции является сбор информации. Представляется возможным выделить следующие основные методы, которые используются злоумышленниками в настоящее время для добывания сведений о коммерческих структурах:

наблюдение, в т.ч. с помощью мобильных и стационарных оптико-технических средств, скрытое фотографирование, видеозапись; выведывание информации; хищения каких-либо внутренних документов лицами, внедренными или приобретенными в коммерческих структурах, которые согласились или оказались вынужденными осуществлять указанные действия по корыстным побуждениям, в результате угроз, по физическому принуждению либо по иным причинам;

перехват информации на различных каналах внутренней и внешней связи коммерческих структур;

получение информации техническими средствами путем использования различных источников сигналов в помещениях коммерческих структур как связанных с функционирующей аппаратурой (персональные компьютеры), так и через специально внедренную технику негласного съема информации (спецзакладки, в т.ч. дистанционного управления);

добывание информации о коммерческих структурах посредством применения системы аналитических методов (структурный анализ, финансовый анализ, анализ образцов научно-технической продукции и т.д.).

В настоящее время использование сотрудников коммерческих структур в качестве источников внутренней информации рассматривается как наиболее надежный, быстрый и эффективный способ получения конфиденциальных данных. Отметим также, что кроме добывания собственно конфиденциальной информации, такой внутренний источник из сотрудников коммерческих организаций может быть использован одновременно для получения уточняющих сведений, которые бы дополняли данные, добытые техническими средствами.

Помимо этого, агентурные информационные источники сегодня все более активно используются для оказания выгодного криминальным структурам, а также конкурентам влияния на стратегию и тактику поведения руководителей соответствующих коммерческих структур, а также иных лиц, принимающих ответственные решения в сфере налогообложения, таможенной политики, экспортно-импортных квот, землеотвода и т.д.

2. Методы сбора информации

1. Кабинетное исследование— метод сбора и оценки уже существующей маркетинговой информации, собранной и подготовленной для других целей.
Кабинетные методы сбора информации используют вторичные источники, поэтому часто называются методами работы с документами.
Источники вторичной информации — это субъекты, предоставляющие информацию о других объектах или из других источников (в уже обработанном виде, предназначенном для своих целей изучения объекта).
Проведение исследования кабинетными методами обладает рядом преимуществ:

- осуществляется быстро и недорого,
- позволяет ознакомиться с отраслью, отследить основные тенденции рынка,
- получить данные, которые фирма не в состоянии собрать самостоятельно.

Часто задействуют сразу несколько источников, чтобы сопоставить данные, выявить несколько подходов для решения проблемы.

Недостатки кабинетных исследований связаны с недостатками качества используемой информации:

- трудно проверить достоверность и надежность вторичной информации,
- она обладает низкой релевантностью, может быть старой или устаревшей;
- разные источники используют различные системы классификаций объектов, методики измерения, поэтому сведения из разных источников могут быть противоречивы и не всегда сопоставлены.
- могут быть опубликованы не все результаты исследования, поэтому информация будет неполной.

Группа кабинетных методов сбора информации включают следующие методы:

- традиционный (классический) метод анализа
- информативно-целевой анализ
- контент-анализ документов

2. Полевое исследование — метод сбора и оценки информации первичной информации, которая собрана непосредственно об объекте исследования.

Источник первичной информации — это непосредственно сам объект исследования, создает информацию в соответствии с поставленными целями ее сбора. Источники первичной информации лишены указанных выше недостатков вторичной информации, и обладают принципиальными достоинствами:

- собираются в точном соответствии с целями исследования,
- методика сбора информации контролируется самой фирмой,
- результаты надежны, предоставляют всю полноту информации.

Информацию от источников первичной информации можно собирать полевыми методами, к которым относятся наблюдение, эксперимент и опрос.

Существует несколько способов сбора первичных данных:

наблюдение,
эксперимент,
опрос.

2.1. Наблюдение — это метод сбора первичной информации путем пассивной регистрации исследователем определенных процессов, действий, поступков людей, событий, которые могут быть выявлены органами чувств.

Наблюдение проводится с соблюдением ряда условий.

Короткий отрезок времени, чтобы изменения в окружающей обстановке не повлияли на изучаемое поведение.

Наиболее значимые характеристики условий и ситуаций, в которых происходит наблюдение, также должны фиксироваться.

Наблюдаемые процессы должны быть доступны и происходить на публике.

Наблюдению подвергается такое поведение, которое люди не имеют желания запоминать.

Наблюдение, как один из полевых методов сбора информации, характеризуется определенными достоинствами и недостатками.

1. 8 Лекция № 8 (2 часа)

Тема: «ИТЗ информации**»**

1.8.1 Вопросы лекции:

1. Направления формирования системы защиты информации

2. Этапы реализации концепции защиты информации

1.8.2 Краткое содержание вопросов:

1. Направления формирования системы защиты информации

Понятие системности заключается не просто в создании соответствующих механизмов защиты, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла ИС. При этом все средства, методы и мероприятия, используемые для защиты информации объединяются в единый целостный механизм - систему защиты.

К сожалению, необходимость системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит должного понимания у пользователей современных ИС.

Сегодня специалисты из самых разных областей знаний, так или иначе, вынуждены заниматься вопросами обеспечения информационной безопасности. Это обусловлено тем, что в ближайшие лет сто нам придется жить в обществе (среде) информационных технологий, куда перекочуют все социальные проблемы человечества, в том числе и вопросы безопасности…

Каждый из указанных специалистов по-своему решает задачу обеспечения информационной безопасности и применяет свои способы и методы для достижения заданных целей. Самое интересное, что при этом каждый из них в своем конкретном случае находит свои совершенно правильные решения. Однако, как показывает практика, совокупность таких правильных решений не дает в сумме положительного результата - система безопасности в общем и целом работает не эффективно.

Если собрать всех специалистов вместе, то при наличии у каждого из них огромного опыта и знаний, создать СИСТЕМУ информационной безопасности зачастую так и не удается. Разговаривая об одних и тех же вещах, специалисты зачастую не понимают друг друга поскольку у каждого из них свой подход, своя модель представления системы защиты информации. Такое положение дел обусловлено отсутствием системного подхода, который определил бы взаимные связи (отношения) между существующими понятиями, определениями, принципами, способами и механизмами защиты…

Постановка задачи.

Одиннадцать отдельно взятых футболистов (даже очень хороших) не составляют команду до тех пор, пока на основе заданных целей не будет отработано взаимодействие каждого с каждым. Аналогично СЗИ лишь тогда станет СИСТЕМОЙ, когда будут установлены логические связи между всеми ее составляющими.

Как же организовать такое взаимодействие? В футболе команды проводят регулярные тренировки, определяя роль, место и задачи каждого игрока. Качество или эффективность команд оценивается по игре в матчах, результаты которых заносятся в турнирную таблицу. Таким образом, после проведения всех встреч команд (каждой с каждой), можно сделать вывод об уровне состояния мастерства как команды в целом, так и отдельных ее игроков. Побеждает тот, у кого наиболее четко организовано взаимодействие…

Выражаясь терминами современного бизнеса, для решения вопросов взаимодействия нужно перейти от "чисто" технического на "конкретно" логический уровень представления процессов создания и функционирования СИСТЕМ защиты информации. Хотелось бы, чтобы все специалисты, считающие себя профессионалами в информационных технологиях, поднялись чуть выше "багов" и "кряков" и уже сейчас задумались над тем как их знания и опыт будут логически увязаны со знаниями и опытом других специалистов.

В "строгой научной постановке" задача автора состоит в предоставлении пользователям вспомогательного инструмента "елки" - (модели СЗИ), а задача читателя

(пользователя) - украсить эту "елку" новогодними игрушками - (своими знаниями и решениями). Даже если "игрушек" пока еще нет, наличие "елки" поможет выбрать и приобрести нужные "украшения".

Конечный результат работы (степень красоты елки) зависит от ваших желаний, способностей и возможностей. У кого-то получится хорошо, у кого-то - не совсем… Но это естественный процесс развития, приобретения знаний и опыта.

Кстати, оценить красоту елки (эффективность системы защиты) весьма проблематично, поскольку у каждого из нас свои требования и вкусы, о которых, как известно, не спорят, особенно с руководством.

Таким образом, многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. В то же время, большой объем имеющихся публикаций вряд ли может сформировать четкое представление о том как же приступить к созданию системы защиты информации для конкретной информационной системы, с учетом присущих ей особенностей и условий функционирования. Как сказал классик юмора: "…многообразие ваших вопросов порождает многообразие наших ответов…"

Возникает вопрос: можно ли сформировать такой подход к созданию систем защиты информации, который объединил бы в нечто единое целое усилия, знания и опыт различных специалистов? При этом желательно что бы указанный подход был универсальным, простым, понятным и позволял бы в одинаковой степени удовлетворить любые вкусы (требования) гурманов информационной безопасности?

Этапы реализации концепции защиты информации

Основными задачами системы защиты информации являются:

проведение единой государственной политики, организация и координация работ по защите информации;

исключение или существенное затруднение добывания информации средствами технической разведки, а также предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждение специальных воздействий на информацию с целью ее уничтожения, искажения и блокирования;

принятие в пределах компетенции межрегиональных и региональных (по субъекту Российской Федерации), правовых актов, регулирующих отношения в области защиты информации;

анализ состояния и прогнозирование источников угроз безопасности информации в целом и в субъектах Российской Федерации;

формирование и организация деятельности межрегиональных, региональных и объектовых органов по защите информации;

разработка и внедрение новых методов, средств и технологий защиты информации и контроля ее эффективности;

контроль состояния защиты информации в органах власти и организациях;

анализ состояния системы защиты информации, выявление ключевых проблем в области защиты информации;

определение приоритетных направлений развития системы защиты информации;

научно-техническое, методическое и информационное обеспечение работ по защите информации в органах власти и организациях;

создание и развитие межрегиональных и региональных учебных, научно-исследовательских, производственных комплексов в области защиты информации;

создание системы мониторинга состояния защиты информации в в интересах информационного обеспечения принятия решений по защите информации;

реализация действующих систем государственного регулирования в области обеспечения защиты информации (лицензирования, сертификации, аттестации);

создание системы подготовки и переподготовки кадров в области защиты информации.

Организационная система защиты информации состоит из трех уровней: межрегионального, регионального и объектового.

На межрегиональном уровне:

Территориальные органы Минобороны России, ФСБ России, МВД России и других федеральных органов исполнительной власти межрегионального уровня, их подразделения по противодействию иностранным техническим разведкам и технической защите информации и постоянно-действующие технические комиссии.

Аппараты органов судебной власти Российской Федерации межрегионального уровня, их подразделения по технической защите информации и постоянно-действующие технические комиссии.

Научно-исследовательские организации в области защиты информации.

Аттестационные центры, органы по сертификации, аттестации объектов информатизации.

1. 9 Лекция № 9 (2 часа)

Тема: «Информационное общество и его безопасность**»**

1.9.1 Вопросы лекции:

1.Понятие информационное общество

2. Ключевые проблемы и условия развития информационного общества.

1.9.2 Краткое содержание вопросов:

1. Понятие информационное общество

Часто понятие "информация" используют, не задумываясь о глубине его содержания, отождествляя понятия знание, данные, информация.

Очевидно, что "обиходное" употребление термина "информация" совершенно неуместно, когда речь идет о теории или теориях информации. Нередко в этих теоретических построениях термин "информация" наполнен разным смыслом, а, следовательно, сами теории высвечивают лишь часть граней некоторой системы знаний, которую можно назвать общей теорией информации или "информологией" - наукой о процессах и задачах передачи, распределения, обработки и преобразования информации.

Возникновение информологии как науки можно отнести к концу 50-х годов нашего столетия, когда американским инженером Р. Хартли была сделана попытка ввести количественную меру информации, передаваемой по каналам связи.

Информация является одним из основных понятий кибернетики в разделе теории информации. В теории информации математическими методами изучаются способы измерения количества информации, содержащейся в каких-либо сообщениях, и передачи информации.

Информация - это продукт взаимодействия данных и методов, рассмотренный в контексте этого взаимодействия.

Информация появляется в процессе коммуникации с определенным объектом. Без коммуникации с объектом получение информации практически невозможно.

Например, для того, чтобы выловить необходимую информацию из газеты, необходимо прочитать саму газету и сделать выводы, то есть собрать и обработать информацию. Если же просто прикоснуться к газете - необходимую информацию мы не получим.

Коммуникация - передача сообщения от одной стороны к другой (кто с кем, посредством чего, каково содержание, эффекты коммуникации).

Коммуникация может происходить на нескольких уровнях - между индивидами, между социальными группами, в рамках одного общества, между разными обществами.

Различные знаки в коммуникации наделяются различными смысловыми значениями и представлены в виде кодов.

Многое в современной коммуникации организовано в виде институтов, обращенных к массовой аудитории.

Коммуникация - это то, что передается, это формы собственности, внутренняя структура, ценность организации, реакция аудитории.

В нашем определении важным является пояснение «…рассмотренный в контексте этого взаимодействия». Приведем примеры, почему это действительно важно. Известно, что книги - это хранилища данных. Они предназначены для получения информации методом чтения. Но если попробовать разные книги на ощупь или на вкус, то тоже можно получить информацию.

Такие методы позволят различить книги, выполненные в кожаных, картонных и бумажных переплетах. Разумеется, это не те методы, которые предполагались авторами книг, но они тоже дают информацию, хотя и не полную.

Анализируя информационную ценность газет, журналов, телепередач, мы можем прийти к выводу, что она зависит как от данных, так и от методов, которыми выполняется их потребление. Одно дело - внимательно просматривать телефильм, вслушиваясь в каждое слово, и вовсе другое смотреть его, одновременно разговаривая по телефону.

2. Ключевые проблемы и условия развития информационного общества

Создание информационной экономики, на базе широкого внедрения цифровых методов обработки информации в различных отраслях экономики, что объективно приводит в информационном обществе к:

- повышению скорости реакции на внешние и внутренние изменения и оперативности принятий управленческих решений;
- повышению точности и качества выполнения непосредственных производственных операций;
- повышению производительности производственного оборудования;
- снижению трудоемкости человеческого труда, используемого в непосредственном производстве промышленных изделий, товаров и усдуг;
- созданию полностью автоматизированных производств за счет компьютеризации и роботизации производственных операций;
- существенному сокращению сроков производства промышленностью конечных изделий и товаров, за счет сокращения сроков разработки, испытаний и постановки на серийное производство создаваемых промышленных изделий и товаров, а также непосредственного их серийного изготовления;
- снижению себестоимости и повышению рентабельности производства создаваемых промышленных изделий, товаров и услуг;
- повышению конкурентоспособности создаваемых промышленных изделий и товаров, за счет повышения их качества, а также функциональных и эксплуатационных характеристик;

Информационное общество в своем становлении и развитии базируется на знаниях, поэтому четвертым условием развития информационного общества является решение двух взаимосвязанных постоянных фундаментальных цивилизационных проблем:

- прогноз развития существующих знаний во всех областях человеческой деятельности, накопленных за предшествующие периоды социально-экономического развития;
- формирование новых знаний и их последующим практическим использованием в социально-экономической деятельности человека, в том числе с использованием технологии форсайт;

- прогрессирующая интеллектуализация товаров и услуг.

Прогноз развития накопленных знаний осуществляется человечеством постоянно на всех этапах социально-экономического развития. При этом для осуществления прогноза существующих знаний в какой-либо анализируемой конкретной сфере человеческой деятельности использовался и продолжает использоваться информационно-логический способ, базирующийся на синтаксическом (количественном) анализе человеком обрабатываемой им информации. На результаты такого прогноза весьма существенное влияние оказывает субъективный фактор (человека-эксперта, непосредственно осуществляющего прогноз), который устранить в полной мере (для получения объективного прогноза) пока еще не удавалось[2].

При этом, если ранее, на всех предшествующих этапах социально-экономического развития человечества, информационно-логический способ синтаксического (количественного) анализа обрабатываемой человеком информации был объективно предопределен (как единственно возможный способ прогноза развития существующих знаний), то в настоящее время, созданные человеком современные мощные программно-информационные комплексы и системы обработки информации различного класса и назначения, открывают возможность разработки и применения для решения указанных выше двух постоянных фундаментальных цивилизационных проблем, уже совершенно нового способа анализа информации, - семантического (т.е. смыслового) способа анализа обрабатываемых массивов синтаксической (текстовой) информации, который неизбежно сменит синтаксический способ, и который позволит, во-первых, на основе проведенного смыслового анализа обрабатываемой информации осуществлять объективный прогноз развития существующих знаний, и, во-вторых, на основе этого прогноза формировать новые знания.

Третьей комплексной ключевой проблемой формирования и развития информационного общества в нашей стране является проблема создания и развертывания во всех регионах Российской Федерации и во всей стране в целом необходимых элементов инфраструктуры различных информационных и телекоммуникационных сетей, информационно сопрягаемых и взаимодействующих как между собой, так и с глобальной сетью Интернет. При этом, в рамках решения этой комплексной ключевой проблемы, необходимо решить также проблему преодоления "цифрового разрыва" различных регионов Российской Федерации.

Данная проблема имеет две стороны своего проявления. Первая - это развертывание в стране всех необходимых элементов инфраструктуры различных информационных и телекоммуникационных сетей, информационно сопрягаемых и взаимодействующих как между собой, так и с глобальной сетью Интернет.

А вторая сторона - это преодоление цифрового разрыва различных групп населения, городов и регионов Российской Федерации, и связана она, во-первых, с различными их возможностями доступа к информационным технологиям и информационным ресурсам и использованием последних при реализации процессов своей жизнедеятельности, и, во-вторых, с разрывом информационного пространства взаимодействующих между собой автоматизированных и информационных систем различных объектов и субъектов информационного взаимодействия (разрыв информационного пространства взаимодействующих автоматизированных и информационных систем, представляющий собой по своей сути фактически разрыв внутреннего содержания баз и банков данных этих систем в местах размещения их баз и банков данных, подробно и детально рассмотрен в работе.

Главной причиной цифрового разрыва различных социальных групп населения (а практически основной массы социально и производственно активного населения страны) с различными возможностями доступа к информационным технологиям и их использованию при реализации процессов своей жизнедеятельности, является, прежде всего, чрезвычайно низкий уровень жизни большинства населения нашей страны в целом.

И для преодоления этой стороны проблемы цифрового разрыва должно быть обеспечено, в качестве главного фактора и условия, существенное повышение жизненного уровня большинства социально и производственно активного населения страны до уровня, на котором оно будет способно стать активным субъектом информационного общества.

Четвертой же ключевой проблемой становления и развития информационного общества для любой страны, и для нашей в том числе, является проблема разработки принципиально новой технологии формирования новых знаний - как базовой фундаментальной основы информационного общества.

1.10 Лекция № 10 (2 часа)

Тема: «Изучение структуры системы ИБ»

1.10.1 Вопросы лекции:

1.Концептуальные положения ООИБ.
2.Концепции национальной безопасности РФ.

1.10.2 Краткое содержание вопросов:

1.Концептуальные положения ООИБ

Примечательная особенность нынешнего периода - переход от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергические ресурсы. Ресурсами, как известно, называют элементы экономического потенциала, которыми располагает общество и которое при необходимости могут быть использованы для достижения конкретной цели хозяйственной деятельности. Давно стали привычными и общеупотребительными такие категории, как материальные, финансовые, трудовые, природные ресурсы, которые вовлекаются в хозяйственный оборот, и их назначение понятно каждому. Но вот появилось понятие "информационные ресурсы", и хотя оно узаконено, но осознано пока еще недостаточно. Информационные ресурсы - отдельные документы и отдельные массивы, документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Информационные ресурсы являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учету и защите, так как информацию можно использовать не только для товаров и услуг, но и превратить ее в наличность, продав кому-нибудь, или, что еще хуже, уничтожить. Собственная информация для производителя представляет значительную ценность, так как нередко получение (создание) такой информации - весьма трудоемкий и дорогостоящий процесс. Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами.

Особое место отводится информационным ресурсам в условиях рыночной экономики.

Важнейшим фактором рыночной экономики выступает конкуренция. Побеждает тот, кто лучше, качественнее, дешевле и оперативнее (ВРЕМЯ-ДЕНЬГИ!!!) производит и продает. В сущности это универсальное правило рынка. И в этих условиях основным выступает правило: кто владеет информацией, тот владеет миром.

В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. Установлено, что 47% охраняемых сведений добывается с помощью технических средств промышленного шпионажа.

В этих условиях защите информации от неправомерного овладения ею отводится весьма значительное место. При этом "целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым

сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения".

Как видно из этого определения целей защиты, информационная безопасность - довольно емкая и многогранная проблема, охватывающая не только определение необходимости защиты информации, но и то, как ее защищать, от чего защищать, когда защищать, чем защищать и какой должна быть эта защита.

Основное внимание уделяется защите конфиденциальной информации, с которой большей частью встречаются предприниматели негосударственного сектора экономики. Люди осознают и отдают себе отчет в сложности проблемы защиты информации вообще, и с помощью технических средств в частности. Тем не менее взгляд на эту проблему излагается на этом Web-сайте, считается, что этим охватывается не все аспекты сложной проблемы, а лишь определенные ее части.

Концепция информационной безопасности

1. Основные концептуальные положения системы защиты информации
2. Концептуальная модель информационной безопасности
3. Угрозы конфиденциальной информации
4. Действия, приводящие к неправомерному овладению конфиденциальной информацией

2.Концепции национальной безопасности РФ

Концепция национальной безопасности 10 января 2000 года утратила свою юридическую силу и была преобразована в Стратегию национальной безопасности РФ, утвержденную Президентом 12 мая 2009 года. Новый документ действует до 2020 года. Необходимость создания нового документа была озвучена в 2008 году, в период вооруженного противостояния в Южной Осетии.

Основные задачи концепции (стратегии) национальной безопасности РФ

Главные задачи составления и реализации стратегии следующие:

- мобилизировать развитие российской экономики и повысить активность внешнеторговых взаимоотношений;
- улучшить общее качество жизни граждан РФ, обеспечить им стабильную заработную плату и пенсии;
- обеспечить политическую стабильность;
- укрепить все сферы правопорядка страны, обеспечить государственную безопасность и оборону;
- повысить престиж РФ на мировой арене и ее конкурентоспособность экономики.

Разделы концепции (стратегии) национальной безопасности РФ

Документ состоит из нескольких основных разделов:

1. Общие положения

В разделе раскрываются:

- основные тенденции развития государства в последние несколько лет,
- суть основных направлений в стратегических и национальных приоритетах,
- важность национальной стратегии, ее признания и всесторонней поддержки сто стороны сил обеспечения нацбезопансости;

- суть основных понятий – угроза национальной безопасности Российской Федерации, национальные интересы РФ, стратегические национальные приоритеты. Кроме этого, раскрывается суть таких определений, как система обеспечения национальной безопасности, средства обеспечения национальной безопасности и так далее.

1.11 Лекция № 12 (2 часа)

Тема: «Изучение нормативно-правовых документов»

1.11.1 Вопросы лекции:

1. Понятие и предмет информационной безопасности
2. Основные составляющие национальных интересов РФ в информационной сфере

1.11.2 Краткое содержание вопросов:

1. Понятие и предмет информационной безопасности

Информационная безопасность не имеет точного определения и, что совсем печально, не имеет в литературе единого предмета исследования. Каждым автором термин «информационная безопасность» определяется по своему, вызывая тем самым коллизии в понимании предмета.

Под предметом ИБ часто понимается область защиты информации на конфиденциальность, целостность и доступность. Это ошибочная трактовка достаточно распространена в литературе. Предмет информационной безопасности значительно шире, хотя бы из определений в нормативно-правовых документах «Информационная безопасность РФ — состояние защищенности ее национальных интересов в информационной сфере, определяющейся совокупностью сбалансированных интересов личности, общества и государства».

Определять «безопасность» через «защищенность» не совсем корректно, поскольку эти слова синонимы, а поэтому данные определения являются тавтологиями. Безопасность есть некоторое состояние объекта, которое можно определить, выделив соответствующие качественные характеристики. Поясним последнюю фразу. Говоря о безопасности вообще и информационной безопасности в частности, мы неявно подразумеваем некую целевую функцию существования объекта или субъекта и безопасность как способность эту функцию реализовать (в случае субъекта — безопасность деятельности). В этом случае состояние системы, характеризующееся способностью объектов и субъектов реализовать свои целевые функции, должно определять состояние ее защищенности. 2. Основные составляющие национальных интересов РФ в информационной сфере

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование

информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;

усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;

обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;

укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

гарантировать свободу массовой информации и запрет цензуры;

не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

2. Основные составляющие национальных интересов РФ в информационной сфере

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.В этих целях необходимо:

повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;

обеспечить защиту сведений, составляющих государственную тайну;

расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

2. Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной политики Российской Федерации;

угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;

противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

1.12Лекция № 12 (2 часа)

Тема: «Элементы теории права»

1.12.1 Вопросы лекции:

1.Система права.

2.Элементы системы права

1.12.2 Краткое содержание вопросов:

1.Система права

Система права — это внутренняя структура права (строение, организация), которая складывается объективным образом как отражение реально существующих и развивающихся общественных отношений.

Система права:

выражает существующую правовую действительность, не есть результат произвольных действий тех, кто создаст нормы права;

предопределена социальным строем общества и соответственно интересами и потребностями людей;

показывает, из каких частей, элементов состоит право и как они соотносятся между собой.

Исторически система права в разных государствах формировалась исходя из потребностей в регулировании некоторых групп наиболее важных, часто встречающихся отношений, которые нуждаются в стабилизации. Именно поэтому формируются группы норм права, регулирующих определенные родовые и видовые группы отношений.

Не следует смешивать понятия «система права» и «правовая система». В первом случае речь идет о внутреннем строении права, взятом в качестве отдельного явления, а во втором — о правовой организации всего общества, совокупности всех явлений юридического характера, существующих и функционирующих в государстве. Система права выступает лишь как часть правовой системы и отличается рядом признаков.

Система права едина, поскольку в образующих ее нормах отражается общая воля общества, государства; кроме того, нормы регулируют единые цели и задачи, прежде всего упорядочение общественных отношений. В то же время нормы права различаются по содержанию, сфере действия, формам выражения, предмету, средствам и способам метода правового регулирования и проч.

Несмотря на единство, правовые нормы могут противоречить друг другу по содержанию, напри м ер из-за того, что законодатель не учел при разработке нормы уже существующих на тот момент норм, из-за большого их массива.

Объективная природа системы права означает, что правовые нормы и другие образования системы права строятся по объективным критериям.

Структурные элементы системы права — это норма права, отрасль права, подотрасль права, институт права, субинститут.

Норма права — первичный элемент системы права. Правовые нормы регулируют не все общественные отношения, а те из них, которые государство, общество рассматривают как наиболее значимые, важные.

Отрасль права - совокупность однородных правовых норм, обособившихся внутри системы права и регулирующих определенный род общественных отношений. Род — широкое понятие, которое может включать довольно большое видовое разнообразие отношений. Отграничение норм по отраслям происходит по таким признакам, как предмет и метод правового регулирования.

2.Элементы системы права

В рамках ряда отраслей формируются подотрасли права. Подотрасль права – это крупная составная часть отрасли права, объединяющая группу однородных правовых институтов. Постепенно развиваясь, формирует новую самостоятельную отрасль права (конституционно-процессуальное, административно-процессуальное, авторское, патентное и т.д.).Критерии деления норм на отрасли и институты: - предмет правового регулирования;- метод правового регулирования. Предмет – определенный вид общественных отношений. Это содержательная сторона правовых норм. Метод правового регулирования – различные способы правового воздействия со стороны государства на общественные отношения. Существует два полярных метода:1) метод автономии (диспозитивный) представляет самим участником регулируемого правом возможность самостоятельно определять свое поведение в рамках закона (в гражданском, семейном, трудовом);2) авторитарный (императивный) основан на использовании властных правовых предписаний, которые устанавливают основания и порядок возникновения конкретных прав и обязанностей у участников правовых отношений (уголовное, административное, финансовое и т.д.).В литературе принято различать отрасли:- публичного;- частного;- конституционного;- административного;- уголовного;- процессуального права. Критерий: сфера интереса (частного или публично-правового). Субъект частный (его частная жизнь и в связи с этим права).Субъект публичный (гражданин, член публично – политической организации).

1. 13 Лекция № 13 (2 часа).

Тема: «Законодательство о Государственной тайне»

1.11.1 Вопросы лекции:

1. Государственная тайна
2. Система защиты государственной тайны

1.11.2 Краткое содержание вопросов:

1. Государственная тайна

В настоящем Законе используются следующие основные понятия:

государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

носители сведений, составляющих государственную тайну, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений;

доступ к сведениям, составляющим государственную тайну, - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Перечень сведений, составляющих государственную тайну, - совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством. (абзац введен Федеральным законом от 06.10.1997 N 131-ФЗ)

2. Система защиты государственной тайны

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Одним из важнейших направлений деятельности НТЦ «Фобос-НТ» является защита сведений, содержащих государственную тайну. Эта особая категория сведений требует мер, которые должны гарантировать надежную защиту от возможных угроз информационной безопасности. НТЦ «Фобос-НТ» организует и проводит полный цикл работ, связанных с проектированием, разработкой, производством и внедрением систем защиты информации. Качество и научно-технический уровень разработок отвечают всем требованиям и стандартам, предусмотренным на территории Российской Федерации.

В отношении сведений, составляющих государственную тайну, НТЦ «Фобос-НТ» предоставляет следующий комплекс действий по технической защите информации:

Экспертиза объектов информатизации на соответствие требованиям ФСТЭК России по защите информации;

Защита помещений (комнат для переговоров) от утечки речевой информации;

Защита телефонных переговоров;

Защита автоматизированных систем (ПЭВМ, компьютерных сетей), технических средств обработки и передачи информации от утечки по техническим каналам;

Защита ПЭВМ, вычислительных сетей от несанкционированного доступа;

Поставка компьютеров и другой оргтехники в защищенном исполнении по требуемой категории (классу) защиты:

прошедших специальную проверку (проверку на наличие внедренных электронных устройств съема информации);

прошедших специальные исследования (исследования на ПЭМИ, исследования на акустоэлектрические преобразования);

оснащенных средствами защиты от несанкционированного доступа;

Поставка, установка и настройка сертифицированных средств защиты информации;

Проведение специальных исследований основных технических средств (ОТСС), вспомогательных технических средств (ВТСС) на наличие технических каналов утечки информации.

1. 14 Лекция № 14 (2 часа)

Тема: «Изучение нормативно-правовых документов»

1.14.1 Вопросы лекции:

1.Защита информации при реализации информационных процессов.

2.Предотвращение и исправление неправильных действий пользователей

1.14.2 Краткое содержание вопросов:

1.Защита информации при реализации информационных процессов

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 подключения к каналам 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; криптографическая защита информации; идентификация и аутентификация пользователей и процессов и др. Технологические средства защиты информации - это комплекс мероприятий, органично встраиваемых в технологические процессы преобразования данных. Среди них: создание архивных копий носителей; ручное или автоматическое сохранение обрабатываемых файлов во внешней памяти компьютера; регистрация пользователей компьютерных средств в журналах; автоматическая регистрация доступа пользователей к тем или иным ресурсам; разработка специальных инструкций по выполнению всех технологических процедур и др. Идентификация - это присвоение какому-либо объекту или субъекту уникального имени или образа. Аутентификация - это установление подлинности, т.е. проверка, является ли объект (субъект) действительно тем, за кого он себя выдает. Конечная цель процедур идентификации и аутентификации объекта (субъекта) - допуск его к информации ограниченного пользования в случае положительной проверки либо отказ в допуске в случае отрицательного исхода проверки. Объектами идентификации и аутентификации могут быть: люди (пользователи, операторы и др.); технические средства (мониторы, рабочие станции, абонентские пункты); магнитные носители информации; документы (ручные, распечатки и др.); информация на экране монитора, табло и др. Один из наиболее распространенных методов аутентификации - присвоение лицу или другому имени пароля и хранение его значения в вычислительной системе. Пароль - это совокупность символов, определяющая объект (субъект). Для идентификации пользователей могут применяться сложные в плане технической реализации системы, обеспечивающие установление подлинности пользователя на основе анализа его индивидуальных параметров: отпечатков пальцев, рисунка линий руки, радужной оболочки глаз, тембра голоса и др. Компьютерный вирус - специи

2.Предотвращение и исправление неправильных действий пользователей

Одна из причин задержки в системе коммутации пакетов вызвана применением промежуточного накопления. Пакет, поступивший в коммутатор пакетов, помещается в очередь. Если пакеты поступают быстрее, чем может перенаправить коммутатор, очередь ожидающих пакетов будет большой и задержка может оказаться чрезмерной. Чрезмерные задержки могут привести к появлению ошибок, связанных с воздействием задержавшихся в очереди пакетов. Например, рассмотрим такую последовательность событий:

§ Два компьютера согласовывают между собой сеанс связи в 13:00.

§ Один компьютер отправляет последовательность из десяти пакетов на другой.

§ В результате сбоя аппаратного обеспечения пакет 3 задерживается.

§ Для установки нарушения передачи данных изменяются маршруты.

§ Программное обеспечение протокола компьютера-отправителя повторно передаёт пакет 3, и он вместе с остальными пакетами передается без ошибок.

§ В 13:05 оба компьютера снова согласовывают между собой сеанс обмена данными.

§ После прибытия второго пакета поступает задержанная копия пакета 3, принадлежащая к предыдущему сеансу связи.

§ Поступает пакет 3, принадлежащий ко второму сеансу связи.

К сожалению, если протокол не был тщательно спроектирован, то пакет из предыдущего сеанса связи может быть принят в следующем сеансе связи, а правильный пакет отброшен как дубликат.

Посторонние пакеты могут также появляться при передаче управляющих пакетов. Например, в протоколах часто применяется передача специальных управляющих пакетов для прекращения сеанса обмена данными. Получение копии запроса на разрыв связи из предыдущего сеанса может заставить программное обеспечение протокола преждевременно прервать текущий сеанс.

Для предотвращения воздействия пакетов, принадлежащих к другим сеансам, в протоколах предусматривается обозначение каждого сеанса уникальным идентификатором (например, с указанием времени установления сеанса), и эти уникальным идентификатором обозначается каждый пакет. Программное обеспечение протокола отбрасывает все поступившие пакеты, которые содержат неправильный идентификатор. Идентификатор не должен использоваться повторно до истечения достаточно большого интервала времени (например, нескольких часов).

Не все компьютеры работают с одинаковой скоростью. Если компьютер-отправитель передаёт данные по сети быстрее, чем может обрабатывать получатель, возникает переполнение данными, что приводит к их потере. Для устранения этой проблемы применяется несколько методов под общим названием управление потоком данных.

Одной из самых простейших форм управления потоком является передача с остановками. В этом случае отправитель ожидает разрешения на передачу каждого пакета. Когда получатель готов к приёму следующего пакета, он отправляет управляющее сообщение, обычно в форме подтверждения. Данный способ решает эту проблему, но использование этого метода может привести к крайне неэффективному использованию пропускной способности сети.

1. 15 Лекция № 15 (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.

1. 16Лекция № 16 (2 часа)

Тема: «Дисциплинарная и уголовная ответственность**»**

1.16.1 Вопросы лекции:

1. Дисциплинарная ответственность
2 Уголовная ответственность

1.16.2 Краткое содержание вопросов:

1. Дисциплинарная ответственность

Дисциплинарную ответственность – это один из видов юридической ответственности, который заключается в праве полномочного представителя работодателя применить к работнику, совершившему дисциплинарный проступок, предусмотренные законодательством меры дисциплинарного взыскания и в корреспондирующей данному праву обязанности работника, допустившего совершение дисциплинарного проступка, претерпеть установленные в законодательстве неблагоприятные последствия.

Существует два вида дисциплинарной ответственности: общая, предусмотренная ТК РФ, и специальная, которую несут работники в соответствии с требованиями федеральных законов, уставов и положений о дисциплине.

К общей дисциплинарной ответственности могут быть привлечены все лица, вступившие в соответствии с ТК РФ в трудовые отношения и получившие статус работников.

Специальная дисциплинарная ответственность отличается от общей дисциплинарной ответственности:

1) кругом лиц, на которых она распространяется;

2) более широким понятием дисциплинарного проступка, противоправность которого предусмотрена специальными федеральными законами, уставами и положениями о дисциплине;

3) специальными мерами дисциплинарного взыскания;

4) кругом должностных лиц и органов, наделенных дисциплинарной властью, и порядком применения дисциплинарных взысканий.

Специальную дисциплинарную ответственность несут работники, на которых распространяются помимо норм ТК РФ отдельные федеральные законы, уставы и

положения о дисциплине (например, Закон Российской Федерации от 26 июня 1992 г. N 3132-1 «О статусе судей в Российской Федерации»; Федеральный закон от 17 января 1992 г. N 2202-1 «О прокуратуре Российской Федерации» и др.). В этих нормативных правовых актах предусмотрены специальные меры дисциплинарного взыскания, как правило, более строгие, порядок их наложения, отмены, рассмотрения споров. К таким работникам относятся, например:

— судьи;

— прокурорские работники;

— государственные служащие;

— работники железнодорожного транспорта;

— работники организаций с особо опасным производством в области использования атомной энергии;

— другие категории работников (морского транспорта, речного транспорта и так далее).

За совершение дисциплинарного проступка, т.е. неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания (ст. 192 ТК РФ):

1) замечание;

2) выговор;

3) увольнение по соответствующим основаниям.

Федеральными законами, уставами и положениями о дисциплине (ч. 5 ст. 189 ТК РФ) для отдельных категорий работников могут быть предусмотрены также и другие дисциплинарные взыскания. Указанные нормативные акты касаются прежде всего государственных служащих, военнослужащих, лиц, работающих в каких-либо специализированных областях (транспорт, рыбная промышленность, добыча нефти и газа и т.п.).

2 Уголовная ответственность

В теории уголовного права многими авторами предлагается рассматривать уголовную ответственность в двух аспектах: в позитивном и в негативном.

Позитивная уголовная ответственность сводится к отсутствию нарушений запретов, установленных уголовным законом. Позитивная уголовная ответственность понимается как «обязанность соблюдать требования уголовного закона», «правовые требования», «выполнение должного», «социальный правовой долг». Правовым последствием данного вида ответственности является положительная уголовно-правовая оценка поведения лица со стороны государства, в том числе поощрение его действий]. По мнению сторонников теории позитивной ответственности, она проявляется, например, в том, что исключается уголовная ответственность за преступление, которое лицо не совершало; в освобождении от ответственности лица, добровольно отказавшегося от совершения преступления и т. д.

Негативная (или ретроспективная) уголовная ответственность связана с совершением лицом преступления (нарушением уголовного закона) и заключается в применяемых государством репрессивных мерах.

Деление уголовной ответственности на негативную и позитивную не является общепринятым в науке уголовного права. Отмечается, что позитивная уголовная ответственность не имеет большого правового значения, поскольку «перенесение понятия ответственности в область должного, толкуемого не как объективная реальность, а как определённый психологический процесс, лишает её правового содержания». Г. В. Назаренко указывает, что позитивная уголовная ответственность скорее является институтом морали, чем права.

Поэтому именно негативная уголовная ответственность имеет наибольшее теоретическое и практическое значение; в большинстве работ в рамках рассмотрения института уголовной ответственности (в том числе далее в настоящей статье) освещается исключительно этот её аспект.

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: «Системная концепция обеспечения безопасности объектов охраны**»**

3.1.1 Задание для работы:

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

2. Определение стратегии комплексной безопасности.

3.1.2 Краткое описание проводимого занятия:

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;

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.

3.1.3 Результаты и выводы:

Студент знакомится с основами обеспечения комплексной безопасности объектов и учится определять стратегию комплексной безопасности.

3.2 Практическое занятие № 2 (2 часа).

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

3.2.1 Задание для работы:

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

3.2.2 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;

3.2.3 Результаты и выводы:

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

3.3 Практическое занятие № 3 (2 часа).

Тема: «Цели и задачи СБО**»**

3.3.1 Задание для работы:

1.Принципы построения службы безопасности

2.Основные задачи службы безопасности

3.3.2 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;

3.3.3 Результаты и выводы:

Студент знакомится с основными принципами построения и основными задачами службы безопасности

3.4 Практическое занятие № 4 (2 часа).

Тема: «Функции и задачи СБ**»**

3.4.1 Задание для работы:

1.Функции службы безопасности

2.Задачи службы безопасности

3.4.2 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;

3.4.3 Результаты и выводы:

Студент знакомится с функциями службы безопасности и задачами службы безопасности

3.5 Практическое занятие № 5 (2 часа).

Тема: «Функции и задачи IT-отдела СБ**»**

3.5.1 Задание для работы:

1. Функции IT-отдела
2. Задачи IT-отдела

3.5.2 Краткое описание проводимого занятия:

1. Функции IT-отдела

В процессе производственной деятельности организации ИТ-отдел осуществляет следующие функции:

1. Приобретение: - активного сетевого оборудования; - серверов; - средств резервного копирования и восстановления данных; - средств защиты информации; - средств контроля и управления сетевой инфраструктурой; - периферийного оборудования; - вычислительной техники и комплектующих; - программного обеспечения; - расходных материалов и запасных частей к устройствам печати и офисной технике.

2. Установка, настройка, техническое сопровождение и обслуживание: - серверов; - активного сетевого оборудования; - аппаратных и программных средств защиты информации; - аппаратных и программных средств контроля и управления сетевой инфраструктурой; - средств резервного копирования и восстановления данных; -

рабочих станций; - периферийного оборудования; - программного обеспечения; - офисной техники.

3. Организация автоматизированных рабочих мест.

4. Диагностика и устранение неисправностей вычислительной и офисной техники.

5. Диагностика и устранение неполадок программного обеспечения.

Задачами ИТ-отдела являются:

1. реализация работ по обеспечению бесперебойного функционирования и развития программно-аппаратных комплексов;

2. обеспечение защиты сведений, составляющих коммерческую тайну, в процессе деятельности организации;

3. осуществление в соответствии с законодательством Российской Федерации работы по комплектованию, хранению, учету и использованию архивных документов, образовавшихся в процессе деятельности организации. 1. реализация концепции развития информационных систем;

4. обеспечение требуемого уровня информационной безопасности;

5. разработка стандартов на использование вычислительной техники и программного обеспечения;

6. обеспечение информационной и технической поддержки средств вычислительной техники и программного обеспечения;

7. проведение работ по оптимизации использования информационнотехнических ресурсов.

3.5.3 Результаты и выводы:

Студент знакомится с функциями и задачами IT-отдела СБ

3.6 Практическое занятие № 6 (2 часа)

Тема: «Организационная структура системы ОИБ**»**

3.6.1 Задание для работы:

1. Цели создания системы ОИБ
2. Основные понятия по ИБ

3.6.2 Краткое описание проводимого занятия:

Конечной *целью создания системы обеспечения безопасности информационных технологий* является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), наносимого субъектам информационных отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Основной задачей системы защиты является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) АС соответствующими множеству значимых угроз методами и средствами.

Обеспечение информационной безопасности - это непрерывный процесс, основное содержание которого составляет управление, - управление людьми, рисками, ресурсами, средствами защиты и т.п. Люди - обслуживающий персонал и конечные пользователи АС, - являются неотъемлемой частью автоматизированной (то есть *«человеко-машинной»)* системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и ее безопасность.

2. Технологии обеспечения информационной безопасности

Под *технологией обеспечения информационной безопасности в АС* понимается определенное распределение функций и регламентация порядка их исполнения, а также

порядка взаимодействия подразделений и сотрудников (должностных лиц) организации по обеспечению комплексной защиты ресурсов АС в процессе ее эксплуатации.

Требования к технологии управления безопасностью:

• соответствие современному уровню развития информационных 4; технологий;

• учет особенностей построения и функционирования различных подсистем АС;

• точная и своевременная реализация политики безопасности организации;

• минимизация затрат на реализацию самой технологии обеспечения безопасности.

Для реализации технологии обеспечения безопасности в АС необходимо:

• наличие полной и непротиворечивой правовой базы (системы взаимоувязанных нормативно - методических и организационно -распорядительных документов) по вопросам ОИБ;

3.6.3 Результаты и выводы:

Студент знакомится с организационной структурой системы ОИБ

3.7 Практическое занятие № 7 (2 часа)

Тема: «Работа с персоналом**»**

3.7.1 Задание для работы:

1. Проблемы безопасности коммерческих структур в работе с кадрам

3.7.2 Краткое описание проводимого занятия:

1. Проблемы безопасности коммерческих структур в работе с кадрам

Анализ сообщений средств массовой информации и оперативных сводок правоохранительных органов о последних диверсионно-террористических актах против коммерческих структур в Москве и других городах России позволяет сделать однозначный вывод о высокой степени осведомленности преступников относительно режима дня и динамики деятельности предпринимателей: жертв, как правило, неизменно встречали в районе проживания или места работы либо с предельной точностью по времени и месту перехватывали на трассе. Заблаговременно были изучены основные и запасные маршруты перемещения коммерсантов. Преступники располагали подробными сведениями о составе семьи и родственниках будущих жертв, марках и номерных знаках личных и служебных автомашин, соседях и т.п. Таким образом очевидно, что любые противоправные деяния, связанные с силовым воздействием на коммерческие структуры, тщательно планируются и, следовательно, состоят из нескольких последовательных этапов, среди которых вторжения, хищения, вооруженные нападения являются фактически финальными акциями преступников.

В этой связи современная система мер безопасности должна быть ориентирована на то, чтобы прогнозировать и выявлять признаки вероятных правонарушений, а тем более преступлений на ранних стадиях, на этапе формирования умысла и разработки криминальными сообществами планов преступных действий, что позволяет предупредить и предотвратить подобного рода деяния.

Неотъемлемым составляющим элементом любой планируемой преступной акции является сбор информации. Представляется возможным выделить следующие основные методы, которые используются злоумышленниками в настоящее время для добывания сведений о коммерческих структурах:

наблюдение, в т.ч. с помощью мобильных и стационарных оптико-технических средств, скрытое фотографирование, видеозапись; выведывание информации; хищения каких-либо внутренних документов лицами, внедренными или приобретенными в коммерческих структурах, которые согласились или оказались вынужденными осуществлять указанные действия по корыстным побуждениям, в результате угроз, по физическому принуждению либо по иным причинам;

перехват информации на различных каналах внутренней и внешней связи коммерческих структур;

3.7.3 Результаты и выводы:

Студент знакомится с проблемой безопасности коммерческих структур в работе с кадрам

3.8 Практическое занятие № 8 (2 часа)

Тема: «ИТЗ информации**»**

3.8.1 Задание для работы:

1. Защита интеллектуальной собственности в интернете

3.8.2 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?

3.8.3 Результаты и выводы:

Студент знакомится с защитой интеллектуальной собственности в интернете

3.9 Практическое занятие № 9 2 часа)

Тема: «Информационное общество и его безопасность**»**

3.9.1 Задание для работы:

1. Разработка политики безопасности

3.9.2 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.

3.9.3 Результаты и выводы:

Студент знакомится с разработкой политики безопасности

3.10 Практическое занятие № 10 (2 часа).

Тема: «Изучение структуры системы ИБ **»**

3.10.1 Задание для работы:

1. Рассмотреть концепцию национальной безопасности РФ.

3.10.2 Краткое описание проводимого занятия:

Главные задачи составления и реализации стратегии следующие:

- мобилизовать развитие российской экономики и повысить активность внешнеторговых взаимоотношений;
- улучшить общее качество жизни граждан РФ, обеспечить им стабильную заработную плату и пенсии;
- обеспечить политическую стабильность;
- укрепить все сферы правопорядка страны, обеспечить государственную безопасность и оборону;
- повысить престиж РФ на мировой арене и ее конкурентоспособность экономики.

Разделы концепции (стратегии) национальной безопасности РФ

Документ состоит из нескольких основных разделов:

1. Общие положения

В разделе раскрываются:

- основные тенденции развития государства в последние несколько лет,
- суть основных направлений в стратегических и национальных приоритетах,
- важность национальной стратегии, ее признания и всесторонней поддержки сто стороны сил обеспечения нацбезопасности;
- суть основных понятий – угроза национальной безопасности Российской Федерации, национальные интересы РФ, стратегические национальные приоритеты. Кроме этого, раскрывается суть таких определений, как система обеспечения национальной безопасности, средства обеспечения национальной безопасности и так далее.

3.10.3 Результаты и выводы:

Студент знакомится с концепцией национальной безопасности РФ

3.11 Практическое занятие №11 (2 часа)

Тема: «Изучение нормативно-правовых документов**»**

3.11.1 Задание для работы:

1. Изучить основные составляющие национальных интересов РФ в информационной сфере

3.11.2 Краткое описание проводимого занятия:

Основные составляющие национальных интересов РФ в информационной сфере

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.В этих целях необходимо:

повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

3.11.3 Результаты и выводы:

Студент знакомится с основными составляющими национальных интересов РФ в информационной сфере

3.12 Практическое занятие №12 (2 часа).

Тема: «Элементы теории права**»**

3.12.1 Задание для работы:

1. Рассмотреть основные элементы системы права

3.12.2 Краткое описание проводимого занятия:

В рамках ряда отраслей формируются подотрасли права. Подотрасль права – это крупная составная часть отрасли права, объединяющая группу однородных правовых институтов. Постепенно развиваясь, формирует новую самостоятельную отрасль права (конституционно-процессуальное, административно-процессуальное, авторское, патентное и т.д.).Критерии деления норм на отрасли и институты: - предмет правового регулирования;- метод правового регулирования. Предмет – определенный вид общественных отношений. Это содержательная сторона правовых норм. Метод правового

регулирования – различные способы правового воздействия со стороны государства на общественные отношения. Существует два полярных метода:1) метод автономии (диспозитивный) представляет самим участником регулируемого правом возможность самостоятельно определять свое поведение в рамках закона (в гражданском, семейном, трудовом);2) авторитарный (императивный) основан на использовании властных правовых предписаний, которые устанавливают основания и порядок возникновения конкретных прав и обязанностей у участников правовых отношений (уголовное, административное, финансовое и т.д.).В литературе принято различать отрасли:- публичного;- частного;- конституционного;- административного;- уголовного;- процессуального права. Критерий: сфера интереса (частного или публично-правового). Субъект частный (его частная жизнь и в связи с этим права).Субъект публичный (гражданин, член публично – политической организации).

3.12.3 Результаты и выводы:

Студент знакомится с основными элементами системы права

3.13 Практическое занятие №13 (2 часа).

Тема: «Законодательство о Государственной тайне**»**

3.13.1 Задание для работы:

1. Рассмотреть систему защиты государственной тайны

3.13.2 Краткое описание проводимого занятия:

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Одним из важнейших направлений деятельности НТЦ «Фобос-НТ» является защита сведений, содержащих государственную тайну. Эта особая категория сведений требует мер, которые должны гарантировать надежную защиту от возможных угроз информационной безопасности. НТЦ «Фобос-НТ» организует и проводит полный цикл работ, связанных с проектированием, разработкой, производством и внедрением систем защиты информации. Качество и научно-технический уровень разработок отвечают всем требованиям и стандартам, предусмотренным на территории Российской Федерации.

В отношении сведений, составляющих государственную тайну, НТЦ «Фобос-НТ» предоставляет следующий комплекс действий по технической защите информации:

Экспертиза объектов информатизации на соответствие требованиям ФСТЭК России по защите информации;

Защита помещений (комнат для переговоров) от утечки речевой информации;

Защита телефонных переговоров;

Защита автоматизированных систем (ПЭВМ, компьютерных сетей), технических средств обработки и передачи информации от утечки по техническим каналам;

Защита ПЭВМ, вычислительных сетей от несанкционированного доступа;

Поставка компьютеров и другой оргтехники в защищенном исполнении по требуемой категории (классу) защиты:

прошедших специальную проверку (проверку на наличие внедренных электронных устройств съема информации);

прошедших специальные исследования (исследования на ПЭМИ, исследования на акустоэлектрические преобразования);

оснащенных средствами защиты от несанкционированного доступа;

Поставка, установка и настройка сертифицированных средств защиты информации;

Проведение специальных исследований основных технических средств (ОТСС), вспомогательных технических средств (ВТСС) на наличие технических каналов утечки информации.

3.13.3 Результаты и выводы:

Студент знакомится с системой защиты государственной тайны

3.14 Практическое занятие № 14 (2 часа).

Тема: «Изучение нормативно-правовых документов**»**

3.14.1 Задание для работы:

1.Защита информации при реализации информационных процессов.

2.Предотвращение и исправление неправильных действий пользователей

3.14.2 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

3.14.3 Результаты и выводы:

Студент знакомится с угрозой конфиденциальной информации

3.15 Практическое занятие №15 (2 часа)

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

3.15.1 Задание для работы:

1.Сфера действия настоящего Федерального закона

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

3.15.2 Краткое описание проводимого занятия:

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.

(в ред. Федерального закона от 29.12.2015 N 393-ФЗ)

(см. текст в предыдущей редакции)

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.

3.15.3 Результаты и выводы:

Студент знакомится с законом «Об информации, информационных технологиях и о защите информации

3.16 Практическое занятие №16 (2 часа)

Тема: «Дисциплинарная и уголовная ответственность**»**

3.16.1 Задание для работы:

1. Дисциплинарная ответственность
2 Уголовная ответственность

3.16.2 Краткое описание проводимого занятия:

Дисциплинарную ответственность – это один из видов юридической ответственности, который заключается в праве полномочного представителя работодателя применить к работнику, совершившему дисциплинарный проступок, предусмотренные законодательством меры дисциплинарного взыскания и в корреспондирующей данному праву обязанности работника, допустившего совершение дисциплинарного проступка, претерпеть установленные в законодательстве неблагоприятные последствия.

Существует два вида дисциплинарной ответственности: общая, предусмотренная ТК РФ, и специальная, которую несут работники в соответствии с требованиями федеральных законов, уставов и положений о дисциплине.

К общей дисциплинарной ответственности могут быть привлечены все лица, вступившие в соответствии с ТК РФ в трудовые отношения и получившие статус работников.

Специальная дисциплинарная ответственность отличается от общей дисциплинарной ответственности:

1) кругом лиц, на которых она распространяется;

2) более широким понятием дисциплинарного проступка, противоправность которого предусмотрена специальными федеральными законами, уставами и положениями о дисциплине;

3) специальными мерами дисциплинарного взыскания;

4) кругом должностных лиц и органов, наделенных дисциплинарной властью, и порядком применения дисциплинарных взысканий.

Специальную дисциплинарную ответственность несут работники, на которых распространяются помимо норм ТК РФ отдельные федеральные законы, уставы и положения о дисциплине (например, Закон Российской Федерации от 26 июня 1992 г. N 3132-1 «О статусе судей в Российской Федерации»; Федеральный закон от 17 января 1992 г. N 2202-1 «О прокуратуре Российской Федерации» и др.). В этих нормативных правовых актах предусмотрены специальные меры дисциплинарного взыскания, как правило, более строгие, порядок их наложения, отмены, рассмотрения споров. К таким работникам относятся, например:

— судьи;

— прокурорские работники;

— государственные служащие;

— работники железнодорожного транспорта;

— работники организаций с особо опасным производством в области использования атомной энергии;

— другие категории работников (морского транспорта, речного транспорта и так далее).

За совершение дисциплинарного проступка, т.е. неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания (ст. 192 ТК РФ):

1) замечание;

2) выговор;

3) увольнение по соответствующим основаниям.

2 Уголовная ответственность

В теории уголовного права многими авторами предлагается рассматривать уголовную ответственность в двух аспектах: в позитивном и в негативном.

Позитивная уголовная ответственность сводится к отсутствию нарушений запретов, установленных уголовным законом. Позитивная уголовная ответственность понимается как «обязанность соблюдать требования уголовного закона», «правовые требования», «выполнение должного», «социальный правовой долг». Правовым последствием данного вида ответственности является положительная уголовно-правовая оценка поведения лица со стороны государства, в том числе поощрение его действий]. По мнению сторонников теории позитивной ответственности, она проявляется, например, в том, что исключается уголовная ответственность за преступление, которое лицо не совершало; в освобождении от ответственности лица, добровольно отказавшегося от совершения преступления и т. д.

Негативная (или ретроспективная) уголовная ответственность связана с совершением лицом преступления (нарушением уголовного закона) и заключается в применяемых государством репрессивных мерах.

Деление уголовной ответственности на негативную и позитивную не является общепринятым в науке уголовного права. Отмечается, что позитивная уголовная ответственность не имеет большого правового значения, поскольку «перенесение понятия ответственности в область должного, толкуемого не как объективная реальность, а как определённый психологический процесс, лишает её правового содержания». Г. В. Назаренко указывает, что позитивная уголовная ответственность скорее является институтом морали, чем права.

Поэтому именно негативная уголовная ответственность имеет наибольшее теоретическое и практическое значение; в большинстве работ в рамках рассмотрения института уголовной ответственности (в том числе далее в настоящей статье) освещается исключительно этот её аспект.

3.16.3 Результаты и выводы:

Студент знакомится с ответственностью за нарушение законодательства