МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению практических работ
по дисциплине
«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск
2025

ВВЕДЕНИЕ

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Организационно-правовое обеспечение информационной безопасности» является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по правовому регулированию отношений в информационной сфере, по обеспечению защиты сведений ограниченного доступа от утечки по техническим каналам, разглашения, несанкционированного доступа на объектах информатизации и в выделенных помещениях, а также по формированию навыков работы в области защиты информации.

Задачами дисциплины являются:

1. Ознакомление с основами правового регулирования отношений в информационной сфере;
2. Ознакомление с конституционными гарантиями прав граждан на получение информации и механизмом их реализации,
3. Изучение понятий и видов защищаемой информации по законодательству РФ,
4. Изучение системы защиты государственной тайны,
5. Ознакомление с основами правового регулирования отношений в области интеллектуальной собственности; способами защиты этой собственности,
6. Изучение понятия и видов компьютерных преступлений;
7. Обучение основам организации обеспечения защиты информации на объектах информатизации и в выделенных помещениях;
8. Формирование практических навыков работы в области защиты информации.

2.Наименование практических занятий

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
6 семестр			
1	Практическая работа№1. Предмет информационного права в информационной безопасности	4	
2	Практическая работа№2 Общая характеристика законодательства российскойфедерации в области информационной безопасности	4	
3	Практическая работа№3 Правовое обеспечение защиты государственной тайны	2	
4	Практическая работа№4 Система защиты государственной тайны	4	
5	Практическая работа№ 5 Правовое обеспечение защиты банковской,профессиональной и служебной тайны	2	
6	Практическая работа№6 Правовое обеспечение защиты банковской, профессиональной и служебной тайны	4	
7	Практическая работа№ 7 Правовое обеспечение защиты коммерческой тайны	4	
8	Практическая работа№ 8 Правовое обеспечение	4	

	защиты персональных данных		
9	Практическая работа№ 9. Правовое обеспечение защиты интеллектуальнойсобственности	4	
	Итого за 6 семестр	**32**	
7 семестр			
1	Практическая работа№ 1. Предмет информационного права в информационной безопасности	4	
2	Практическая работа№ 2. Система обеспечения информационной безопасности	4	
3	Практическая работа№ 3. Организационные структуры системы обеспечения безопасности информации	4	
4	Практическая работа№ 4. Разработка модели информационных потоков предприятия (организации) с использованием программного комплекса гриф-2006	4	
5	Практическая работа№ 5. Организация режимов безопасности	4	
6	Практическая работа№ 6. Организация работы с персоналом	4	
7	Практическая работа№ 7. Исследование юридической ответственности	4	
8	Практическая работа№ 8. Борьба с компьютерными преступлениями	2	
9	Практическая работа№ 9. Борьба с компьютерными преступлениями	2	
10	Практическая работа№ 10. Организация защиты прав	2	
11	Практическая работа№ 11. Организация защиты прав	2	
	Итого за 7 семестр	**36**	
	Итого	**68**	

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1. 2

Предмет информационного права в информационной безопасности

Предмет информационного права в информационной безопасности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Право – это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Законодательство Российской Федерации представляет собой совокупность Конституции и принимаемых в соответствии с ней законов и подзаконных актов.

Внутреннее строение системы права РФ можно представить в вертикальном и горизонтальном срезах.

Вертикальное строение права – совокупность элементов, включающих: отрасль, подотрасль, институт, субинститут и правовое предписание.

Горизонтальное строение права позволяет увидеть все отрасли, его составляющие. Если их классифицировать, то можно выделить две группы отраслей.

В первую группу объединяются **регулятивные отрасли права**, т. е. отрасли, в которых основной упор делается на установление прав и обязанностей участников правоотношений.

Вторую группу отраслей составляют **охранительные отрасли права**, основной задачей которых является защита правоотношений.

Структура правоотношений и виды юридической ответственности

Правоотношение – это такое общественное отношение, в котором стороны связаны между собой взаимными юридическими правами и обязанностями, охраняемыми государством. Правоотношение есть та мера

внешней свободы, которая предоставляется его участникам нормами позитивного (писаного) права.

Структура правового отношения имеет четыре необходимых элемента: субъекты, объект, право и обязанность:

Субъекты правоотношений – это отдельные индивиды и организации, которые в соответствии с нормами права являются носителями юридических прав и обязанностей. В реальной жизни не все индивиды и организации могут быть субъектами правоотношений, например, малолетние дети, душевнобольные, организации, прекратившие свое существование, фактически не могут участвовать в правоотношениях по понятным причинам.

Мера участия субъектов в правовых отношениях определяется их правоспособностью и дееспособностью.

Правоспособность – это способность субъекта иметь юридические права и нести юридические обязанности. Она начинается с момента рождения индивида и прекращается смертью. Однако чтобы стать реальным участником правоотношения, правоспособный субъект должен быть дееспособным.

Дееспособность – это способность субъекта самостоятельно, своими действиями осуществлять юридические права и нести обязанности.

1. **Объект правоотношений** – это то, на что воздействует правоотношение. Объектом правоотношения является фактическое поведение его участников. В соответствии с содержанием субъективного права и юридической обязанности участники правоотношения строят свое поведение. Вступая в правоотношения, субъекты удовлетворяют определенные материальные, духовные и иные потребности (например, приобретают вещи, пользуются авторскими правами, правами изобретателя). Объектом правоотношений выступает поведение людей, которое может быть различным по содержанию.
2. **Субъективное право –** это предоставляемая и охраняемая государством возможность (свобода) субъекта по своему усмотрению удовлетворять те интересы, которые предусмотрены позитивным правом. Право, принадлежащее субъекту, называется субъективным потому, что только от воли субъекта зависит, как им распорядиться. Это возможность не произвольная, а правовая, устанавливающая меру дозволенного поведения.
3. **Юридическая обязанность –** это предусмотренная законодательством и охраняемая государством необходимость должного поведения участника правового отношения в интересах управомоченного субъекта (индивида, организации, государства в целом). Если содержание субъективного права образует мера дозволенного поведения, то содержание обязанности – мера

должного, необходимого поведения в правоотношении.

Юридическая ответственность – это применение к правонарушителю предусмотренных санкцией юридической нормы мер государственного принуждения, выражающихся в форме лишений личного, организационного либо имущественного характера. Фактическим основанием для юридической ответственности является правонарушение. Лицо может быть привлечено к ответственности только при наличии в его действии всех элементов состава правонарушения.

Состав правонарушения состоит из четырех составляющих:

- **объект правонарушения** – область общественных отношений, регулируемых и охраняемых правом, в котором произошло деяние и (или) которой данным деянием причинен вред;
- **объективная сторона** – характеристика деяния, способа его совершения (группой, с применением оружия, систематически, повторно), обстоятельств (во время военных действий, стихийных бедствий и т. п.);
- **субъект** – лицо, которое совершило правонарушение, характеристика правонарушителя;
- **субъективная сторона** – форма вины (умысел или неосторожность).

Само по себе правонарушение не порождает автоматически возникновения ответственности, а является лишь основанием для такого применения. Для реального же осуществления юридической ответственности необходим **правоприменительный акт** – решение компетентного органа, который возлагает юридическую ответственность, устанавливает объем и форму принудительных мер к конкретному лицу. Это может быть приговор суда, приказ администрации и т. п. Наибольшее распространение получило деление юридической ответственности по отраслевому признаку. По данному основанию различают ответственность *уголовную, административно-правовую, гражданско-правовую, дисциплинарную и материальную*.

Уголовная ответственность наступает за совершение преступлений и в отличие от других видов ответственности устанавливается только уголовным законом. Никакие иные нормативные акты не могут определять общественно опасные деяния как преступные и устанавливать за них меры ответственности. В Российской Федерации исчерпывающий перечень преступлений зафиксирован в Уголовном кодексе. Порядок привлечения к уголовной ответственности регламентируется Уголовно-процессуальным кодексом. Полномочиями привлечения к уголовной ответственности обладает только суд.

Административно-правовая ответственность наступает за совершение административных проступков, предусмотренных Кодексом об административных правонарушениях. Кроме того, этот вид ответственности может устанавливаться указами Президента Российской Федерации, постановлениями Правительства Российской Федерации и нормативными актами субъектов Федерации. Дела об административных правонарушениях рассматриваются компетентными органами государственной власти, круг которых закреплен в кодексе. Меры административного принуждения – предупреждение, штраф, лишение специального права, административный арест.

Гражданско-правовая ответственность наступает за нарушения договорных обязательств имущественного характера или за причинение имущественного внедоговорного вреда. Ее сущность состоит в принуждении лица нести отрицательные имущественные последствия. Полное возмещение вреда – основной принцип гражданско-правовой ответственности (статья 1064 ГК). Возмещение убытков в некоторых случаях дополняется штрафными санкциями, например, выплатой неустойки.

Дисциплинарная ответственность возникает вследствие совершения дисциплинарных проступков. Привлекать к дисциплинарной ответственности может руководитель, осуществляющий распорядительно-дисциплинарную власть над конкретным работником. Меры дисциплинарной ответственности – выговор, строгий выговор, отстранение от занимаемой должности и т. п.

Материальная ответственность рабочих и служащих за ущерб, нанесенный предприятию, учреждению, заключается в необходимости возместить ущерб в порядке, установленном законом. Основанием этого вида ответственности является нанесение ущерба во время работы предприятию, с которым работник находится в трудовых отношениях. Размер возмещаемого ущерба определяется в процентах к заработной плате (1/3, 2/3 месячного заработка).

Информационное законодательство – это совокупность норм права, регулирующих общественные отношения в информационной сфере.

Предметом правового регулирования в информационной сфере являются:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация права на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;

- создание и применение средств информационной безопасности.

В целях реализации этих прав и свобод принимаемые законодательные акты устанавливают гарантии, обязанности, механизмы защиты и ответственность.

Информационное законодательство имеет вертикальную (по видам правовых актов) и горизонтальную (по отраслям законодательства) структуру.

Вертикальная структура строится исходя из принципа «верховенства закона»: нормы вышестоящего по иерархии акта обладают более высокой юридической силой и являются определяющими для соответствующих норм всех нижестоящих актов.

Структура информационного законодательства как комплексной отрасли включает в себя:

- Международные акты информационного законодательства.
- Информационно-правовые нормы Конституции РФ.
- Отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства.
- Отрасли законодательства, акты которых включают отдельные информационно-правовые нормы.

Совокупность вышеперечисленных документов составляет правовую базу, обеспечивающую нормативное регулирование процессов информационного обмена, в том числе и защиту информации.

Информация имеет ряд особенностей, отличающих ее от других видов товаров:

- нематериальность (идеальность) информации;
- информационный продукт подвергается только моральному износу;
- информация находится на материальном носителе;
- информация не исчезает при потреблении и может быть использована многократно;
- производство информации требует значительных затрат по сравнению с затратами на тиражирование;
- при копировании количество информации не изменяется, а цена снижается.

Основные определения в области информационного права:

Информация – это сведения о лицах, предметах, фактах, явлениях, процессах независимо от формы их представления.

Документированная информация – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Объект правоотношений – это то, на что воздействуют правоотношения. **Субъект правоотношений** – предоставленная и охраняемая государством возможность субъекта по своему усмотрению удовлетворять потребности,
предусмотренные позитивным правом.

Юридическая ответственность – применение предусмотренных санкций, юридических норм, мер государственного принуждения.

Юридические обязанности – предусмотренная законодательством и охраняемая государством необходимость должностного поведения участника правоотношений.

Правовые принципы защиты информации:

- полнота правового регулирования;
- принципы единства нормативно-правовой базы;
- непротиворечивость законодательной базе;
- принцип соблюдения рациональных пропорций между правовыми и технико-юридическими нормами;
- нормативно-правовые акты должны предусматривать развернутую защиту прав граждан.

Контрольные вопросы

1. Дайте определение понятию «право».
2. Назовите и охарактеризуйте способы представления внутреннего строения системы права Российской Федерации.
3. Дайте определение понятию «правоотношение».
4. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
5. Чем определяется мера участия субъектов в правовых отношениях?

6. Назовите и охарактеризуйте составляющие состава правонарушения.
7. Назовите и охарактеризуйте виды юридической ответственности.
8. Что является предметом правового регулирования в информационной сфере?
9. Охарактеризуйте вертикальную структуру информационного законодательства.
10. Перечислите особенности информации, отличающие ее от других видов товаров.
11. Перечислите правовые принципы защиты информации.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3-4.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3-4

Общая характеристика законодательства российской федерации в области информационной безопасности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

В настоящее время с учетом сложившейся практики обеспечения информационной безопасности принято выделять следующие направления защиты информации:

- *правовая защита* – это специальные законы и другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- *организационная защита* – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;
- *инженерно-техническая защита* – это использование различных технических средств, препятствующих нанесению ущерба.

Правовое обеспечение информационной безопасности любой страны
содержит как международные, так и национальные правовые нормы. В нашей стране правовые или законодательные основы обеспечения информационной безопасности составляют Конституция РФ, Законы РФ, Кодексы, Указы и другие нормативные акты, регулирующие отношения в области информации.

Правовая защита информации как ресурса признана на международном уровне и определяется межгосударственными договорами, конвенциями,
декларациями, реализуется правовыми механизмами защиты патентных и авторских прав.

В реализации государственной политики в сфере информатизации участвуют следующие структуры власти:

- Президент Российской Федерации;
- Совет Федерации;

- Государственная дума Федерального собрания Российской Федерации;
- Правительство Российской Федерации;
- Совет безопасности Российской Федерации;
- федеральные органы исполнительной власти;
- органы государственной власти Российской Федерации;
- органы местного самоуправления.

Совет безопасности Российской Федерации рассматривает наиболее важные вопросы, связанные с безопасностью Российской Федерации в современном мире, в том числе и вопросы информационной безопасности.

Структуру аппарата системы безопасности Российской Федерации составляют:

- Управление информационной безопасности и стратегического прогнозирования;
- Межведомственная комиссия Совета безопасности Российской Федерации по информационной безопасности.

В Государственной думе Российской Федерации функционируют:

- Комитет по информационной политике и связи;
- Комитет по безопасности, составной частью которого является комитет по информационной безопасности.

На внутригосударственном уровне правовая защита регулируется государственными и ведомственными актами. Государственными актами являются Конституция РФ, законы РФ, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями.

Информационное законодательство – совокупность норм права, регулирующих общественные отношения в информационной среде.

Предметом правового регулирования в информационной среде являются:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация прав граждан на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;
- создание и применение средств информационной безопасности.

Таким образом, законодательство по информационной безопасности является неотъемлемой частью всей системы законов Российской Федерации.

Федеральный закон «Об информации, информационных технологиях и о защите информации»

Со дня вступления в силу Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» утратили силу Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» и Федеральный закон от 04 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене».

Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Термины, используемые в законе, их определения

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким- либо признакам.

Доступ к информации – возможность получения информации и ее использования.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Предоставление информации – действия, направленные на получение

информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

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.

Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Важнейшие задачи обеспечения информационной безопасности Российской Федерации:

1. Противодействие угрозе развязывания противоборства в информационной сфере.
2. Реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности.
3. Совершенствование и защита отечественной информационной структуры, интеграция России в мировое информационное пространство.

Доктрина информационной безопасности РФ развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере и служит основой для:

1) формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
2) подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
3) разработки целевых программ обеспечения информационной безопасности Российской Федерации.

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.

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.

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.

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.

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.

Федеральный закон «О техническом регулировании»

Федеральный закон «О техническом регулировании» от 27 декабря 2002 года № 184-ФЗ регулирует отношения, возникающие при:

1) разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;
2) разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
3) оценке соответствия продукции установленным законодательством требованиям.

Требования к функционированию единой сети связи Российской Федерации и к продукции, связанные с обеспечением целостности,
устойчивости функционирования указанной сети связи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра,
соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи.

Действие закона не распространяется на государственные
образовательные стандарты, положения (стандарты) о бухгалтерском учете и правила (стандарты) аудиторской деятельности, стандарты эмиссии ценных бумаг и проспектов эмиссии ценных бумаг.

Термины, используемые в законе, их определения

Аккредитация – официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия.

Безопасность продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации – состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц,
государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений.

Декларирование соответствия – форма подтверждения соответствия продукции требованиям технических регламентов.

Декларация о соответствии – документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов.

Заявитель – физическое или юридическое лицо, осуществляющее обязательное подтверждение соответствия.

Знак обращения на рынке – обозначение, служащее для информирования приобретателей о соответствии выпускаемой в обращение продукции требованиям технических регламентов.

Знак соответствия – обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту.

Идентификация продукции – установление тождественности характеристик продукции ее существенным признакам.

Контроль (надзор) за соблюдением требований технических регламентов – проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки.

Международный стандарт – стандарт, принятый международной организацией.

Национальный стандарт – стандарт, утвержденный национальным органом Российской Федерации по стандартизации.

Орган по сертификации – юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации.

Оценка соответствия – прямое или косвенное определение соблюдения требований, предъявляемых к объекту.

Подтверждение соответствия – документальное удостоверение соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

Продукция – результат деятельности, представленный в материально-вещественной форме и предназначенный для дальнейшего использования в хозяйственных и иных целях.

Риск – вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда.

Сертификация – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

Сертификат соответствия – документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров.

Система сертификации – совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом.

Стандарт – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

Стандартизация – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Техническое регулирование – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия.

Технический регламент – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации).

Форма подтверждения соответствия – определенный порядок документального удостоверения соответствия продукции или иных объектов, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров.

Закон Российской Федерации «О безопасности»

Закон РФ «О безопасности» от 5 марта 1992 года № 2446-1 закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Термины, используемые в законе, их определения

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К основным объектам безопасности относятся:

1)личность – ее права и свободы;

2)общество – его материальные и духовные ценности;

3)государство – его конституционный строй, суверенитет и территориальная целостность.

Субъект обеспечения безопасности – государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей. Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством Российской Федерации, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, определяет содержание деятельности по обеспечению внутренней и внешней безопасности.

Принципы обеспечения безопасности

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации разрабатывается система правовых норм, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом образуются государственные органы обеспечения безопасности.

При обеспечении безопасности не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом.

Граждане, общественные и иные организации и объединения имеют право получать разъяснения по поводу ограничения их прав и свобод от органов, обеспечивающих безопасность. По их требованию такие разъяснения даются в письменной форме в установленные законодательством сроки.

Должностные лица, превысившие свои полномочия в процессе деятельности по обеспечению безопасности, несут ответственность в соответствии с законодательством.

Контрольные вопросы

1. Дайте определение понятию «право».
2. Назовите и охарактеризуйте способы представления внутреннего строения системы права Российской Федерации.
3. Дайте определение понятию «правоотношение».
4. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
5. Чем определяется мера участия субъектов в правовых отношениях?
6. Назовите и охарактеризуйте составляющие состава правонарушения.
7. Назовите и охарактеризуйте виды юридической ответственности.
8. Что является предметом правового регулирования в информационной сфере?
9. Охарактеризуйте вертикальную структуру информационного законодательства.
10. Перечислите особенности информации, отличающие ее от других видов товаров.
11. Перечислите правовые принципы защиты информации.
12. Назовите и охарактеризуйте направления защиты информации.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5-6.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5-6
Правовое обеспечение защиты государственной тайны

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Информация ограниченного доступа, включающая государственную тайну и конфиденциальную информацию, имеет особую важность для государства и общества. В той или иной мере правовые институты тайн есть во всех развитых демократиях мира.

Опыт показывает, что с ростом значимости информации в общей системе государственного и муниципального управления (ГМУ) наиболее важным элементом с годами становится достижение превосходства в информационной сфере. Этим обстоятельством и определяется существование институтов тайн, создающих возможность для ГМУ проводить независимую информационную политику, защищать свои интересы, осуществлять управление обществом, регионом, муниципальным образованием.

Система секретной и конфиденциальной информации – наиболее сильное звено регулирования общественных отношений в информационной сфере. Вследствие возможного существенного ущерба от ее разглашения информация ограниченного доступа занимает особое место в системе управления. Институт тайн – важнейший элемент системы государственного и муниципального управления.

Основу нормативно-правового обеспечения защиты информации ограниченного доступа в России составляют Конституция РФ, законы
«О безопасности» от 5 марта 1992 года № 2446-1, «О государственной тайне» от 21 июля 1993 года № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ и другие.

В условиях сегодняшней России (расширяющееся международное сотрудничество, либерализация экономики, увеличение количества объектов иностранных инспекций, свободное перемещение иностранцев по большей части территории страны, внедрение компьютерной техники иностранного производства) значительной возросла опасность утечки сведений, составляющих информацию ограниченного доступа. Вследствие этого важнейшими задачами органов ГМУ являются обеспечение необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями на ее распространение, а также развитие и защита государственного и муниципального ресурса.

В действующем законодательстве РФ встречается упоминание более чем о

30 видах различных тайн (государственная, служебная, коммерческая, банковская, личная, семейная, тайна следствия, связи, почтовых отправлений и другие).
Приведем наиболее важные определения в этой области и дадим необходимую классификацию.
Защищаемой информацией называется информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Собственником информации может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. К защищаемой информации относится информация с ограниченным доступом, а также открытая информация, представляющая ценность.
Информацией с ограниченным доступом называется информация, доступ к которой ограничен в соответствии с Законом с целью защиты прав и законных интересов субъектов права на тайну. Она состоит из государственной тайны и конфиденциальной информации.
Конфиденциальная информация в свою очередь включает множество видов тайны, которые сводятся к шести основным видам:

1) персональные данные;
2) тайна следствия и судопроизводства;
3) служебная тайна;
4) профессиональная тайна;
5) коммерческая тайна;
6) тайна изобретения, полезной модели и промышленного образца.

Особую важность с точки зрения безопасности государства имеет защита информации, составляющей государственную и служебную тайну.
Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
Конфиденциальная информация – информация, не составляющая государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.
Персональные данные – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
Тайна следствия и судопроизводства – защищаемая по закону конфиденциальная информация, ставшая известной в органах следствия и судопроизводства только на законных основаниях в ходе следствия и судопроизводства, а также служебная информация о деятельности органов следствия и судопроизводства, доступ к которой ограничен федеральным законом или в силу служебной необходимости.
Служебная тайна – защищаемая по закону конфиденциальная

информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Профессиональная тайна – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений, банковская тайна и т. д.).

Коммерческая тайна – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, имеющая действительную потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности меры охраны.

Тайна изобретения, полезной модели или промышленного образца – сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Согласно законодательству обязательными признаками информации с ограниченным доступом должны быть:

1. Информация имеет действительную или потенциальную ценность для ее обладателя в силу неизвестности ее третьим лицам. Такими лицами могут быть государство, юридические или физические лица.
2. К информации нет свободного доступа на законном основании.

Возможность сохранения ее неизвестной для третьих лиц установлена законом.

3. Обладатель информации принимает меры по ее защите.

К государственной тайне относятся сведения, удовлетворяющие следующим признакам:

1. Сведения в строго установленных сферах деятельности государства (военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно розыскной деятельности) и ни в каких других.
2. Сведения, не известные широкому, точнее – неопределенному неконтролируемому кругу лиц, и представляющие ценность именно в силу такой неизвестности.
3. Сведения, распространение которых может нанести ущерб безопасности РФ. При этом величина ущерба такова, что влияет на безопасность государства.
4. Сведения, относительно которых предпринимаются специальные меры защиты, направленные на предотвращение их неконтролируемого распространения.

Система документов по защите государственной тайны

Документы по защите государственной тайны по функционально-целевому назначению подразделяются на следующие основные классы:

- нормативные правовые;
- организационно-распорядительные;
- нормативные;
- плановые;
- информационные.

Нормативные правовые акты в области защиты государственной тайны включают:

- федеральные законы;
- указы и распоряжения Президента РФ;
- постановления и распоряжения высших органов исполнительной и судебной властей РФ.

Базовыми законами в области защиты государственной тайны являются специальные законы «О государственной тайне» от 21 июля 1993 года № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ, а также нормативные правовые акты более общего характера: Конституция РФ, Гражданский и Уголовный кодексы РФ и др.

На их основе **организационно-распорядительные документы** определяют состав и регламентируют деятельность соответствующих органов и служб при организации и осуществлении защиты государственной тайны. Эти

документы по характеру регламентируемых вопросов (решаемых задач) и продолжительности действия подразделяют на два вида:

- основополагающие (руководящие) документы;
- распорядительные документы (документы оперативного управления).

Основополагающие (руководящие) документы помимо самостоятельного использования служат основой при разработке нормативных, плановых и информационных документов. Они являются подзаконными актами, детализирующими и раскрывающими положения нормативных правовых актов, и устанавливают основные направления, единые принципы, порядок организации защиты государственной тайны соответствующими органами и службами с приведением их задач, функций, прав, обязанностей и мер ответственности.

Положения по защите государственной тайны издаются на основе нормативных правовых актов и принятых концепций и детализируют указные документы, в основном по вопросам организации защиты государственной тайны в конкретном органе государственной власти (ведомстве) и, в частности, регламентируют:

- основные направления работ по защите государственной тайны;
- структуру органов и служб, ответственных за организацию и осуществление защиты государственной тайны, их права и обязанности;
- порядок организации и проведения типовых работ по защите государственной тайны для основных объектов защиты;
- финансово-экономические вопросы обеспечения работ по защите государственной тайны;
- вопросы государственноголицензирования в области защиты государственной тайны.

Детальные разъяснения отдельных практических вопросов по организации и осуществлению защиты государственной тайны включаются в соответствующие руководства, наставления, инструкции и правила.

Распорядительные документы – документы текущего (оперативного) управления издают во исполнение или в дополнение к основополагающим документам. Основными видами распорядительных документов по защите государственной тайны являются решения, приказы, директивы, распоряжения, указания.

Нормативные документы устанавливают единые требования, нормы и правила защиты информации, составляющей государственную тайну,
обязательные для исполнения в пределах установленной при их введении сферы действия и области их распространения.

Основными видами нормативных документов, в которых

регламентируются вопросы защиты государственной тайны, являются:

- специальные нормативные документы федеральных органов исполнительной власти, ответственных за обеспечение защиты государственной тайны;
- нормативные документы государственной системы стандартизации. К специальным нормативным документам относятся:
- требования и нормы по защите государственной тайны;
- методики проведения работ в области защиты государственной тайны;
- лицензии предприятиям на право осуществления работ в области защиты государственной тайны;
- сертификаты соответствия средств защиты информации;
- аттестаты на объекты защиты.

Плановые документы включают целевые программы и планы в области защиты государственной тайны или соответствующие разделы программ и планов более общего характера, по которым осуществляется самостоятельное финансирование.

Информационные документы служат для информационного обеспечения решения задач организации и осуществления защиты государственной тайны.

По форме представления информационные документы могут быть следующих видов:

- справочные документы;
- отчетная научно-техническая документация;
- учебная и научная литература;
- формы документов служебного делопроизводства.

Федеральный закон «О государственной тайне»

Положения федерального закона «О государственной тайне» от 21 июля 1993 года № 5485-1 обязательны для исполнения на территории Российской Федерации и за ее пределами органами *законодательной,* исполнительной и судебной властей, местного самоуправления, предприятиями, учреждениями и организациями, независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Термины, используемые в законе, их определения

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 также 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.

Правовой режим защиты государственной тайны

Перечневый подход к организации защиты государственной тайны

В настоящее время в России существуют как открытые, так и закрытые перечни сведений. Открытыми перечнями являются приведенный в Законе «О государственной тайне» перечень сведений, составляющих государственную тайну, а также утверждаемый Указом Президента РФ перечень сведений, отнесенных к государственной тайне. Кроме того, существуют ведомственные перечни сведений, подлежащих засекречиванию, которые могут быть как открытыми, так и закрытыми. С их помощью реализуется подход к организации защиты государственной

тайны в виде системы перечней, включающей:

- перечень сведений, составляющих государственную тайну (определен в Законе «О государственной тайне»);
- перечень сведений, отнесенных к государственной тайне (утверждается Указом Президента РФ);
- развернутый перечень сведений, подлежащих засекречиванию в органе государственной власти (утверждается руководителями органов власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне);
- перечни сведений, подлежащих засекречиванию, на предприятии, в учреждении и организации (представляют собой выписки из развернутых перечней сведений, подлежащих засекречиванию).

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.

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым Законом «О государственной тайне», руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделяемых полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом РФ. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Перечень не закрепощает набор конкретных сведений путем прямого отнесения их к государственной тайне, а лишь создает законодательную базу для отнесения конкретных сведений к государственной тайне, если для этого имеется соответствующее обоснование. Такой подход должен позволить системе засекречивания адаптироваться к динамичному развитию нашего общества, ослабить искусственную секретность, наносящую ущерб экономическим интересам РФ.

Установлена персональная ответственность конкретных должностных лиц за принятие решения по отнесению сведений к государственной тайне. Именно за ними сохраняется ответственность за обоснованность, в том числе экономическую, установленной степени секретности конкретных сведений. Именно на них возложена функция гибкого и своевременного реагирования на внешние условия изменения режима секретности, чтобы последний не превращался в фактор, тормозящий развитие экономики, науки и межгосударственных отношений.

Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

1) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
2) о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
3) о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
4) о фактах нарушения прав и свобод человека и гражданина;
5) о размерах золотого запаса и государственных валютных резервах РФ;
6) о состоянии здоровья высших должностных лиц РФ;
7) о фактах нарушения законности органами государственной власти и их должностными лицами.

Должностные лица, принявшие решение о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Контрольные вопросы

1. Перечислите основные виды тайн. Охарактеризуйте каждый вид.
2. Назовите обязательные признаки информации с ограниченным доступом.
3. На какие классы по функциональному назначению подразделяются документы по защите государственной тайны?
4. Дайте определение понятию «гриф секретности».
5. Какие сведения не относятся к государственной тайне и не подлежат засекречиванию?
6. Перечислите органы защиты государственной тайны.
7. Какие существуют методы защиты сведений, составляющих государственную тайну?
8. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7-8.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7-8
Система защиты государственной тайны

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

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.

К органам защиты государственной тайны относятся:

- межведомственная комиссия по защите государственной тайны;
- органы федеральной исполнительной власти (Федеральная служба безопасности РФ, Министерство обороны РФ, Служба специальной связи и информации при Федеральной службе охраны), Служба внешней разведки РФ, Государственная техническая комиссия при Президенте РФ и их органы на местах;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Межведомственная комиссия по защите государственной тайны является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне.

Функции межведомственной комиссии по защите государственной тайны и ее надведомственные полномочия реализуются в соответствии с Положением о межведомственной комиссии по защите государственной тайны, утверждаемым Президентом РФ.

Федеральная служба безопасности РФ, Министерство обороны РФ, Служба специальной связи и информации при Федеральной службе охраны,

Служба внешней разведки РФ, Государственная техническая комиссия при президенте РФ и их органы на местах организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством РФ.

Органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственную тайну, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.

Защита государственной тайны является основным видом деятельности органов государственной власти, предприятий, учреждений или организаций.

Цель защиты государственной тайны заключается в предотвращении или снижении величины ущерба безопасности государства путем исключения (существенного затруднения) утечки информации по всем возможным каналам.

Методы защиты сведений, составляющих государственную тайну, подразделяются на правовые, организационно-технические и экономические.

К **правовым методам** обеспечения защиты сведений, составляющих государственную тайну, относится разработка нормативных правовых актов, регламентирующих отношения в области защиты государственной тайны, и нормативных методических документов по вопросам обеспечения защиты государственной тайны.

Организационно-техническими методами обеспечения защиты сведений, составляющих государственную тайну, являются:

- создание и совершенствование системы защиты государственной тайны в РФ;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, включая предупреждение и пресечение правонарушений в области защиты государственной тайны, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств

информатизации и связи;

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно- телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности РФ;
- формирование системы мониторинга показателей и характеристик информационной безопасности РФ в наиболее важных сферах жизни и деятельности общества и государства, в том числе и по вопросам обеспечения защиты государственной тайны.

Экономические методы обеспечения защиты государственной тайны включают в себя:

- разработку федеральных программ в области защиты государственной тайны и определение порядка их финансирования;
- установление и наложение штрафов на должностных и юридических лиц за нарушения требований по защите государственной тайны.

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:

- бумажные документы;
- магнитные носители информации в электронно-вычислительных машинах;
- электромагнитные поля, создаваемые радиоэлектронными средствами при передаче информации;
- физические проявления объектов (органов управления, промышленных предприятий и др.), сведения о которых составляют государственную тайну, в виде разнообразных полей и следов деятельности.

Как носители сведений в современных условиях особую роль имеют технические средства сбора, передачи, хранения и обработки информации. С их использованием обрабатывается основной объем информации,
составляющей государственную тайну. Их недостатком является уязвимость для широкого спектра угроз несанкционированного распространения защищаемой информации. Защите информации на таких носителях уделяется особое внимание.
Человек в действующем Законе РФ «О государственной тайне»
не рассматривается как специфический носитель сведений, хотя он в своей памяти может хранить эти сведения. Тем самым человек не ставится на один
уровень с техническими носителями. Он в проблеме защиты государственной тайны рассматривается как субъект общественных отношений, возникающих в процессе защиты государственной тайны.

Полномочия органов государственной власти и
должностных лиц в области защиты государственной тайны

Палаты Федерального собрания:

- осуществляют законодательное регулирование отношений в области государственной тайны;
- рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;
- определяют полномочия должностных лиц в аппаратах палат Федерального собрания по обеспечению защиты государственной тайны.

Президент РФ:

- утверждает государственные программы в области защиты государственной тайны;
- утверждает по представлению Правительства РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает по представлению Правительства РФ перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, а также перечень сведений, отнесенных к государственной тайне;
- заключает международные договоры РФ о совместном использовании и защите сведений, составляющих государственную тайну;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в Администрации Президента РФ;
- в пределах своих полномочий решает иные вопросы, возникающие в

связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой.

Правительство РФ:

- организует исполнение Закона РФ «О государственной тайне» ;
- представляет на утверждение Президенту РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает порядок разработки Перечня сведений, отнесенных к государственной тайне;
- организует разработку и выполнение государственных программ в области защиты государственной тайны;
- определяет полномочия должностных лиц по обеспечению защиты государственной тайны в аппарате Правительства РФ;
- устанавливает размеры и порядок предоставления льгот гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;
- устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику информации в результате ее засекречивания;
- заключает межправительственные соглашения, принимает меры по выполнению международных договоров РФ о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам;
- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой.

Органы государственной власти РФ, органы государственной власти субъектов РФ и органы местного самоуправления во взаимодействии с органами защиты государственной тайны, расположенными в пределах
соответствующих территорий:

- обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями сведений, составляющих государственную тайну, а также сведений, засекречиваемых ими;
- обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями актов законодательства РФ;

- обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к государственной тайне;
- реализуют предусмотренные законодательством меры по ограничению прав граждан и предоставлению льгот лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;
- вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты государственной тайны.

Органы судебной власти:

- рассматривают уголовные и гражданские дела о нарушениях законодательства РФ о государственной тайне;
- обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны;
- обеспечивают в ходе рассмотрения указанных дел защиту государственной тайны;
- определяют полномочия должностных лиц по обеспечению защиты государственной тайны в органах судебной власти.

Допуск должностных лиц и граждан к государственной тайне 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.

Допуск должностных лиц и граждан РФ к государственной тайне осуществляется в добровольном порядке.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

Принятие на себя обязательств перед государством по
нераспространению доверенных им сведений, составляющих государственную тайну;

- согласие на частные, временные ограничения их прав в соответствии со статьей 24 Закона «О государственной тайне»;
- письменное согласие на проведение в отношении их полномочий органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных Законом «О государственной тайне»;
- ознакомление с нормами законодательства РФ о государственной тайне,

предусматривающими ответственность за его нарушение;

- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются следующие льготы:

- процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и/или штатных мероприятий.

Основанием для отказа гражданину в допуске к государственной тайне в соответствии со статьей 22 Закона «О государственной тайне» могут являться:

- признание его судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;
- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения РФ;
- постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное место жительства в другое государство;
- выявление в результате проведения проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности РФ;
- уклонение от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

Решение об отказе гражданину в допуске к государственной тайне принимается руководителем организации в индивидуальном порядке с учетом результатов проверочных мероприятий.

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска:

- **первая форма** – для граждан, допускаемых к сведениям особой важности;
- **вторая форма** – для граждан, допускаемых к совершенно секретным сведениям;
- **третья форма** – для граждан, допускаемых к секретным сведениям. Наличие у должностных лиц и граждан допуска к сведениям более

высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности РФ и ее территориальными органами.

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством РФ, лицензий на проведение работ со сведениями соответствующей степени секретности.

Основными **целями** контроля и надзора являются:

- обеспечение выполнения единых правил и норм в организации работ по защите государственной тайны;
- своевременное выявление предпосылок к утечке информации, составляющей государственную тайну.

Основными **задачами** контроля и надзора являются:

- оценка полноты и качества выполнения органами, организациями и должностными лицами, осуществляющими деятельность в области защиты государственной тайны, возложенных на них обязанностей и функций;
- оценка целесообразности и обоснованности принимаемых управленческих решений и мер по защите государственной тайны с целью предупреждения возможных неблагоприятных последствий их выполнения;
- выявление нарушений установленных требований или норм по защите государственной тайны, установление их причин, подготовка в необходимых случаях материалов для привлечения виновных к ответственности;
- профилактика различных видов нарушений;
- выявление нерешенных проблем и противоречий в правовом, организационном, научно-техническом, информационном и других видах обеспечения эффективной защиты государственной тайны.

Рассмотрим основные термины в области контроля и надзора за обеспечением защиты государственной тайны.

Контроль состояния защиты государственной службы – проверка соответствия организации и эффективности защиты информации, составляющей государственную тайну, установленным требованиям и/или нормам по защите государственной тайны.

Контроль организации защиты информации – проверка соответствия организации, наличия и содержания документов требованиям правовых,

организационно-распорядительных и нормативных документов в области защиты информации.

Контроль эффективности защиты информации – проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации.

Надзор – наблюдение, разновидность контроля, одна из форм деятельности различных государственных органов по обеспечению законности. Надзор – это контроль в форме правового регулирования. Эта форма применяется, прежде всего, для осуществления контроля за соблюдением законов, установленных норм, требований, стандартов. Органы надзора вправе при соответствующих обстоятельствах применять к объектам надзора меры административного принуждения. Необходимым условием надзора является отсутствие между субъектами и объектами надзора организационной соподчиненности.

Контрольные вопросы

Перечислите органы защиты государственной тайны.

1. Какие существуют методы защиты сведений, составляющих государственную тайну?
2. Перечислите органы защиты государственной тайны.
3. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.
4. Назовите цели и задачи контроля и надзора за обеспечением защиты государственной тайны.
5. Поясните сущность ведомственного контроля над обеспечением защиты государственной тайны.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 9-10.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 9-10
Правовое обеспечение защиты банковской, профессиональной и служебной тайны

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Банковская тайна – защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в
интересах клиентов. К основным объектам банковской тайны относятся: тайна банковского счета, тайна операций по банковскому счету, тайна банковского вклада, тайна частной жизни клиента.

Банковская тайна является видом конфиденциальной информации или видом сведений, перечень которых достаточно четко определен законом.

Статья 857 «Гражданского кодекса РФ (Часть вторая)» от 26 января 1996 года № 14-ФЗ «Банковская тайна» содержит следующие нормы:

1) банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте;
2) сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям.

Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренном законом;

3) в случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

Федеральный закон «О банках и банковской деятельности»
от 2 декабря 1990 года № 395-1 содержит более расширенную группу норм (статья 26):

Кредитная организация. Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной

организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

- Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям). Счетной палате Российской Федерации, органам государственной налоговой службы и налоговой полиции, таможенным органам Российской Федерации в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора – органам предварительного следствия по делам, находящимся в их производстве.
- Справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, а при наличии согласия прокурора – органами предварительного следствия по делам, находящимся в их производстве.
- Справки по счетам и вкладам в случае смерти их владельцев выдаются кредитной организацией лицам, указанным владельцем счета или вклада в сделанном кредитной организации завещательном распоряжении, нотариальным конторам по находящимся в их производстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан – иностранным консульским учреждениям.
- Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.
- Аудиторские организации не вправе раскрывать третьим лицам сведения об операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.
- За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и их работники несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом.

Таким образом, сведения, составляющие банковскую тайну, не устанавливаются по волеизъявлению субъекта предпринимательской
деятельности – банка или иной кредитной организации, а это определенные законом сведения, которые принадлежат клиентам банка (банковский счет, банковский вклад, операции по счету, сведения о клиенте). При этом
обязанность сохранять эти сведения является односторонней обязанностью

банка – клиент не связан этими обязательствами. Вторым отличием банковской тайны, выводящим ее за пределы частного случая коммерческой тайны, является тот факт, что банковская тайна может выступать как охранительный институт для личной и семейной тайны, если граждане желают сохранять в тайне свое финансовое положение.

Пользование информацией,
составляющей профессиональную тайну

В сфере ГМУ широко распространена **профессиональная тайна**, которая представляет собой одну из самых специфических систем ограничений на доступ к информации. Профессиональная тайна чаще всего имеет дело с информационными блоками, защита от несанкционированного распространения которых является обязанностью субъекта в силу выполняемых им профессиональных функций. При этом в качестве субъекта, на который возлагается обязанность сохранения профессиональной тайны, может выступать как физическое, так и юридическое лицо. Соблюдение тайн представителями определенных профессий является их обязанностью, возникающей вне зависимости от того, урегулирована она какими-либо юридическими нормами либо нет. В этом случае обязательства по нераспространению сведений являются неотъемлемой частью самой профессии. Гражданин не обратился бы к адвокату, нотариусу или частнопрактикующему врачу, если бы не был уверен, что доверенные этому лицу сведения не будут сохранены в тайне от посторонних, которыми в данном случае являются любые третьи лица.

Система исходящих от государства норм поведения также не может оставаться в стороне от регулирования этой группы общественных отношений. Нормы законодательства, регулирующие данные отношения, характеризуются в целом двумя моментами:

- данные нормы содержатся в соответствующих профильных законах;
- как правило, эти нормы содержат только запреты на распространение определенных категорий сведений, не описывая механизма их защиты.

Объектом профессиональной тайны является, прежде всего, информация, принадлежащая гражданам, обращающимся за профессиональными услугами (нотариальными, страховыми, медицинскими и др.). С развитием рыночных отношений и появлением большого числа субъектов предпринимательской деятельности в России юридические лица также стали полноправными участниками этих отношений. Нотариальная тайна, тайна связи, адвокатская тайна – действие этих правовых институтов в равной степени распространяется и на сведения, обладателями которых являются юридические лица.

Профессиональная тайна является неотъемлемой частью определенных видов профессиональной деятельности вне зависимости от того, ведется она от имени государства или от частного лица. И даже если она ведется от имени государства, это не значит, что государство в лице других органов ГМУ может без ограничений получать доступ к таким сведениям.

К примеру, по действующему законодательству РФ информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при обследовании и лечении, составляют **врачебную (медицинскую) тайну.**

Включаемый в данный институт перечень сведений достаточно подробно представлен в действующем законодательстве РФ. Прежде всего следует отметить нормы статьи 61 «Основ законодательства РФ об охране здоровья граждан», утвержденные ВС РФ 22 июля 1993 года № 5487-1, которая именуется «Врачебная тайна». На основе этих норм к медицинской тайне относятся:

- факт обращения гражданина за медицинской помощью;
- состояние здоровья гражданина;
- диагноз заболевания;
- иные сведения, полученные при обследовании и лечении.

Допускается предоставление сведений, составляющих медицинскую тайну, без согласия гражданина или его законного представителя:

- в целях обследования гражданина, не способного выразить свою волю;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством;
- в случае оказания помощи несовершеннолетнему в возрасте до 15 лет для информирования его родителей или законных представителей;
- при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий.

Нотариальная тайна вытекает из законодательной базы деятельности нотариата в РФ, которую определяет Конституция РФ и Основы законодательства РФ о нотариате.

Адвокатская тайна – сведения, сообщенные адвокату гражданином в связи с оказанием ему юридической помощи.

Процессуальные тайны – тайна совещания судей, тайна совещания присяжных заседателей, данные предварительного следствия (дознания) –

содержат в себе признаки как служебной тайны, так и профессиональной.
Первые два вида направлены на обеспечение невмешательства в отправление правосудия и представляют из себя административно-правовой запрет на контакт с судьями в период их совещания по поводу вынесения приговора (вердикта, решения).
Тайна страхования – это разновидность служебной, а также коммерческой тайны. Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о застрахованном лице, о состоянии его здоровья, а также о его имущественном положении.
Тайна связи – регулируется конституционными нормами (часть 2 статьи 23 Конституции РФ), а также соответствующими нормами федеральных законов «О связи» от 07 июля 2003 года № 126-ФЗ, «О почтовой связи» от 17 июля 1999 года № 176-ФЗ.
Пользование информацией, составляющей служебную тайну
В сфере ГМУ нередко фигурирует служебная тайна, которая наиболее сложна с точки зрения определения ее понятия и правового режима, поскольку в этот вид тайны в разное время включалось и теперь включается различное содержание. Служебная тайна является разновидностью конфиденциальной информации. Согласно Закону РФ «О государственной тайне» от 21 июля 1993 года № 5485-1, прежний режим служебной тайны упразднен, и секретные сведения относятся к государственной тайне. Однако в различных правовых актах термин «служебная тайна» продолжает упоминаться и в него вкладывается различное значение, причем в большинстве случаев оно даже не раскрывается.
Объектами служебной тайны являются преднамеренно скрываемые интересы и сведения о различных сторонах и сферах государственной, военной, управленческой, научно-технической, финансовой, экономической и др. деятельности хозяйствующего субъекта, охрана которых обусловлена возможной угрозой безопасности хозяйствующего субъекта.
Субъектами служебной тайны являются собственник служебной информации ограниченного распространения (юридическое лицо, обладающее на законном основании служебной конфиденциальной информацией), конфидент служебной информации ограниченного распространения (физическое или юридическое лицо, использующее служебную информацию ограниченного распространения в пределах, установленных собственником или владельцем служебной информации ограниченного распространения на основании договора или распорядительных документов).
Содержащие служебную тайну документы:

- печатаются в специально выделенной комнате;

- учитываются, как правило, отдельно от несекретной документации;
- передаются работникам подразделений под расписку;
- пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
- размножаются только с письменного разрешения соответствующего руководителя;

Контрольные вопросы

1. Какие сведения относятся к банковской тайне?
2. Перечислите известные вам виды профессиональной тайны.
3. Раскройте порядок обращения с документами, содержащими служебную тайну.
4. Какая информация относится к сведениям конфиденциального характера?
5. Какие сведения в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» запрещено относить к конфиденциальной информации?
6. Опишите структуру законодательства РФ о коммерческой тайне.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 11-12.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 11-12
Правовое обеспечение защиты коммерческой тайны

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Конфиденциальная информация – достаточно широкое понятие, поскольку к этой категории (за исключением сведений, относящихся к государственной тайне) относятся все виды информации ограниченного доступа, защищаемой законами.

В соответствии с Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188 к этим сведениям относятся:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
2) сведения, составляющие тайну следствия и судопроизводства;
3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);
4) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.);
5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);
6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Расширительному толкованию этот перечень не подлежит. Поэтому

произвольное отнесение кем-либо к разряду конфиденциальной другой, не предусмотренной перечнем информации не влечет за собой правовых последствий. Более того, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ запрещено относить к конфиденциальной информации:

1) законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
2) документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
3) документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;
4) документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений и организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет ФСТЭК.

Под **технической защитой конфиденциальной информации** понимается комплекс мероприятий и (или) услуг по защите ее от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней.

В соответствии с Положением «О лицензировании деятельности по технической защите конфиденциальной информации» лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

1) осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности

«компьютерная безопасность», «комплексное обеспечение информационной безопасности автоматизированных систем» или «информационная безопасность

телекоммуникационных систем», либо специалистами, прошедшими переподготовку по вопросам защиты информации;

2) соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами РФ, руководящими и нормативно-методическими документами, утвержденными приказами ФСТЭК, которые зарегистрированы в Министерстве юстиции РФ;
3) использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;
4) использование третьими лицами программ для ЭВМ или баз данных на основании договора с их правообладателем.

Законодательство Российской Федерации о коммерческой тайне

В условиях рыночного хозяйствования коммерческая тайна защищает производителя от недобросовестной конкуренции, к которой относятся противоправные действия в виде скрытого использования торговой
марки, подделки продукции конкурента, обманной рекламы, подкупа, шантажа и т. п.

Законодательство Российской Федерации о коммерческой тайне есть совокупность федеральных законодательных актов, которые содержат
правовые нормы, регулирующие группу однородных общественных отношений, возникающих в связи и по поводу коммерческой тайны между ее обладателем и иными субъектами.

Закон «О предприятиях и предпринимательской деятельности»
от 25 декабря 1990 года № 445-1 впервые закрепил понятие «коммерческая тайна»: информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Федеральный закон «О коммерческой тайне»

Федеральный закон «О коммерческой тайне» от 29 июля 2004 года
№ 98-ФЗ регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).

Положения закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована и не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения

законодательства Российской Федерации о государственной тайне.

Основные понятия и определения

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну (секрет производства) – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

Обладатель информации, составляющей коммерческую тайну – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Доступ к информации, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Контрагент – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Предоставление информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам

государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение информации, составляющей коммерческую тайну – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Информация, относящаяся к коммерческой тайне

Состав сведений, составляющих коммерческую тайну, представляет собой одно из центральных звеньев в системе мер, осуществляемых
предприятием по защите своей интеллектуальной собственности. Ошибочное или несвоевременное выделение предмета защиты существенно снижает эффективность системы информационной безопасности предприятия, что
чревато существенным экономическим ущербом для него.

Перечень сведений, составляющих коммерческую тайну предприятия, следует формировать по следующим признакам:

- эта информация должна быть экономически выгодной для предприятия или выгодной для его конкурента в случае ее утечки. В качестве критерия важности конкретной информации принимается количественный показатель величины наносимого ущерба;
- эта информация не должна быть общеизвестной или общедоступной на законных основаниях;
- эти сведения не должны содержать государственной тайны или защищаться согласно нормам авторского или патентного права;
- информация, которая зафиксирована в письменной или иной материальной форме или находится в исключительном ведении предприятия;
- такая информация должна быть понятным образом специально обозначена («грифована») и в отношении нее должны быть обеспечены необходимые меры по сохранению конфиденциальности;
- эти сведения не должны напрямую касаться деятельности предприятия, способной нанести ущерб обществу, жизни и здоровью людей.

При этом информация, подтверждающая сведения, компрометирующие компанию, не может быть только на этом основании отнесена к коммерческой тайне.

Обеспечение конфиденциальности требует определенных затрат, в число которых входят, с одной стороны, затраты на обеспечение режимных
мероприятий, а с другой – потери от ограничений в использовании

конфиденциальной информации. Экономический же эффект от утаения информации может выразиться как в получении реальной прибыли, так и в предотвращении возможного ущерба предприятию. Сравнение положительных и отрицательных последствий ограничения доступа к рассматриваемым сведениям и их открытого использования, анализ возможностей предприятия по обеспечению необходимых защитных мер позволит определить экономическую или иную целесообразность отнесения тех или иных сведений к коммерческой тайне.

С течением времени ценность информации уменьшается, а суммарные затраты растут. Чем выше уровень защиты, тем дороже обходится ее обеспечение, поэтому необходимо оценивать оптимальный уровень защиты.

Самое сложное из приведенных понятий – отсутствие доступа на законном основании. За этой формулировкой стоят перечни сведений, которые запрещено относить к тому или иному виду тайны.

В законе «О коммерческой тайне» приведены сведения, которые не могут составлять коммерческую тайну.

Таким образом, режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и о наличии свободных рабочих мест;
- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

В статье 10 закона «О коммерческой тайне» приведены меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;
2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, или лиц, которым такая информация была предоставлена или передана;
4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, приведенных выше.

Наряду с приведенными мерами обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

Кроме того, меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Контрольные вопросы

1. Что представляет собой информация, составляющая коммерческую тайну?
2. Что понимается под разглашением информации, составляющей коммерческую тайну?
3. По каким признакам определяется перечень сведений, составляющих коммерческую тайну предприятия?
4. В отношении каких сведений не может быть установлен режим коммерческой тайны?
5. Приведите меры по охране конфиденциальности информации в соответствии с законом «О коммерческой тайне».

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 13-14.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 13-14
Правовое обеспечение защиты персональных данных

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

По смыслу Конституции РФ **личность** – это человек как член общества и как носитель индивидуального начала. Главное в конституционном понятии личности – это социальная ценность человека, в соответствии с чем он является субъектом различных прав, свобод и обязанностей.

Сущность информационной свободы состоит, по крайней мере, из четырех правомочий: право на индивидуализацию; право на защиту чести и достоинства; право на дачу согласия на сбор, хранение и использование материалов о частной жизни; право на неприкосновенность частной жизни, личную и семейную тайну.

Право на неприкосновенность частной жизни, личную и семейную тайну означает, что человек вправе строить свою жизнь в семье, в неформальном общении с друзьями и другими лицами таким образом, как он сам того желает.

В Российском законодательстве существуют следующие источники права на личную или семейную тайну:

1. Конституция РФ признает права и свободы человека высшей ценностью, а их защиту – обязанностью государства.
2. Федеральный Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ регулирует отношения, возникающие при:

~ формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;

~ создании и использовании информационных технологий и средств их обеспечения;

~ защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

3. Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ регулирует отношения, возникающие при:

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

4. Уголовный кодекс РФ. Статья 137. Нарушение неприкосновенности частной жизни.

Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

4. Трудовой кодекс РФ. Осуществляет защиту персональных данных работника – информации, необходимой работодателю в связи с трудовыми отношениями.
5. Гражданский кодекс РФ. Статьи 150-152, призванные защитить право человека на неприкосновенность частной жизни.

Наиболее емким потоком конфиденциальной информации являются сведения о гражданах. Действующее законодательство определяет их как персональные данные. Это понятие было введено Федеральным Законом «Об информации, информатизации и о защите информации» и получило дальнейшее развитие в Указе Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188.

Предметом личной и семейной тайны являются следующие сведения:

1. О фактах биографии.

2. О состоянии здоровья человека.
3. Об имущественном положении.
4. О роде занятий и совершенных поступках.
5. О взглядах, оценках, убеждениях человека.
6. Об отношениях в семье, а также отношениях человека с другими людьми.

В соответствии с Федеральным законом «О персональных данных» под **персональными данными** понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных – действия, в результате которых

невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

К персональным данным относятся: биографические и опознавательные данные, личные характеристики, сведения о семейном положении, социальном положении, образовании, навыках, профессии, служебном положении, финансовом положении, состоянии здоровья и прочее.

Обработка персональных данных должна осуществляться на основе принципов:

1) законности целей и способов обработки персональных данных и добросовестности;
2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
4) достоверности персональных данных, их достаточности для целей

обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении
целей обработки или в случае утраты необходимости в их достижении.

Обработка персональных данных может осуществляться оператором с
согласия субъектов персональных данных за исключением следующих случаев:

1) если обработка персональных данных осуществляется на основании Федерального закона «О персональных данных», устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за
исключением случаев обезличивания персональных данных и в отношении

общедоступных персональных данных.
В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.
Независимо от вида деятельности на любом предприятии имеется информация, требующая защиты. На коммерческом предприятии это коммерческая тайна и персональные данные сотрудников (ПДР).
Персональные данные работника – информация о конкретном лице, необходимая работодателю в связи с возникновением трудовых отношений.
Данная информация в соответствии с законодательством (Закон РФ «Об информации, информационных технологиях и о защите информации») является конфиденциальной. На каждого работника ведется личное дело, в состав которого входят данные, представленные на рисунке 2.3.
Согласно «Перечню типовых управленческих документов, образующихся в деятельности организаций с указанием сроков хранения», личные дела рядовых работников предприятия должны храниться 75 лет, а руководителей – постоянно.
Личные дела работников хранятся как документы, доступ к которым ограничен.
Отбор документов предприятия на хранение или уничтожение осуществляется по решению экспертной комиссии, руководствующейся федеральными, отраслевыми и внутренними нормативными актами, например:

- «Положение об Архивном фонде РФ»;
- «Основные правила работы ведомственных архивов»;
- «Положение об экспертной комиссии»;
- «Номенклатура дел»;
- «Инструкция по делопроизводству» и др.

Экспертиза ценности документов производится ежегодно. Документы по личному составу или содержащие КТ, отобранные на хранение, требуют дополнительного оформления:

- производится нумерация листов в правом верхнем углу;
- составляется внутренняя опись;
- дело переплетается и прошивается в четыре прокола. Опись дел по личному составу обозначают: опись №1 л/с.

Очень важной и дорогостоящей информацией фирмы являются сведения о

клиентах и конкурентах. Западные специалисты рекомендуют использовать два документа: «профиль клиента» и «профиль конкурента», которые должны постоянно пополняться и обновляться информацией. Эти базы данных позволяют найти индивидуальный подход к деловому партнеру и предвидеть шаги конкурентов.

Доказательством высокого качества делового партнерства и обеспечения интересов клиента служит наличие на фирме сертификата по Международной системе стандартов качества ISO 9000. В настоящее время система ISO оценивает не только качество конечного продукта бизнеса, но и сам бизнес- процесс предприятия: проектирование, разработку, закупку сырья и комплектующих, создание, обработку, документирование, заключение контрактов, обучение персонала, обслуживание и поддержку клиентов и информационную безопасность.

По имеющимся данным к 2002 году 76 стран мира проводят сертификацию на соответствие стандартам ISO 9000. Сертификат получили более 100000 компаний. Наличие сертификата позволяет заключать сделки с ведущими мировыми компаниями, получать госзаказы, принимать участие в международных проектах.

Исследования поведения компаний при проведении такой сертификации позволяет заглянуть под маску рекламного имиджа, что значительно увеличивает безопасность деловых отношений.

Неоправданный риск сомнительных сделок может серьезно отразиться на жизнеспособности предприятия. Результатом недобросовестной конкуренции может стать уничтожение или потеря значительной части информационных ресурсов предприятия. В ряде случаев такие потери могут привести к банкротству и ликвидации предприятия.

В Российской Федерации принят закон «О несостоятельности (банкротстве)» от 26 октября 2002 года № 127-ФЗ, определяющий условия банкротства и регламент действий и процедур в отношении должника.

Ответственность за нарушение норм защиты персональных данных

В соответствии с Трудовым кодексом РФ работодатель обязан соблюдать следующие требования при работе с персональными данными.

В соответствии со статьей 13.11 КоАП нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц

– от пяти тысяч до десяти тысяч рублей.

В УК РФ уголовная ответственность в отношении ПДР дана в ст. 137 «Нарушение неприкосновенности частной жизни»: штраф в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.

То же преступление, совершенное лицом с использованием своего служебного положения, наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

Контрольные вопросы

1. Назовите основные источники права в области защиты персональных данных.
2. Какие сведения являются предметом личной и семейной тайны?
3. Что понимается под обработкой персональных данных?
4. Поясните понятие «трансграничная передача персональных данных».
5. Перечислите принципы обработки персональных данных.
6. Какие требования необходимо выполнить при работе с персональными данными работника?

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 15-16.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 15-16
Правовое обеспечение защиты интеллектуальной собственности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Понятие интеллектуальной собственности (ИС) используется с момента создания 14 июля 1967 года Всемирной организации интеллектуальной собственности (ВОИС), но в советском законодательстве этот термин появился впервые в Законе СССР «О собственности в СССР» (6 марта 1990 года), а в российском был утвержден в декабре 1993 года – с принятием Конституции РФ и с принятием первой части Гражданского кодекса РФ.

Наряду с упоминанием в ГК РФ был принят ряд законов:

- «Патентный закон Российской Федерации» от 23 сентября 1992 года № 3517-1;
- «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» от 23 сентября 1992 года № 3520-1;
- «О правовой охране топологий интегральных микросхем» от 23 сентября 1992 № 3526-1;
- «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 № 3523-1;
- «Об авторском праве и смежных правах» от 9 июля 1993 года № 5351-1.

К настоящему времени в Российской Федерации в отношении ИС действует четвертая часть Гражданского кодекса РФ от 18 декабря 2006 г., вступившего в силу с 1 января 2008 г. В Федеральном законе «О введении в действие части четвертой Гражданского кодекса Российской Федерации» от 18 декабря 2006 г. в ст. 2 приведен перечень нормативно-правовых актов, утративших силу с 1 января 2008 г., среди которых были и перечисленные

выше законы. Нормы Гражданского кодекса РФ (в дальнейшем – ГК) образуют в своей совокупности особую подотрасль российского гражданского права – право интеллектуальной собственности. С учетом общности ряда объектов интеллектуальной собственности указанная подотрасль российского гражданского права обычно подразделяется на четыре относительно самостоятельных института. Несмотря на тесную взаимосвязь и наличие целого ряда общих моментов, каждый из этих институтов имеет присущие лишь ему черты, которые находят отражение в нормах российского законодательства.

Прежде всего выделяется *институт авторского права и прав, смежных с авторским.* Им регулируются отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного и кабельного вещания (смежные права). Объединение в едином институте, который в дальнейшем для краткости будет именоваться авторским правом, двух указанных групп норм объясняется теснейшей зависимостью возникновения и осуществления смежных прав от прав авторов творческих произведений, а также регулирование соответствующих отношений единым законом.

Другим правовым институтом, входящим в систему подотрасли «право интеллектуальной собственности», является *патентное право.* Оно регулирует имущественные, а также связанные с ними личные неимущественные отношения, возникающие в связи с созданием и использованием изобретений, полезных моделей и промышленных образцов.

С развитием товарно-денежных отношений в России все более важным элементом рыночной экономики становятся такие объекты промышленной собственности, как фирменные наименования, товарные знаки, знаки обслуживания и наименования мест происхождения товаров. Создание равных условий хозяйствования для всех товаровладельцев, внедрение конкурентных начал в их деятельность и повышение ответственности за ее результаты, необходимость насыщения рынка товарами и услугами для удовлетворения потребностей населения обусловливают объективную потребность в правовом механизме, обеспечивающем должную индивидуализацию предприятий и организаций, а также производимых ими товаров и услуг. Такой правовой механизм представлен особым институтом рассматриваемой подотрасли гражданского права, а именно *институтом средств индивидуализации участников гражданского оборота и производимой ими продукции (работ, услуг).* Данный правовой институт, как и патентное право, имеет дело с так называемой промышленной собственностью, то есть с исключительными правами, реализуемыми в сфере производства, торгового обращения, оказания

услуг и т. п. Основной функцией рассматриваемого института интеллектуальной собственности является обеспечение должной индивидуализации производителей и их товаров, работ и услуг.

Творения, признаваемые произведениями науки, литературы или искусства, а также изобретениями, полезными моделями и промышленными образцами, не исчерпывают всего многообразия результатов творческой деятельности. Наряду с ними имеется немало объектов, которые создаются творческими усилиями людей, представляют ценность для общества и также нуждаются в общественном признании и правовой охране. Помимо традиционных объектов, охраняемых авторским и патентным правом, а также институтом средств индивидуализации участников гражданского оборота, российское гражданское право предоставляет охрану селекционным достижениям, топологиям интегральных микросхем, информации, составляющей служебную и коммерческую тайну, и некоторым другим результатам интеллектуальной деятельности. Опираясь на отличия указанных результатов интеллектуальной деятельности от традиционных объектов интеллектуальной собственности, все их можно условно отнести к сфере единого правового института, а именно *института охраны нетрадиционных объектов интеллектуальной собственности.*

Современное российское законодательство об ИС подразделяется на пять основных частей:

- авторское право;
- охрана смежных прав;
- патентное право;
- законодательство о средствах индивидуализации участников гражданского оборота, товаров и услуг;
- законодательство о нетрадиционных объектах ИС (научные открытия, рацпредложения, ноу-хау);
- законодательство о защите против недобросовестной конкуренции.

Каждый из этих институтов имеет свои особенности. Рассмотрим основные из них при краткой характеристике каждого по структуре: источники права; объекты и субъекты права; основные права субъектов; способы их охраны и защиты.

Результатом интеллектуальной деятельности человека является информационный продукт, который представляется на рынке в виде информационных товаров и услуг. Свойство информационного продукта, такое как трудность производства и относительная простота тиражирования создает немало проблем в связи с определением прав собственности в области информационной деятельности.

Законодательными актами РФ регламентируется право собственности на информацию, полученную юридическими и физическими лицами в результате интеллектуальной деятельности. Это исключительное право представляет собой интеллектуальную собственность (ИС).

Под **интеллектуальной собственностью** понимаются результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана.

Конкретизация понятия интеллектуальная собственность дана в Конвенции, учреждающей Всемирную организацию интеллектуальной собственности (ВОИС). Конвенция была принята на Стокгольмской конференции в 1967 году и ратифицирована в 1968 году СССР.

Правовая охрана интеллектуальной собственности

Существует три общепризнанные в мире правовые формы защиты интеллектуальной собственности: авторское право, патентное право и коммерческая тайна.

Авторское право – форма правовой защиты в отношении литературных, художественных и научных произведений.

Смежные права – это права, примыкающие к авторскому праву, они защищают: исполнителей (актеров, певцов, танцоров и т. д.); производителей фонограмм; организации эфирного и кабельного вещания.

Патентное право – форма правовой защиты в отношении изобретений во всех областях человеческой деятельности.

Коммерческая тайна – не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам. К информации, составляющей КТ, относят сведения, которые называют «ноу- хау».

Ноу-хау – не являющиеся общеизвестными и практически применяемые в производственной и хозяйственной деятельности: различного рода технические знания и опыт, включая методы, способы и навыки; разработки и использования технологических процессов; методы и способы лечения и т. п.

Объекты патентного права

Объектами патентных прав являются результаты интеллектуальной деятельности в научно-технической сфере, отвечающие установленным настоящим кодексом требованиям к изобретениям и полезным моделям, и результаты интеллектуальной деятельности в сфере художественного конструирования, отвечающие установленным ГК РФ требованиям к

промышленным образцам. На изобретения, содержащие сведения, составляющие государственную тайну (секретные изобретения), положения ГК РФ распространяются, если иное не предусмотрено специальными правилами статей 1401–1405 ГК РФ и изданными в соответствии с ними иными правовыми актами. Полезным моделям и промышленным образцам, содержащим сведения, составляющие государственную тайну, правовая охрана в соответствии с настоящим кодексом не предоставляется.

Не могут быть объектами патентных прав:

1) способы клонирования человека;
2) способы модификации генетической целостности клеток зародышевой линии человека;
3) использование человеческих эмбрионов в промышленных и коммерческих целях;
4) иные решения, противоречащие общественным интересам, принципам гуманности и морали.

В качестве **изобретения** охраняется техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу (процессу осуществления действий над материальным объектом с помощью материальных средств). Изобретению предоставляется правовая охрана, если оно является:

- новым – оно не известно из уровня техники
- имеет изобретательский уровень – если для специалиста оно не следует из уровня техники явным образом.
- промышленно применимо – если оно может быть использовано в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере.

Уровень техники включает любые сведения, ставшие общедоступными в мире до даты приоритета изобретения.

При установлении новизны изобретения в уровень техники также включаются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на выдачу патентов на изобретения и полезные модели, с документами которых вправе ознакомиться любое лицо и запатентованные в Российской Федерации изобретения и полезные модели.

Раскрытие информации, относящейся к изобретению, автором изобретения, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности изобретения стали общедоступными, не является обстоятельством, препятствующим

признанию патентоспособности изобретения, при условии, что заявка на выдачу патента на изобретение подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию
патентоспособности изобретения, имели место, лежит на заявителе.

Не являются изобретениями:

1) открытия;
2) научные теории и математические методы;
3) решения, касающиеся только внешнего вида изделий и направленные на удовлетворение эстетических потребностей;
4) правила и методы игр, интеллектуальной или хозяйственной деятельности;
5) программы для ЭВМ;
6) решения, заключающиеся только в представлении информации.

В соответствии с ГК РФ исключается возможность отнесения этих объектов к изобретениям только в случае, когда заявка на выдачу патента на изобретение касается этих объектов как таковых.

Не предоставляется правовая охрана в качестве изобретения:

1) сортам растений, породам животных и биологическим способам их получения, за исключением микробиологических способов и продуктов, полученных такими способами;
2) топологиям интегральных микросхем.

В качестве **полезной модели** охраняется техническое решение, относящееся к устройству.

Полезной модели предоставляется правовая охрана, если она является новой (если совокупность ее существенных признаков не известна из уровня техники) и промышленно применимой (если она может быть использована в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере).

Уровень техники включает опубликованные в мире сведения о средствах того же назначения, что и заявленная полезная модель, и сведения об их
применении в Российской Федерации, если такие сведения стали
общедоступными до даты приоритета полезной модели. В уровень техники также включаются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на выдачу патента на
изобретения и полезные модели, с документами которых вправе ознакомиться любое лицо в соответствии с пунктом 2 статьи 1385 или пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации изобретения

и полезные модели.
Раскрытие информации, относящейся к полезной модели, автором полезной модели, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о сущности полезной модели стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности полезной модели, при условии, что заявка на выдачу патента на полезную модель подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности полезной модели, имели место, лежит на заявителе.
Не предоставляется правовая охрана в качестве полезной модели:

1) решениям, касающимся только внешнего вида изделий и направленным на удовлетворение эстетических потребностей;
2) топологиям интегральных микросхем.

В качестве **промышленного образца** охраняется художественно-конструкторское решение изделия промышленного или кустарно-ремесленного производства, определяющее его внешний вид.
Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является новым и оригинальным. К существенным признакам промышленного образца относятся признаки, определяющие эстетические и (или) эргономические особенности внешнего вида изделия, в частности, форма, конфигурация, орнамент и сочетание цветов.
Промышленный образец является новым, если совокупность его существенных признаков, нашедших отражение на изображениях изделия и приведенных в перечне существенных признаков промышленного образца (пункт 2 статьи 1377), не известна из сведений, ставших общедоступными в мире до даты приоритета промышленного образца. При установлении новизны промышленного образца также учитываются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на промышленные образцы, с документами которых вправе ознакомиться любое лицо в соответствии с пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации промышленные образцы.
Промышленный образец является оригинальным, если его существенные признаки обусловлены творческим характером особенностей изделия.
Раскрытие информации, относящейся к промышленному образцу, автором промышленного образца, заявителем или любым лицом, получившим от них прямо или косвенно эту информацию, в результате чего сведения о

сущности промышленного образца стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности промышленного образца, при условии, что заявка на выдачу патента на промышленный образец подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности промышленного образца, имели место, лежит на заявителе.

Не предоставляется правовая охрана в качестве промышленного образца:

1) решениям, обусловленным исключительно технической функцией изделия;
2) объектам архитектуры (кроме малых архитектурных форм), промышленным, гидротехническим и другим стационарным сооружениям;
3) объектам неустойчивой формы из жидких, газообразных, сыпучих или им подобных веществ.

Субъекты патентного права

К основным субъектам патентного права относятся авторы (изобретения, полезной модели, промышленного образца), патентообладатели, их правопреемники, патентное ведомство, патентные поверенные.

Автор – любое физическое лицо, творческим трудом которого созданы изобретение, полезная модель, промышленный образец, селекционное достижение.

За лиц до 14 лет права осуществляют их законные представители (родители, опекуны).

Не признаются авторами физические лица, не внесшие личного творческого вклада в создание объекта промышленной собственности, оказавшие автору только техническую, организационную или материальную помощь, либо только способствовавшие оформлению прав на его использование.

Патентообладатель – лицо, владеющее патентом на изобретение, промышленный образец, свидетельством на полезную модель, селекционное достижение и вытекающими из патента (свидетельства) исключительными правами на использование указанных объектов.

Патентообладателями могут быть:

- авторы изобретения, полезной модели, промышленного образца, селекционного достижения; их наследники или иные правопреемники;
- физические и юридические лица (при условии их согласия), указанные автором или его правопреемником в заявлении, поданном в Патентное ведомство

до момента регистрации изобретения, полезной модели, промышленного образца;

- работодатели – в отношении объектов промышленной собственности, созданных работником в связи с выполнением служебного задания, с выплатой последнему вознаграждения в размере и на условиях специального соглашения между ними.

Наследники – могут быть по закону и по завещанию. Если умерший патентообладатель не оставил завещания и не имел законных наследников, то в качестве наследника, в отличие от авторского права, выступает государство в лице Федерального фонда изобретений России.

Патентное ведомство – федеральный орган исполнительной власти, обеспечивающий формирование и осуществление единой государственной политики в области правовой охраны промышленной собственности.

На Патентное ведомство возложены также задачи приема и рассмотрения заявок на изобретения, полезные модели и промышленные образцы;
проведения экспертизы по заявкам; государственной регистрации; выдачи патентов; публикации официальных сведений; издания патентных правил и разъяснений по применению Патентного закона и др.

Патентные поверенные – граждане РФ, имеющие в соответствии с законом право на представительство физических и юридических лиц перед Роспатентом и организациями, входящими в единую патентную службу.

В качестве патентного поверенного может быть аттестован (проверка документов и квалификационный экзамен) и зарегистрирован в Роспатенте (на основании личного заявления) гражданин РФ, имеющий постоянное местожительство в РФ, высшее образование и не менее четырех лет практической работы в этой сфере. Полномочия поверенных на ведение дел подтверждаются доверенностью.

Порядок получения патента

Заявка на выдачу патента на изобретение, полезную модель или промышленный образец подается в федеральный орган исполнительной власти по интеллектуальной собственности лицом, обладающим правом на получение патента в соответствии с настоящим кодексом (заявителем).

Заявление о выдаче патента на изобретение, полезную модель или промышленный образец представляется на русском языке. Прочие документы заявки представляются на русском или другом языке. Если документы заявки представлены на другом языке, к заявке прилагается их перевод на русский язык.

Заявление о выдаче патента на изобретение, полезную модель или

промышленный образец подписывается заявителем, а в случае подачи заявки через патентного поверенного или иного представителя – заявителем или его представителем, подающим заявку.

Требования к документам заявки на выдачу патента на изобретение, полезную модель или промышленный образец устанавливаются на основании 4 части ГК РФ федеральным органом исполнительной власти, осуществляющим нормативно-правовое регулирование в сфере интеллектуальной собственности.

К заявке на выдачу патента на изобретение, полезную модель или промышленный образец прилагается документ, подтверждающий уплату патентной пошлины в установленном размере, или документ, подтверждающий основания освобождения от уплаты патентной пошлины, либо уменьшения ее размера, либо отсрочки ее уплаты.

Заявка на выдачу патента на изобретение (заявка на изобретение) должна относиться к одному изобретению или к группе изобретений, связанных между собой настолько, что они образуют единый изобретательский замысел (требование единства изобретения).

Заявка на изобретение должна содержать:

1) заявление о выдаче патента с указанием автора изобретения и лица, на имя которого испрашивается патент, а также места жительства или места нахождения каждого из них;
2) описание изобретения, раскрывающее его с полнотой, достаточной для осуществления;
3) формулу изобретения, выражающую его сущность и полностью основанную на его описании;
4) чертежи и иные материалы, если они необходимы для понимания сущности изобретения;
5) реферат.

Датой подачи заявки на изобретение считается дата поступления в федеральный орган исполнительной власти по интеллектуальной собственности заявки, содержащей заявление о выдаче патента, описание изобретения и чертежи, если в описании на них имеется ссылка, а если указанные документы представлены не одновременно, – дата поступления последнего из документов.

Правовая охрана патентных прав

Правовая охрана на объекты промышленной собственности начинается с даты поступления заявки в Патентное ведомство и подтверждается патентом на изобретение, промышленный образец или свидетельством на полезную модель.

Заявка на выдачу патента подается автором, работодателем или их правопреемником в Патентное ведомство и должна содержать в себе:

- заявление о выдаче патента;
- описание разработки;
- формулу изобретения, полезной модели;
- чертежи, необходимые для понимания сущности разработки;
- реферат;
- комплект фотографий, макет или рисунок об общем виде изделия. Заявитель имеет право внести исправления и уточнения в материалы заявки без изменения сущности разработки до принятия решения о выдаче

патента. Если изменения были внесены по инициативе заявителя в течение двух месяцев со дня подачи заявки, патентная пошлина за внесение изменений не взимается.

После проведения экспертизы заявки Патентное ведомство при положительном результате устанавливает приоритет разработки и принимает решение о выдаче патента, по истечении 18 месяцев с даты поступления заявки публикует сведения о заявке, публикует в официальном бюллетене сведения о выдаче патента, одновременно внося разработку в соответствующий

Государственный реестр, выдает патент лицу, на имя которого он испрашивался.

В патентном праве различают:

1) личные неимущественные права автора изобретения (право на авторство, право на имя, право на вознаграждение);
2) право на получение патента
3) исключительные (имущественные) права патентообладателя на использование разработок по своему усмотрению;
4) права патентообладателя по распоряжению патентом (уступка прав, выдача разрешения на использование запатентованных разработок).

Право авторства является неотчуждаемым личным правом и охраняется бессрочно.

Имущественные (исключительные) права патентообладателя действуют с даты поступления заявки в Патентное ведомство в течение срока действия

патента (на изобретение – 20 лет, на полезную модель – 10 лет, на промышленный образец – 15 лет) и могут быть продлены. За поддержание патента и его продление патентообладатель обязан платить пошлины.

При признании патента полностью недействительным, при неуплате в установленный срок пошлины либо на основании заявления патентообладателя, действие патента прекращается досрочно.

Правовая охрана в соответствии с Патентным законом не предоставляется секретным изобретениям, полезным моделям, промышленным образцам.

Порядок обращения с такими разработками регулируется специальным

законодательством.

Защита патентных прав

Так же, как и в авторском праве, различают две основные формы защиты:

1. Неюрисдикционная – самозащита гражданами и организациями своих прав. Применяется редко.
2. Юрисдикционная – деятельность уполномоченных государством органов по принудительной защите прав и законных интересов авторов и патентообладателей в общем судебном порядке (через суды) и

административном порядке (через Апелляционную палату Патентного ведомства и Высшую патентную палату).

В судебном порядке рассматриваются следующие споры:

- об авторстве на изобретение, полезную модель, промышленный образец;
- об установлении патентообладателя;
- о нарушении исключительного права на использование охраняемого объекта промышленной собственности и других имущественных прав патентообладателя;
- о заключении и исполнении лицензионных договоров на использование охраняемого объекта промышленной собственности;
- о выплате вознаграждения автору работодателем;
- о выплате компенсаций, предусмотренных Патентным законом.

Обязанность доказывания факта нарушения патента возлагается на патентообладателя.

В судебном порядке различают гражданско-правовые и уголовно- правовые способы защиты прав и законных интересов патентообладателей.

К основным способам гражданско-правовой защиты прав авторов и патентных прав относятся права требовать возмещение убытков виновными нарушителями.

Основным средством уголовно-правовой защиты является жалоба потерпевшего. Уголовная ответственность может наступить лишь в случае причинения крупного ущерба при незаконном использовании изобретения, полезной модели или промышленного образца, разглашения до официальной публикации без согласия автора или заявителя их сущности, присвоения

авторства или принуждения к соавторству, и наказывается штрафом либо лишением свободы на срок до двух лет.

Общие положения об авторских и смежных правах

Источники авторского права

Основным источником авторского права РФ является четвертая часть Гражданского кодекса РФ, а также подзаконные нормативные акты –

постановления Правительства РФ, ведомственные нормативно-правовые акты,

судебная практика, международные договоры и соглашения: Бернская конференция (1971 г.) об охране литературных и художественных
произведений, Всемирная конвенция (1952 г.) об авторском праве, Римская конвенция (1961 г.) об охране прав артистов-исполнителей, изготовителей фонограмм и вещательных организаций и др.

Объекты авторского права

Объектами авторских прав являются произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от
способа его выражения:

- литературные произведения;
- драматические и музыкально-драматические произведения, сценарные произведения;
- хореографические произведения и пантомимы;
- музыкальные произведения с текстом или без текста;
- аудиовизуальные произведения;
- произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;
- произведения декоративно-прикладного и сценографического искусства;
- произведения архитектуры, градостроительства и садово-паркового искусства, в том числе в виде проектов, чертежей, изображений и макетов;
- фотографические произведения и произведения, полученные способами, аналогичными фотографии;
- географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам;
- другие произведения.

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения.

Кроме того, к объектам авторских прав относятся производные произведения, то есть произведения, представляющие собой переработку другого произведения, и составные произведения, то есть произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Авторские права распространяются как на обнародованные, так и на необнародованные произведения, выраженные в какой-либо объективной форме, в том числе в письменной, устной форме (в виде публичного произнесения, публичного исполнения и иной подобной форме), в форме

изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме.
Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей. В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя в соответствии с правилами статьи 1262 ГК РФ.
Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования. Не являются объектами авторских прав:

1) официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы;
2) государственные символы и знаки (флаги, гербы, ордена, денежные знаки и тому подобное), а также символы и знаки муниципальных образований;
3) произведения народного творчества (фольклор), не имеющие конкретных авторов;
4) сообщения о событиях и фактах, имеющие исключительно информационный характер (сообщения о новостях дня, программы телепередач, расписания движения транспортных средств и тому подобное).

Авторские права распространяются на часть произведения, на его название, наперсонаж произведения, если по своему характеру они могут быть признаны самостоятельным результатом творческого труда автора.
Объектами смежных прав являются:

1) исполнения артистов-исполнителей и дирижеров, постановки режиссеров-постановщиков спектаклей (исполнения), если эти исполнения выражаются в форме, допускающей их воспроизведение и распространение с помощью технических средств;
2) фонограммы, то есть любые исключительно звуковые записи исполнений или иных звуков либо их отображений, за исключением звуковой записи, включенной в аудиовизуальное произведение;
3) сообщения передач организаций эфирного или кабельного вещания, в том числе передач, созданных самой организацией эфирного или кабельного вещания либо по ее заказу за счет ее средств другой организацией;
4) базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов;

5) произведения науки, литературы и искусства, обнародованные после их перехода в общественное достояние, в части охраны прав публикаторов таких произведений.

Для возникновения, осуществления и защиты смежных прав не требуется регистрация их объекта или соблюдение каких-либо иных формальностей.

Предоставление на территории Российской Федерации охраны объектам смежных прав в соответствии с международными договорами Российской Федерации осуществляется в отношении исполнений, фонограмм, сообщений передач организаций эфирного или кабельного вещания, не перешедших в общественное достояние в стране их происхождения вследствие истечения установленного в такой стране срока действия исключительного права на эти объекты и не перешедших в общественное достояние в Российской Федерации вследствие истечения предусмотренного настоящим кодексом срока действия исключительного права.

Субъекты авторского права

К субъектам авторского права относятся:

- авторы (в том числе соавторы);
- наследники и иные правопреемники;
- организации, управляющие имущественными правами авторов на коллективной основе.

Субъектами смежных прав являются исполнители, производители фонограмм, организации эфирного или кабельного вещания.

Автор – это любое физическое лицо, независимо от возраста, гражданства и состояния дееспособности, творческим трудом которого создано произведение. Если произведение (в том числе программа для ЭВМ, база данных, топология) создано совместным творческим трудом двух и более физических лиц, каждое из этих лиц признается автором (соавтором).

Наследниками по закону являются только граждане (согласно очередности), а наследниками по завещанию – физические и юридические лица. Если умерший автор не оставил завещания и не имел законных наследников, то его авторские права прекращаются.

Организации, управляющие имущественными правами авторов и обладателей смежных прав на коллективной основе, создаются непосредственно обладателями авторских и смежных прав, действуют на основании устава и выполняют три основных функции: предоставление лицензий пользователям на соответствующие способы использования авторских произведений и объектов смежных прав, сбор вознаграждения за их использование и распределение этого вознаграждения обладателям авторских и смежных прав.

Правовая охрана прав автора и смежных прав

Авторское право на произведение возникает в силу факта его создания, для своего осуществления не требует регистрации произведения, иного специального оформления или соблюдения каких-либо формальностей и носит исключительный характер.

Автору в отношении его произведения принадлежат личные неимущественные права и имущественные (исключительные) права.

Личные неимущественные права принадлежат автору независимо от его имущественных прав, сохраняются за ним в случае уступки (передачи) исключительных прав на использование произведения и включают в себя следующие основные права:

1) право авторства – право признаваться автором произведения;
2) право автора на имя – право использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом или анонимно;
3) право на неприкосновенность произведения – не допускается без согласия автора внесение в его произведение изменений, сокращений и дополнений, снабжение произведения при его использовании иллюстрациями, предисловием, послесловием, комментариями или какими бы то ни было пояснениями;
4) право на обнародование – право обнародовать или разрешать обнародовать произведение в любой форме, включая право на отзыв. Право на отзыв реализуется с возмещением возможных убытков за счет автора.

Права на авторство, на имя, на защиту являются неотчуждаемыми и охраняются бессрочно.

Имущественные права – это исключительные права на использование произведений в любой форме и любым способом, которые включают в себя следующие права:

1) воспроизведение произведения, то есть изготовление одного и более экземпляра произведения или его части в любой материальной форме, в том числе в форме звуко- или видеозаписи, изготовление в трех измерениях одного и более экземпляра двухмерного произведения и в двух измерениях одного и более экземпляра трехмерного произведения. При этом запись произведения на электронном носителе, в том числе запись в память ЭВМ, также считается воспроизведением, кроме случая, когда такая запись является временной и составляет неотъемлемую и существенную часть технологического процесса, имеющего единственной целью правомерное использование записи или правомерное доведение произведения до всеобщего сведения;
2) распространение произведения путем продажи или иного отчуждения его оригинала или экземпляров;

3) публичный показ произведения, то есть любая демонстрация оригинала или экземпляра произведения непосредственно либо на экране с помощью пленки, диапозитива, телевизионного кадра или иных технических средств, а также демонстрация отдельных кадров аудиовизуального произведения без соблюдения их последовательности непосредственно либо с помощью технических средств в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от того, воспринимается произведение в месте его демонстрации или в другом месте одновременно с демонстрацией произведения;
4) импорт оригинала или экземпляров произведения в целях распространения;
5) прокат оригинала или экземпляра произведения;
6) публичное исполнение произведения, то есть представление произведения в живом исполнении или с помощью технических средств (радио, телевидения и иных технических средств), а также показ аудиовизуального произведения (с сопровождением или без сопровождения звуком) в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, независимо от того, воспринимается произведение в месте его представления или показа либо в другом месте одновременно с представлением или показом произведения;
7) сообщение в эфир, то есть сообщение произведения для всеобщего сведения (включая показ или исполнение) по радио или телевидению (в том числе путем ретрансляции), за исключением сообщения по кабелю. При этом под сообщением понимается любое действие, посредством которого произведение становится доступным для слухового и (или) зрительного восприятия независимо от его фактического восприятия публикой. При сообщении произведений в эфир через спутник под сообщением в эфир понимается прием сигналов с наземной станции на спутник и передача сигналов со спутника, посредством которых произведение может быть доведено до всеобщего сведения независимо от его фактического приема публикой. Сообщение кодированных сигналов признается сообщением в эфир, если средства декодирования предоставляются неограниченному кругу лиц организацией эфирного вещания или с ее согласия;
8) сообщение по кабелю, то есть сообщение произведения для всеобщего сведения по радио или телевидению с помощью кабеля, провода, оптического волокна или аналогичных средств (в том числе путем ретрансляции). Сообщение кодированных сигналов признается сообщением по кабелю, если средства декодирования предоставляются неограниченному кругу лиц организацией

кабельного вещания или с ее согласия;

9) перевод или другая переработка произведения. При этом под переработкой произведения понимается создание производного произведения (обработки, экранизации, аранжировки, инсценировки и тому подобного). Под переработкой (модификацией) программы для ЭВМ или базы данных понимаются любые их изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой, за исключением адаптации, то есть внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя;
10) практическая реализация архитектурного, дизайнерского, градостроительного или садово-паркового проекта;
11) доведение произведения до всеобщего сведения таким образом, что любое лицо может получить доступ к произведению из любого места и в любое время по собственному выбору (доведение до всеобщего сведения).

Имущественные права автора могут быть ограничены случаями свободного использования:

1. Свободное воспроизведение произведения в личных целях. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение гражданином исключительно в личных целях правомерно обнародованного произведения, за исключением:
   - воспроизведения произведений архитектуры в форме зданий и аналогичных сооружений;
   - воспроизведения баз данных или их существенных частей;
   - воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса;
   - репродуцирования (пункт 2 статьи 1275) книг (полностью) и нотных текстов;
   - видеозаписи аудиовизуального произведения при его публичном исполнении в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи;
   - воспроизведения аудиовизуального произведения с помощью профессионального оборудования, не предназначенного для использования в домашних условиях.
2. Свободное использование произведения в информационных, научных, учебных или культурных целях. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения, но с обязательным указанием

имени автора, произведение которого используется, и источника заимствования:

- цитирование в оригинале и в переводе в научных, полемических, критических или информационных целях правомерно обнародованных произведений в объеме, оправданном целью цитирования, включая воспроизведение отрывков из газетных и журнальных статей в форме обзоров печати;
- использование правомерно обнародованных произведений и отрывков из них в качестве иллюстраций в изданиях, радио- и телепередачах, звуко- и видеозаписях учебного характера в объеме, оправданном поставленной целью;
- воспроизведение в прессе, сообщение в эфир или по кабелю правомерно опубликованных в газетах или журналах статей по текущим экономическим, политическим, социальным и религиозным вопросам или переданных в эфир произведений такого же характера в случаях, когда такое воспроизведение или сообщение не было специально запрещено автором или иным правообладателем;
- воспроизведение в прессе, сообщение в эфир или по кабелю публично произнесенных политических речей, обращений, докладов и других аналогичных произведений в объеме, оправданном информационной целью. При этом за авторами таких произведений сохраняется право на их опубликование в сборниках;
- воспроизведение или сообщение для всеобщего сведения в обзорах текущих событий средствами фотографии, кинематографии, путем сообщения в эфир или по кабелю произведений, которые становятся увиденными или услышанными в ходе таких событий, в объеме, оправданном информационной целью;
- воспроизведение без извлечения прибыли рельефно-точечным шрифтом или другими специальными способами для слепых правомерно опубликованных произведений, кроме произведений, специально созданных для воспроизведения такими способами.

В случае, когда библиотека предоставляет экземпляры произведений, правомерно введенные в гражданский оборот, во временное безвозмездное пользование, такое пользование допускается без согласия автора или иного правообладателя и без выплаты вознаграждения. При этом выраженные в цифровой форме экземпляры произведений, предоставляемые библиотеками во временное безвозмездное пользование, в том числе в порядке взаимного использования библиотечных ресурсов, могут предоставляться только в помещениях библиотек при условии исключения возможности создать копии этих произведений в цифровой форме.

Создание произведения в жанре литературной, музыкальной или иной пародии либо в жанре карикатуры на основе другого (оригинального)

правомерно обнародованного произведения и использование этой пародии либо карикатуры допускаются без согласия автора или иного обладателя исключительного права на оригинальное произведение и без выплаты ему вознаграждения.

3. Свободное использование произведения путем репродуцирования. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения, но с обязательным указанием имени автора, произведение которого используется, и источника заимствования репродуцирования в единственном экземпляре без извлечения прибыли:

~ правомерно опубликованного произведения библиотеками и архивами для восстановления, замены утраченных или испорченных экземпляров произведения и для предоставления экземпляров произведения другим библиотекам, утратившим их по каким-либо причинам из своих фондов;

~ отдельных статей и малообъемных произведений, правомерно опубликованных в сборниках, газетах и других периодических изданиях, коротких отрывков из правомерно опубликованных письменных произведений (с иллюстрациями или без иллюстраций) библиотеками и архивами по запросам граждан для использования в учебных или научных целях, а также образовательными учреждениями для аудиторных занятий.

Под репродуцированием (репрографическим воспроизведением) понимается факсимильное воспроизведение произведения с помощью любых технических средств, осуществляемое не в целях издания. Репродуцирование не включает воспроизведение произведения или хранение его копий в
электронной (в том числе в цифровой), оптической или иной машиночитаемой форме, кроме случаев создания с помощью технических средств временных
копий, предназначенных для осуществления репродуцирования.

4. Свободное использование произведения, постоянно находящегося в месте, открытом для свободного посещения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение, сообщение в эфир или по кабелю фотографического произведения, произведения архитектуры или произведения изобразительного искусства, которые постоянно находятся в месте, открытом для свободного посещения, за исключением случаев, когда изображение произведения таким способом является основным объектом этого воспроизведения, сообщения в эфир или по кабелю либо когда изображение произведения используется в коммерческих целях.
5. Свободное публичное исполнение музыкального произведения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения публичное исполнение музыкального произведения во время официальной или религиозной церемонии либо похорон в объеме, оправданном

характером такой церемонии.

6. Свободное воспроизведение произведения для целей правоприменения. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение произведения для осуществления производства по делу об административном правонарушении, для производства дознания, предварительного следствия или осуществления судопроизводства в объеме, оправданном этой целью.
7. Свободная запись произведения организацией эфирного вещания в целях краткосрочного пользования. Организация эфирного вещания вправе без согласия автора или иного правообладателя и без выплаты дополнительного вознаграждения делать запись в целях краткосрочного пользования того произведения, в отношении которого эта организация получила право на сообщение в эфир, при условии, что такая запись делается организацией эфирного вещания с помощью ее собственного оборудования и для собственных передач. При этом организация обязана уничтожить такую запись в течение шести месяцев со дня ее изготовления, если более продолжительный срок не согласован с правообладателем или не установлен законом. Такая запись может быть сохранена без согласия правообладателя в государственных или муниципальных архивах, если она носит исключительно документальный характер.
8. Свободное воспроизведение программ для ЭВМ и баз данных. Декомпилирование программ для ЭВМ. Лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного вознаграждения:

~ внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя и осуществлять действия, необходимые для функционирования таких программ или базы данных в соответствии с их назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также осуществить исправление явных ошибок, если иное не предусмотрено договором с правообладателем;

~ изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована в иных целях, чем цели, указанные выше, и должна быть уничтожена, если владение экземпляром таких программы или базы данных перестало быть правомерным.

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления действий, предусмотренных предыдущим подпунктом.
Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст
(декомпилировать программу для ЭВМ) или поручить иным лицам
осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, присоблюдении следующих условий:

- информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;
- указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;
- информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

По общему правилу авторское право действует в течение всей жизни
автора и 70 лет после его смерти, начиная с 1 января года, следующего после смерти.
Имущественные права передаются по договору. Имущественные права на использование служебного произведения принадлежат работодателю, если в договоре между ним и автором не предусмотрено иное.
Правообладатель для оповещения о своих авторских правах на каждом экземпляре произведения вправе использовать знак охраны авторского права, состоящий из трех элементов: буквы «С» в окружности или в круглых скобках (С); имени правообладателя, года первого опубликования (выпуска в свет) произведения; для оповещения о смежных правах на фонограмму – указывать

знак охраны в виде прописной буквы «Р», информации о самом правообладателе, года первого наименования фонограммы.

Исполнители (артисты, режиссеры, дирижеры) имеют как личные преимущественные, так и имущественные права при условии соблюдения ими прав автора исполняемого произведения, остальные объекты – только имущественные права.

Имущественные права обладателей смежных прав обеспечиваются их исключительным правом на использование исполнения, постановки, фонограммы, передачи в любой форме, в том числе право на вознаграждение за каждый вид использования исполнения, постановки, фонограммы, представления разрешения на использование передачи.

Защита авторских и смежных прав

Под защитой понимается совокупность мер, предусмотренных законом, по признанию, восстановлению прав и законных интересов их обладателей при нарушении или оспаривании этих прав и интересов.

Различают две основные формы защиты:

1) неюрисдикционная – самозащита гражданами и организациями своих прав и законных интересов в порядке необходимой обороны и крайней необходимости (отказ совершить определенные действия; отказ от исполнения договора в целом и т. п.). Применяется редко;
2) юрисдикционная – деятельность уполномоченных государством органов по принудительной защите прав и законных интересов их обладателей в судебном порядке или административном порядке.

Основным средством защиты в судебном порядке является иск, а в административном порядке – жалоба.

В судебном порядке различают по способам защиты прав и ответственности гражданско-правовые, административные и уголовно- правовые.

К основным способам гражданско-правовой защиты исключительных прав и законных интересов относится право требовать от нарушителя:

- признания прав;
- восстановления положения, существовавшего до нарушения права;
- прекращение действий, нарушающих право или создающих угрозу его нарушению (запрет на воспроизведение, на выпуск в свет, на распространение и т. п.);
- возмещение убытков;
- взыскания дохода, полученного нарушителем вследствие нарушения прав;

- выплаты компенсации в определенных законом пределах;
- возмещения морального ущерба;
- прекращения или изменения договора в связи с действиями нарушителя;
- запрет совершать определенные действия ответчику (изготовление, воспроизведение, продажу, прокат и др.).

В случае наступления административной ответственности применяются:

- взыскание штрафа;
- обязательная конфискация по решению суда контрафактных (изготовленных или используемых с нарушением авторских прав) экземпляров произведений или фонограмм либо материалов и оборудования, используемых для их изготовления.

Контрольные вопросы

1. Перечислите основные законодательные акты, регламентирующие защиту интеллектуальной собственности.
2. Какие существуют институты защиты интеллектуальной собственности?
3. Перечислите и охарактеризуйте основные объекты интеллектуальной собственности.
4. Дайте определение понятиям «Изобретение», «полезная модель», «промышленный образец».
5. Назовите объекты патентного права.
6. Какие объекты патентного права не являются изобретениями?
7. Охарактеризуйте правовую основу защиты промышленного образца.
8. Перечислите и охарактеризуйте субъекты патентного права.
9. Перечислите объекты и субъекты авторского права.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 17-18.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 17-18
Безопасность информационной инфраструктуры

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин

Учебная и воспитательная цели:

Изучить понятие информационной инфраструктуры и теорию безопасности ее. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

1 Теория обеспечения безопасности информационной инфраструктуры

Краткие теоретические или справочно-информационные материалы

1 Теория обеспечения безопасности информационной инфраструктуры

Понятие «информация» — одно из базовых понятий теории обеспечения информационной безопасности. Объем явлений, охватываемых этим понятием, во многом определяет предмет обеспечения безопасности, характер угроз и методы противодействия этим угрозам.

В настоящее время отсутствует общепринятое представление о том, что такое информация. Однако критический анализ известных определений позволяет считать, что **информация —** это явление жизни организмов, заключающееся в отражении окружающей действительности для оценки происходящих в ней изменений и выбора системы действий по приспособлению

к этим изменениям.
Каждый тип организма обладает свойственной только ему совокупностью средств адаптации к изменениям окружающей действительности, что позволяет в определенных пределах обеспечивать приемлемые условия для протекания биохимических процессов, составляющих сущность организма. Уникальность средств адаптации каждого типа организмов обусловливает, в свою очередь, уникальность его «информационного» взгляда на мир, во многом не пересекающегося с «мировоззрением» других видов организмов.
По содержанию **информация** — это результат отображения в организме движения объектов окружающей действительности, включающей как материальную, так и нематериальную составляющие.
Известно, что материя в качестве субстанции выступает как объективная реальность, рассматриваемая со стороны ее внутреннего единства, безотносительно ко всем тем бесконечно многообразным видоизменениям, в которых она существует.
К числу самых важных категорий философии, обозначающих атрибуты материи, относят движение, отражение и взаимодействие.
Категория «движение» в материалистической философии определяет различные типы изменчивости, наблюдаемые в объективном мире начиная от перемещения объектов в пространстве и кончая процессами биологической и социальной эволюции. Категория «отражение» охватывает проявления свойства одних объектов материального мира воспроизводить в их природе особенности других взаимодействующих с ними объектов, т.е. свойства сохранять «следы» некоторых характеристик объектов взаимодействия. Наконец, категория
«взаимодействие» описывает явления взаимного изменения объектов материального мира в процессе их движения.
Отражение взаимосвязано с взаимодействием и движением. Везде, где имеет место движение и взаимодействие, присутствует отражение.
В философии принято различать отражение в неживой и живой природе. В неживой природе отражение носит пассивный характер. Оно проявляется в виде

соответствующих изменений физических или химических свойств и состояний объектов, происходящих в результате внешнего воздействия. Отражение дви- жения объектов материального мира в организмах, как было отмечено ранее, связано с изменением происходящих в них биохимических преобразований. Продукты измененных биохимических преобразований составляют материальную основу результата отражения движения в организмах, т.е. информации, а отраженный в организме образ действительности — его нематериальную основу.

В мире взаимодействующих организмов информация проявляется в форме сведений и в форме сообщений.

Сведения представляют собой результат отражения окружающей действительности в организме.

Как уже было отмечено, каждый тип организмов обладает определенной, свойственной только ему «информационной» моделью мира. Эта модель возникает на основе обобщения сведений, отражаемых и накапливаемых организмом. Получаемые организмом сведения служат, с одной стороны, для формирования и актуализации «информационной» модели, выявления изменения состояния объектов материального мира, а с другой — для оценки возможных последствий выявленных изменений для существования организма и выбора рационального «варианта поведения». Структура «информационной» модели определяется генотипом организма. В наиболее простом виде данная модель включает отражаемые объекты реального мира, характеристики их состояния, оценки возможного влияния состояния этих объектов на жизнедеятельность организма, набор вариантов «поведения» организма в ситуациях, требующих реагирования, а также отношения (связи) между характеристиками состояния отражаемых объектов и вариантами «поведения».

Можно предположить, что «информационная» модель организмов, не обладающих большим разнообразием вариантов адаптации к изменениям окружающей действительности, имеет жесткую структуру, которая остается неизменной в течение их жизни. Структура «информационной» модели

организмов с достаточным разнообразием таких вариантов является гибкой, т.е. в определенных пределах может изменяться, накапливая сведения об окружа- ющем мире.

Организмы, обладающие развитой нервной системой и психикой, имеют более широкие возможности как по модификации структуры «информационной» модели, так и по оперированию с содержащимися в ней сведениями. В частности, эти организмы способны вырабатывать **знания,** представляющие собой специфический вид сведений, отражающих закономерности изменения окружающей действительности и результативности использования имеющихся средств адаптации к данным изменениям. Специфика знаний заключается в том, что они являются результатом не непосредственного отражения движения каких-либо объектов действительности, а обобщения сведений о движениях этих объектов, накопленных в «информационной» модели. Знания позволяют организму прогнозировать на основе отражения реальной действительности позитивные и негативные последствия происходящих изменений или осуществляемых действий, что существенно повышает возможности его «комфортного» существования и выживания. Можно предположить, что способность выявления знаний появляется у организмов тогда, когда число возможных вариантов
«поведения» становится значительным и их рефлекторное использование не позволяет обеспечить приемлемую эффективность адаптации.

Исключительно важную, с рассматриваемой точки зрения, часть живого мира образуют социальные организмы, условием существования которых является взаимодействие с другими такими же организмами. Их
«информационные» модели, кроме сведений, получаемых самостоятельно, включают сведения, поступающие от других членов социума. Способность обмениваться сведениями реализуется через отправку и получение информации в форме сообщений.

Сообщение представляет собой набор знаков, с помощью которых сведения, накопленные одним организмом, могут быть переданы другому организму и восприняты им.

Способность обмениваться информацией реализуется организмами путем определенных алгоритмов кодирования сведений, т.е. Превращения их в набор знаков, воспринимаемых другими организмами и составляющих содержание сообщений, и алгоритмов декодирования поступающих сообщений, т.е. превращения набора знаков в сведения. При этом совершенно несущественно, каким именно способом осуществляется передача сообщения и какой набор знаков использован для его формирования.

Сведения, получаемые организмом от других организмов, образуют социальную составляющую его «информационной» модели мира, а совокупность этих составляющих «информационных» моделей взаимодействующих организмов — распределенную «информационную» модель социума, его «коллективный разум»-

Одними из социальных организмов, существующих на Земле, являются человек и общество, которые обладают способностью отражать окружающую действительность в своей «информационной» модели мира в виде сведений, накапливать сведения, обобщать их и формировать знания, а также обмениваться сведениями с другими людьми и обществами.

С этой точки зрения информация представляет собой явление жизни и человека и общества, важнейший фактор их существования.

Информация в выделенных формах обладает во многом отличающимися свойствами, содержание которых отражено на рис. 2.

Приведенная трактовка сущности, содержания и форм информации не противоречит тому, как это понятие раскрывается и обыденной жизни и в праве. Так, в справочной литературе под информацией понимается «информирование о положении дел в какой-либо области, о каких-либо событиях; сообщение о поло- жении дел где-либо, о каких-либо событиях; сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальными устройствами». В федеральном законодательстве дефиниция «информация» раскрывается как «сведения (сообщения, данные) независимо от формы их представления»[2]. Понятие «данные» можно рассматривать как разновидность

сообщений, предназначенных для автоматизированной обработки с использованием средств вычислительной техники. Эти сведения (сообщения, данные) могут отражать характеристики состояния объектов (лиц, предметов, фактов, событий) или движения конкретных объектов (явлений, процессов) окружающей действительности.

Не умаляя фундаментального характера теории информации, разработанной К.Шенноном, и методологического подхода к исследованию окружающей действительности, составляющего ос**нову** разработанной Н. Винером кибернетики, можно отметить, **что** используемая ими концепция «информации» ограничивается рассмотрением только той составляющей этого явления, которая **имеет** форму сообщений. Применительно к ней раскрываются закономерности, связывающие количество двоичных знаков (би**тов),** достаточных для описания одной буквы или знака сообще**ния** (количество информации), с пропускной способностью ка**нала** связи, характеризуемой максимальным количеством инфор**мации** (битов, достаточных для описания одного знака), которое **можно** передать по нему за одну секунду.

Таблица 2 - Формы информации и ее свойства

Формы информации	
Сведения – это результат отражения окружающей действительности в организме	Сообщения – это набор знаков, с помощью которого сведения, накопленные одним организмом, могут быть переданы другому организму и восприняты им
Свойства	
Духовность – это невозможность восприятия органами чувств	Материальность – способность воздействовать на органы чувств
Субъективность – зависимость количества и ценности сведений от получающего субъекта	Объективность – независимость от получающего их субъекта

Неуничтожаемость – невозможность физического уничтожения	Уничтожаемость – возможность физического уничтожения
Динамичность – возможность изменения отношений между объектами материального мира, запечатленными в организме, и их характеристиками	Статичность – независимость набора знаков от времени, прошедшего с момента создания
Ограниченная воспроизводимость – невозможность точного воспроизведения без закрепления на некотором носителе	

Вообще говоря, между количеством информации по К. Шен***нону*** (т.е. количеством битов, достаточных для передачи одного ***знака*** сообщения) и количеством сведений (т.е. количеством но***вых*** элементов «информационной» модели человека, которые воз***никают*** вследствие осознания им сообщения) трудно установить ***Какое*** бы то ни было соотношение. Единственное, что можно в связи с этим отметить: если предположить, что каждый бит соответствует некоторому знаку, а знак, в свою очередь,

— элементу части передаваемой «информационной» модели, то количество информации по К.Шеннону позволяет оценить количество знаков, достаточных для кодирования этой части модели.

Теория информации К. Шеннона безусловно вскрыла ряд объективных закономерностей природы. В процессе развития этой теории последователями Шеннона произведено существенное расширение трактовки понятия «информация». «У большинства из тех, кто думал над этим кругом проблем, возникло предчувствие, что достаточно сделать небольшое обобщение, похожее на сделанное в свое время обобщение понятия энергии, и термин «информация» поможет установить какую-то глубинную закономерность нашего мира, эквивалентную по своему познавательному значению закону сохранения энергии». К сожалению, этого пока не произошло.

Другим выдающимся достижением, оказавшим существенное влияние на превращение понятия «информация» в общенаучную категорию, были разработанные Н.Винером основы кибернетики. Введенный им термин «кибернетика» был предназначен для обозначения всей теории управления и связи в машинах и живых организмах. В рамках этой работы Н.Винер также

пришел к понятию количества информации, но в результате изучения не проблем кодирования информации, а проблем сообщений и шумов в электрических фильтрах.

Наиболее известным научным результатом работы Н.Винера можно считать открытие достаточно широкого класса задач, связанных с поддержанием целенаправленного функционирования динамических объектов, а также метода «управления с помощью информирующей обратной связи», используемого в этих объектах. Существо этого метода в упрощенном виде может быть сфор- мулировано как использование при управлении не только сведений о том, как должен двигаться управляемый объект, но и сведений о том, как он двигается к поставленной цели на самом деле. Для этого оцениваются отклонения параметров движения объекта от требуемых значений, на основе которых формируются управляющие воздействия на движущие элементы объекта в целях внесения требуемых изменений в это движение. Для реализации данного метода требуется наличие системы связи, передающей сообщения от управляющего центра к управляемым движителям и обратно, что, естественно, требует исследования и собственно сообщений.

Объекты, в которых используется указанный метод управления, как правило, описываются линейными дифференциальными уравнениями, решения которых инвариантны к временным сдвигам. Широкая распространенность таких объектов в реальной жизни обусловила и большую востребованность кибернетических идей и методов при решении практических задач в различных сферах человеческой деятельности.

В то же время между управлением в технических системах и управлением в биологических и социальных системах наряду с наличием общих черт существуют и определенные различия. В биологических и социальных системах, как следует из вышеизложенного, управление осуществляется с использованием сведений, а в технических системах — с использованием сообщений. Вследствие этого управление в биологических и социальных системах не имеет той жесткости, которая свойственна управлению в технических системах. Если в

технической системе для оказания управляющего воздействия достаточно отправить сообщение или сигнал, то в биологических и социальных системах этого не всегда достаточно. Это особенно наглядно проявляется на примере социальных систем, в которых для реализации управляющего воздействия, как правило, требуется приложить определенные дополнительные усилия, чтобы индивиды, составляющие социальную систему, согласились выполнять такое управляющее воздействие.

Если в качестве управляемого объекта выступают отдельные органы человеческого организма, то управление практически не отличается от аналогичного процесса в технических системах. Это обусловлено особенностями человеческого организма, которые заключаются в том, что все его внутренние органы работают, как правило, независимо от сознания и с точки зрения управления образуют самостоятельные биологические системы со своей «ин- формационной» моделью, слабо связанные с «информационной» моделью, используемой сознанием человека. Система управления такими органами и была выбрана Н.Винером в качестве объекта исследования. Если бы в качестве объекта исследования выступало сознание, то система управления выглядела бы значительно сложнее.

Передача сообщений через естественную среду обитания — воз- дух — обеспечивает обмен сведениями между индивидами, однако обладает рядом объективных ограничений по дальности и оперативности осуществления информационного обмена, по длительности хранения переданных сообщений и возможности их ретроспективного анализа. Эти ограничения, в свою очередь, сказываются на активности информационного взаимодействия между индивидами и, соответственно, на развитии социума, использовании имеющихся у него ресурсов и сил для адаптации к изменяющимся условиям существования.

Преодоление выделенного ограничения связано с созданием искусственной среды передачи информации, которая придаст процессу информационного взаимодействия новое качество. Способность организмов создавать такую искусственную среду существенно зависит от имеющихся у них

средств воздействия на окружающую действительность и от способности использовать коллективные действия для повышения эффективности адаптации. Наибольшими возможностями осуществления подобной деятельности обладает человек. Можно сказать, что если информация — явление жизни человека и общества, то **информационная инфраструктура —** это явление социальной жизни индивидов. Сущность данного явления заключается в разрешении противоречия между социально обусловленными потребностями в информационном обмене между членами общества для решения задач эконо- мического, социального, политического и духовного развития и исторически обусловленными социальными и техническими возможностями удовлетворения
этих потребностей.

Содержание данного явления общественной жизни определяется совокупностью используемых обществом информационных технологий и технических систем, реализующих эти технологии, а также совокупностью социальных институтов, обеспечивающих создание, эксплуатацию и модернизацию технических систем обеспечения информационного взаимодействия.

Ключевым элементом информационной инфраструктуры, во многом определяющим ее содержание, являются информационные технологии. Под информационной технологией понимается упорядоченная совокупность методов обработки сообщений, включающих поиск, сбор, хранение, передачу и распространение сообщений, а также их предоставление человеку.

Информационная инфраструктура по форме — это совокупность социально-технических систем, реализующих функции обеспечения информационного взаимодействия, и общественно поддерживаемого порядка использования данных систем в жизни человека и общества.

В информационной инфраструктуре современного общества выделяют три основных сегмента: субъектный, общественный и смешанный.

Субъектный сегмент ориентирован на обеспечение информационного обмена в интересах отдельных субъектов информационной сферы и образуется

инфраструктурами сетей связи и информатизации индивидуального пользования.
Сети связи представляют собой технологические системы, включающие средства и линии связи и предназначенные для осуществления электросвязи или почтовой связи[1]. Понятие «электросвязи» раскрывается в законодательстве как
«любые излучения, передача или прием знаков, сигналов, голосовой инфор- мации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам». Дефиниция «почтовая связь» в законодательстве определена как «вид связи, представляющий собой единый производственно-технологический комплекс технических и транспортных средств, обеспечивающий прием, обработку, перевозку, доставку (вручение) почтовых отправлений, а также осуществление почтовых переводов денежных средств».
Особое значение для удовлетворения потребностей общества в информационном обмене имеет федеральная связь, объединяющая все организации и государственные органы, осуществляющие и обеспечивающие электросвязь и почтовую связь на территории Российской Федерации[4].
Можно сказать, что в рамках сети связи сосредоточены все основные технологические средства передачи информации в форме сообщений в интересах граждан, субъектов, представляющих социальные институты общества, государственных органов.
Инфраструктура информатизации индивидуального пользования призвана обеспечить «организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов». Она определяется совокупностью информационных технологий, информационных ресурсов и систем, средств, обеспечивающих возможность использования информационных ресурсов и систем субъектами информационной сферы, систем автоматизированного управления, систем автоматизации производства, а

также кадров, обеспечивающих их эксплуатацию. При этом технологическую основу инфраструктуры информатизации субъектов составляют информационные ресурсы, информационные технологии и Федеральный закон
«О связи» от 18 июня 2003 г. Ст. 2. Там же. Ст. 2. Федеральный закон «О почтовой связи» от 17 июля 1999 г. Ст. 2. А Федеральный закон «О связи» от 18 июня 2003 г. Ст. 11, п. 1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. Ст.

2. телекоммуникационные системы, обеспечивающие возможность удаленного доступа субъектов к информационным ресурсам и системам.

Общественный сегмент информационной инфраструктуры ориентирован на обеспечение информационного обмена в интересах общества и государства и образуется инфраструктурами средств массовой информации и информатизации общего пользования.

Средства массовой информации представляют собой «периодическое печатное издание, радио-, теле-, видеопрограмму, кинохроникальную программу, иную форму периодического распространения массовой информации», т.е. печатных, аудио-, аудиовизуальных и иных сообщений и материалов, предназначенных для неограниченного круга лиц. При этом под массовой информацией понимаются «предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы», а под периодическим печатным изданием — «газета, журнал, альманах, бюллетень, иное издание, имеющее постоянное название, текущий номер и выходящее в свет не реже одного раза в год». Другими словами, средства массовой информации есть издание (радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации), отличающееся наличием трех признаков: постоянным названием, текущим номером и определенной периодичностью выхода в свет.

Средства информатизации общего пользования образуются сово- купностью открытых информационных ресурсов библиотек, архивных и музейных фондов, а также открытых государственных информационных

ресурсов, обеспечивающих свободный доступ граждан к сведениям о деятельности государственных органов, к публикуемым ими нормативным правовым актам и другой общественно значимой информации.

Смешанный сегмент информационной инфраструктуры представляет собой совокупность инфраструктур глобальных информационно- телекоммуникационных систем.

Основной составляющей смешанного сегмента информационной инфраструктуры являются глобальные информационно-телекоммуникационные системы (например, система Интернет) — совокупность средств связи и информатизации, предназначенных как для обеспечения информационного взаимодействия между конкретными субъектами, так и для распространения массовой информации для неограниченного круга лиц.

Функциональные возможности данного сектора информационной инфраструктуры определяются, с одной стороны, имеющимися в его составе средствами получения и передачи сообщений между отдельными субъектами, сбора и хранения полученной информации, а с другой — средствами производства и распространения массовой информации посредством установления информационного взаимодействия отдельного субъекта с неогра- ниченным количеством других субъектов.

Основные сегменты информационной инфраструктуры представлены на рис. 3.

Общей особенностью использования средств информационной инфраструктуры для осуществления информационного взаимодействия является наличие посредника между субъектами, устанавливающими информационное взаимодействие.

В качестве такого посредника могут выступать конкретные физические или юридические лица (посыльный, фельдъегерская служба, телефонная компания), выполняющие функции либо установления информационного взаимодействия, либо предоставления возможности для информационного взаимодействия. Данное обстоятельство обусловливает возникновение

определенных общественных отношений между посредником и обслуживаемыми им субъектами.

С появлением электрической связи, развитием глобальных *ин-* формационно-телекоммуникационных систем функции посредника все больше смещаются в сторону предоставления возможностей информационного взаимодействия.

Таблица 3 - Сегменты информационной инфраструктуры

Сегменты информационной инфраструктуры		
Субъектный	Общественный	Смешанный
Образуются		
инфраструктурами связи и информатизации индивидуального пользования	инфраструктурами СМИ и информатизации общего пользования	инфраструктурами глобальных информационно-коммуникационных систем
Применяются		
для информационного взаимодействия отдельных субъектов	для обеспечения информационного взаимодействия неограниченного круга лиц	для обеспечения информационной деятельности как отдельных субъектов, так и неограниченного круга лиц

Отчетность за занятие

1 Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.

2 Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

1 *Белл Д.* Грядущее постиндустриальное общество. Опыт социального прогнозирования / пер. под ред. В. Л. Иноземцева. — М., 1999.
2 *Гейтс Б.* Дорога в будущее. — М., 1994.
3 *Зиновьев А.А.* На пути к свсрхобществу. — М.: Центрполиграф, 2000.
4 *Иноземцев В.Л.* К теории постэкономической общественной форма- ции. — М,, 1995.
5 *Иноземцев В.Л.* Современное постиндустриальное общество: приро- да, противоречия, перспективы. — М.: Логос, 2000.
6 *Тоффлер О.* Третья волна. — М., 1995.
7 *Чоговадзе Г. Г.* Информация. Общество. Человек. — М.: Дата+, 2003.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности

Для выполнения практического занятия студент должен:

1 Ознакомиться с методикой и порядком выполнения работы.

2 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.

3 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

~ работать без соответствующего освещения и вентиляции рабочего места;

~ работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;

~ передвигаться по аудитории без разрешения преподавателя;

работать в специализированных аудиториях без сменной обуви;
работать на одном рабочем месте более двух человек.

4 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.

5 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы
Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов
Не требуется

Порядок оформления отчета по практическому занятию и его защиты Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на вопросы для контроля владения
компетенциями работы.

Рекомендации для преподавателей по проведению занятия
К защите требуется отчет с подробными ответами на вопросы.

Задания для контроля владения компетенциями:

1 Что такое информация?
2 Каковы основные формы и свойства информации?
3 Что такое информационная инфраструктура?
4 Каковы основные составляющие информационной инфраструктуры?

Содержание отчета о практическом задании
По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 19.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 19
Система обеспечения информационной безопасности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 90 мин
Вступительная часть 2 мин
Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Учебная и воспитательная цели:

Изучить теорию обеспечения информационной безопасности организации и Российской Федерации. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

1 Обеспечение информационной безопасности организации
2 Обеспечение информационной безопасности Российской Федерации

Краткие теоретические или справочно-информационные материалы 1 Обеспечение информационной безопасности предприятия

При всем многообразии видов организаций, направлений и масштабов их деятельности, численности участников **основными объектами обеспечения информационной безопасности,** как правило, являются:

- информация в форме сведений (сведения об участниках орга- низации, о состоянии рынка и ее активов; репутация организации и доброе имя участников организации и т.п.);
- информация в форме сообщений (документы, закрепляющие права собственности организации на материальные и нематериальные активы; документация бухгалтерского учета, налоговые декларации, договоры на выполнение работ и оказание услуг, документация на выпускаемые изделия и т.п.);
- информационная инфраструктура (автоматизированные системы обработки информации и технологического управления; техническое и программное обеспечение информационных и коммуникационных систем и сетей связи, используемых в организации, и т.п.);
- правовой статус организации как субъекта информационной сферы (права на объекты интеллектуальной собственности, на выполнение работ и оказание услуг, на доступ к открытой информации государственных органов, на коммерческую тайн} и т.п., а также обязанности по представлению в уполномоченные государственные органы сведений о результатах экономической деятельности, по соблюдению режима персональных данных, по представлению заинтересованным лицам документов в случае направления заявки на участие в конкурсах и аукционах и т.п.).

Наиболее опасные угрозы безопасности этих объектов проявляются в следующих формах:

- мошенничество, связанное с завладением чужим имуществом или приобретением права на него путем обмана или злоупотребления доверием, основанных на неправомерном доступе к информационно-коммуникационным системам, конфиденциальной информации, на подделке или искажении электронных документов в информационных и коммуникационных системах, сетях следующие:
- клевета, основанная на распространении заведомо ложной информации, порочащей честь и достоинство руководителей орга**низации;**
- нарушение авторских и смежных прав, связанных с объектами интеллектуальной собственности;
- шантаж, связанный с угрозой распространения персональ**ных** данных, иной информации, охраняемой законом в режиме **тайны;**
- противоправное раскрытие информации ограниченного доступа третьим лицам;
- уничтожение или повреждение информационных ресурсов, информационно-коммуникационных систем и сетей связи посредством использования и распространения вредоносных программ, нарушения правил эксплуатации ЭВМ и их сетей;
- причинение имущественного ущерба собственнику или иному владельцу информационно-коммуникационных систем и се**тей** связи путем обмана или злоупотребления доверием без признаков хищения.

Вследствие проявления указанных угроз существенно возрас**тают** риски,

связанные с осуществлением основной деятельнос**ти** организации (риск утраты репутации, риск ликвидности, операционные риски, риски утраты собственности или важных ак**тивов** организации). Эти риски связаны с возможностью возникновения ситуаций проявления угроз, требующих дополнитель**ных,** часто существенных затрат материальных, людских, вре**менных,** финансовых и иных ресурсов на ликвидацию послед**ствий** проявления угроз. Увеличение рисков приводит к увеличе**нию** издержек и соответствующему снижению эффективности деятельности организации, уменьшению ее конкурентоспособ- **ности.**

Система обеспечения информационной безопасности организация характеризуется двумя составляющими: деятельностью по подготовке и реализации мер, направленных на противодействие проявлению угроз информационной безопасности и минимиз**ацию** последствий этих проявлений; субъектами этой деятельности.

Деятельность по обеспечению информационной безопасности организаций базируется на следующих основных принципах:

- законность, заключающаяся в строгом и неуклонном испол**нении** норм законодательства Российской Федерации, соблюдении прав и свобод человека и гражданина;
- непрерывность, предполагающая рассмотрение деятельности в качестве одной из функций организации;
- комплексность, заключающаяся во всестороннем анализе факторов, оказывающих влияние на риски информационной безвинности, при планировании данной деятельности и использовании всех имеющихся возможностей и выделенных ресурсов для реализации составленных планов;
- замкнутость, заключающаяся в совместном осуществлении деятельности по предупреждению проявления угроз, снижению их опасности, выявлению проявлений угроз, минимизации последствий этих проявлений, а также по оценке эффективности выполнения планов противодействия угрозам и их соответствующего уточнения.

В этой деятельности широко используются методы поощрения, убеждения и принуждения.

Меры по противодействию проявлению угроз информационной безопасности организации и минимизации последствий этих проявлений охватывают три основных направления деятельности:

- управление персоналом;
- организация объектового режима;
- организационно-техническое обеспечение.

Меры по управлению персоналом направлены на минимизацию рисков, связанных с проявлением личностных свойств и качеств участников организации, а также взаимодействующих с ней субъектов. Они включают подбор и расстановку кадров, обеспечение должной мотивации сотрудников к добросовестной работе, подготовку и повышение их квалификации.

Меры по организации объектового режима нацелены на минимизацию рисков, связанных с возможными попытками нанесения ущерба организации ее участникам и взаимодействующим с ней субъектам. Эти мероприятия включают осуществление пропускного и внутриобъектового режимов, в том числе установ- ление и поддержание режимов информации, информационно- коммуникационных систем и систем связи, контроль поддержания установленных режимов и проведение служебных расследований по фактам их нарушения. При этом режимы информационно-коммуникационных систем и систем связи направлены на достижение требуемых значений основных свойств безопасности используемых в организации информационных технологий: конфиденциальности, целостности и готовности к использованию.

Меры по организационно-техническому обеспечению позволяют использовать возможности техники для установления и поддержания объектового режима. Они включают мероприятия по использованию средств защиты информации, информационных и коммуникационных систем, средств связи, а также по установлению и реализации политики безопасности в информационно-ком- муникационных системах.

Важную роль в эффективной реализации мер по противодействию угрозам информационной безопасности играет нормативно-методическое обеспечение.

Основными субъектами обеспечения информационнои **безопасности организаций** являются создаваемые в них координационные (например, советы по безопасности информационных технологий) и кадровые органы, специализированные структурные подразделения по вопросам информационной

безопасности или должностные лица, а также структурные образования, специализирующиеся на оказании услуг в данной области, объединяемые в единую систему.

Структура указанной системы и ее составных частей может быть различной. Например, в организации может быть создан совет по безопасности информационных технологий, который решает вопросы выработки внутренней политики в этой области, ее реализации и нормативно-методического обеспечения.

Для качественного выполнения данных функций в состав совета включают представителей высшего руководства организации и должностных лиц, осуществляющих непосредственное управление обеспечением информационной безопасности. В некоторых случаях управление этой деятельностью может быть возложено на ответственных сотрудников соответствующих структурных подразделений.

2 Обеспечение информационной безопасности Российской Федерации

Осуществление деятельности по обеспечению информационной безопасности Российской Федерации возложено на государство, которое в соответствии с законодательством является основным субъектом обеспечения безопасности.

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

В соответствии с Доктриной информационной безопасности Российской Федерации национальные интересы в информационной **сфере** включают следующие основные составляющие:

- 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;

- информационное обеспечение государственной политики Рос- сийской Федерации;
- развитие современных информационных технологий, отечественной индустрии информации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на Мировой рынок;
- обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- защита национальных информационных ресурсов от несанк- ционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Основными объектами обеспечения информационной безопасности Российской Федерации являются ее национальные интересы:

- информация в форме сведений (свобода мысли, национальные культурные ценности);
- информация в форме сообщений (архивные документы; документы, являющиеся музейными предметами или составляющие музейные коллекции; тиражированные документы);
- информационная инфраструктура (сети связи и инфраструктура информатизации; инфраструктура средств массовой информации и книгоиздания; инфраструктура открытых информационных ресурсов библиотек, архивных и музейных фондов);
- правовой статус субъектов информационной сферы Российской Федерации (совокупность реальных прав и обязанностей субъектов).

К угрозам информационной безопасности Российской Федерации**,** в частности, относятся:

- противодействие реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- противоправные сбор и использование информации;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи,

дешифрование этой информации и навязывание ложной информации;

- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктурь;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение ин**формации.**

Деятельность по обеспечению информационной безопасности Российской **Федерации** осуществляется на основе принципов, разделяемых на общие и особенные.

К наиболее важным общим принципам деятельности по обеспечению безопасности относятся гуманизм, конкретность, эффективность, сочетание гласности и профессиональной тайны, законность и конституционность.

Принцип гуманизма заключается в обеспечении прав и свобод человека и гражданина при осуществлении противодействия угро**зам** информационной безопасности, недопущении противоправ**ных** посягательств на его личность, унижения чести и достоинства человека, произвольного вмешательства в его частную жизнь, личную и семейную тайны, ограничения свободы его информационной деятельности, а также в минимизации ущерба этим пра**вам** и свободам в случаях, когда их ограничение осуществляется **на** законных основаниях.

Принцип конкретности состоит в обеспечении безопасности применительно к конкретным жизненным обстоятельствам с учетом разнообразных форм проявления объективных законов на основе достоверной информации как о внутренних и внешних угрозах, так и о возможностях противодействия им. Достоверная информация позволяет установить конкретные формы проявления угроз, определить в соответствии с этим цели и действия по обеспечению безопасности, конкретизировать методы противо- действия угрозам, а также необходимые для их реализации силы и средства.

Принцип эффективности заключается в достижении целей про- тиводействия при наименьших затратах сил и средств. Обеспечение информационной безопасности в любой социальной общности требует

определенных материальных, финансовых и людских Ресурсов. Исходя из этого обеспечение безопасности, как и всякая. Общественно полезная деятельность людей, должна осуществляться рационально и эффективно. Обычно критерием эффективности, который применяется на практике, является отношение размера предотвращенного ущерба от реализации угроз к затратам на противодействие этим угрозам.

Принцип сочетания гласности и профессиональной тайны состоит в нахождении и поддержании необходимого баланса между открытостью деятельности по противодействию угрозам информационной безопасности, позволяющей добиться доверия и поддержки общества, и защитой определенной информации, разглашение которой может снизить эффективность противодействия угрозам безопасности.

Принцип законности и конституционности означает осуществление всех свойственных государственным организациям и должностным лицам функций в строгом соответствии с действующей конституцией, законами и подзаконными актами, согласно установленной в законодательном порядке компетенции. Строгое и неуклонное соблюдение законности и конституционности должно быть непременным требованием, принципом деятельности не только государственных, но и негосударственных органов, учреждений и организаций.

К числу особенных принципов деятельности по обеспечению информационной безопасности следует отнести, прежде всего, глобальность.

Принцип глобальности заключается в том, что указанная деятельность должна осуществляться согласованно как в конкретном обществе, так и в международном сообществе. К важным формам осуществления деятельности по обеспечению информационной безопасности относится социальное регулирование, в том числе правовые и организационные мероприятия.

Важнейшими формами осуществления деятельности по обеспечению информационной безопасности являются регулятивная и организационная формы.

Регулятивная форма деятельности по обеспечению информационной

безопасности характеризуется нормами регулирования общественных отношений по поводу противодействия угрозам и мерами по выработке и поддержанию этих норм. Выделяют два основных типа норм: технические и социальные.

Технические нормы определяют порядок взаимодействия человека с окружающей средой, осуществления деятельности по созданию материальных благ, пользования орудиями труда, в частности средствами и системами информатизации, телекоммуникации и связи. Современную систему технических норм составляют правила использования современных информационных технологий, правила защиты информации и информационных систем от несанкционированного доступа, правила пользования средствами автоматизации управления и обработки информации. Следование этим правилам способствует более производительной и эффективной работе, предупреждает нанесение ущерба таким объектам национальных интересов, как информация и информационно-телекоммуникационные системы, производственный травматизм и заболевания.

Социальные нормы регулируют поведение индивидов и подразделяются на поддерживаемые силами социальной общности без участия государства и на поддерживаемые с использованием государственного принуждения.

Первые включают, прежде всего, мораль, обычаи и традиции, корпоративные и религиозные нормы. Эти нормы играют большую роль в противодействии угрозам сохранения национальной идентичности.

Мораль, или моральные нормы — правила поведения, основанные на представлениях национальной общности о добре и зле, справедливости и несправедливости, честности и бесчестии и других подобных этических качествах. Значительная часть моральных норм вырабатывается и поддерживается нацией в целом или большей частью ее социальных групп.

Под обычаями понимаются правила поведения, сложившиеся в далеком прошлом и поддерживаемые в силу привычки в современном обществе. Норма, ставшая обычаем, оказывает свое регулирующее воздействие в силу ее

эмоционального восприятия членами общества, привыкшими к ее соблюдению настолько, что реализация данной нормы превратилась в потребность.

Традиции представляют собой правила поведения, которые определяют порядок, процедуру проведения каких-либо мероприятий, связанных с торжественными или знаменательными, значительными событиями в жизни индивида как представителя конкретной нации, а также другие элементы социального и культурного наследия, передающиеся от поколения к поколению (идеи, Взгляды, вкусы, образ действия и мысли и т.п.).

Широкое распространение в современном обществе получили нормы общественных объединений, политических партий, закрепленные их уставами,

— корпоративные нормы. Эти нормы определяют порядок участия членов в деятельности конкретных организаций, их взаимоотношения с руководством, взаимодействие с другими организациями.

Религиозные нормы представляют собой правила, установленные различными вероисповеданиями. Такие нормы содержатся в Библии**,** Коране, Талмуде и других религиозных книгах либо в сознании верующих, исповедующих языческие, различные культы. Они определяют порядок совершения религиозных обрядов**.**

Общим для всех этих норм является то, что они, как правило, составляют значительную часть национальных духовных ценно- отличающих одну нацию от другой.

Важной составляющей социального регулирования деятельности по обеспечению информационной безопасности является **праворегулирование общественных отношений.** Оно заключается в установлении определенных правовых норм осуществления наиболее важных общественных отношений и охраны этих норм от нарушения с использованием государственного принуждения. Правовое регулирование отношений в целях обеспечения информационной безопасности осуществляется в рамках правовой деятельности государства, в структуре которой выделяются законодательная (пра- вотворческая), правоприменительная и судебная деятельность.

Законодательная деятельность заключается в подготовке, принятии и издании законодательными органами нормативных правовых актов, регулирующих отношения в области удовлетворения национальных интересов в информационной сфере, а также создающих условия для предотвращения реализации угроз информационной безопасности или минимизации их воздействия на защищаемые общественные отношения. Законодательная деятельность направлена на создание правовой основы выполнения госу- дарственными органами задач по противодействию угрозам, на установление таких правил реализации общественных отношений в рассматриваемой области, при которых ни внешние, ни внутренние угрозы не оказывают на защищаемые отношения существенного негативного воздействия. Совокупность нормативных правовых актов, являющихся источниками права в данной сфере, составляют основу так называемого нормативного правового обеспечения информационной безопасности.

Правоприменительная деятельность представляет собой основанную на законодательстве оперативную, повседневную реализацию органами исполнительной власти (государственного управления) функций государства в области обеспечения информационной безопасности. Эта деятельность осуществляется в следующих формах:

- подготовка, принятие и исполнение решений органов испол- нительной власти об осуществлении конкретных мероприятий по противодействию угрозам информационной безопасности;
- координация деятельности органов исполнительной власти в процессе подготовки и реализации конкретных мероприятий;
- осуществление правоприменительной практики в рассматриваемой области;
- проведение консультативной и информационной деятельности органов исполнительной власти, направленной на создание условий для эффективного выполнения возложенных на эти органы задач;
- выполнение учетной, аналитической, прогнозной и программной работы, административных договоров;
- взаимодействие органов исполнительной власти с другими ветвями и институтами государственной власти в целях согласования усилий по противодействию угрозам;
- информационное обеспечение всех субъектов противодействия

угрозам информационной безопасности в системе исполнительной власти;

- государственный контроль за законностью деятельности субъектов правового регулирования в рассматриваемой области.

Судебная деятельность охватывает реализацию функции государства по обеспечению правосудия в процессе выполнения задач противодействия угрозам информационной безопасности. Эта деятельность является неотъемлемой составляющей обеспечения информационной безопасности, так как позволяет каждому реализовать свое конституционное право на объективное рассмотрение всех обстоятельств, связанных с применением к нему мер государственного принуждения.

Правовое обеспечение информационной безопасности характеризуется двумя основными составляющими: деятельностью государства по обеспечению информационной безопасности, осуществляемой в правовой форме; органами государственной власти, осуществляющими эту деятельность. Данное правовое обеспечение возникает в процессе взаимодействия права (как средства регулирования общественных отношений) и государства (как основного субъекта противодействия угрозам его безопасности). Правовое обеспечение проявляется в воздействии правовых механизмов на общественные отношения в целях осуществления функций государства по противодействию угрозам безопасности.

Правовое обеспечение информационной безопасности регулирует отношения в области организации противодействия угрозам информационной безопасности как отдельных организаций, так в Российской Федерации в целом, во многом определяя структуру и принципы других видов обеспечения информационной безопасности, в частности организационного обеспечения.

Правовые средства обеспечения информационной безопасности выражаются в установлениях (субъективные права, обязанности, льготы, запреты, поощрения, наказания и т.п.) и деяниях (технологии — акты реализации прав и обязанностей), противодействующих реализуемым в информационной сфере угрозам интересам субъектов права и обеспечивающих достижение

социально полезных целей. Они отражают функциональную, прикладную сторону правовой системы, выступают в качестве элементов механизма правового регулирования, во многом определяя эффективность данного механизма.

Организационное обеспечение информационной безопасности **с**остоит в осуществлении планирования и управления материальными, людскими, финансовыми и другими ресурсами государства, выделяемыми для противодействия угрозам. В рамках этой деятельности могут приниматься меры, направленные на развитие научных исследований в области повышения устойчивости информационной инфраструктуры к проявлению угроз, на содействие в установленном законодательством порядке работе общественных организаций, ставящих своей целью противодействие угрозам информационной безопасности и определение форм возможного взаимодействия с ними, на согласование деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в области противодействия угрозам, на развитие системы массовой информации, способной удовлетворять потребности граждан в актуальных, достоверных сведениях об интересующих их событиях общественной жизни, обеспечивать их своевременное поступление к гражданам и т.д.

Организационное обеспечение информационной безопасности Российской Федерации осуществляется с использованием средств технического, кадрового, материального, финансового, информационного **и** научного обеспечения.

Средства технического обеспечения информационной безопасности образуются совокупностью технических и программных средств защиты информации, предотвращения несанкционированного доступа в информационные, телекоммуникационные и вычислительные системы и сети связи, а также методического обеспечения их использования.

Средства кадрового обеспечения информационной безопасности характеризуются программами подготовки кадров по различным аспектам данной деятельности, а также используемыми учебными и методическими

материалами.

Средства материального обеспечения характеризуются совокупностью объектов, выделяемых для размещения средств технологического обеспечения, сил, участвующих в обеспечении информационной безопасности, средств организации их деятельности и т.п.

Средства финансового обеспечения представляют собой совокупность экономических инструментов получения, привлечения, перераспределения и использования денежных средств для решения задач обеспечения информационной безопасности.

Средства информационного обеспечения образуются совокупностью информационных фондов и банков данных, используемых в процессе решения задач обеспечения информационной безопасности, а также средств их актуализации.

Средства научного обеспечения информационной безопасности определяются совокупностью научных теорий, концепций, категорий, закономерностей и методов, предназначенных для изучения процессов и явлений развития информационной сферы общества, угроз национальным интересам, реализуемым в этой сфере, и для противодействия этим угрозам.

Общая структура средств обеспечения информационной безопасности представлена на рис. 7.

Основные субъекты обеспечения информационной безопасности Российской Федерации объединены в рамках государственной системы защиты информации. К их числу относятся:

- службы контроля, надзора и обеспечения информационной безопасности государственных органов;
- специализированные предприятия и организации, осуществляющие деятельность в области разработки средств и предоставления услуг по защите информации;
- сертификационно-испытательные центры;
- аттестационные центры;
- службы безопасности и защиты информации предприятий и организаций, осуществляющих обработку персональных данных, Конфиденциальной информации и информации, составляющей государственную тайну.

Таблица 6 - Средства обеспечения информационной безопасности

<table>
<tr><th colspan="4">Средства обеспечения информационной безопасности</th></tr>
<tr><td>Правовые</td><td>Политические</td><td colspan="2">Организационные</td></tr>
<tr><td rowspan="4">Совокупность правовых механизмов

противодействия проявлениям угроз национальным интересам в

информационной сфере</td><td rowspan="4">Совокупность средств борьбы за государственную власть и использования государственной власти для противодействия угрозам информационной безопасности</td><td colspan="2">Мероприятия, осуществляемые субъектами обеспечения информационной безопасности</td></tr>
<tr><td>технологические</td><td>материальные</td></tr>
<tr><td>кадрового обеспечения</td><td>финансовые</td></tr>
<tr><td>научного

обеспечения</td><td>информационного обеспечения</td></tr>
</table>

Отчетность за занятие

1 Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.
2 Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

1 *Белл Д.* Грядущее постиндустриальное общество. Опыт социального прогнозирования / пер. под ред. В. Л. Иноземцева. — М., 1999.
2 *Гейтс Б.* Дорога в будущее. — М., 1994.
3 *Зиновьев А.А.* На пути к свсрхобществу. — М.: Центрполиграф, 2000.
4 *Иноземцев В.Л.* К теории постэкономической общественной форма- ции. — М,, 1995.
5 *Иноземцев В.Л.* Современное постиндустриальное общество: приро- да, противоречия, перспективы. — М.: Логос, 2000.
6 *Тоффлер О.* Третья волна. — М., 1995.
7 *Чоговадзе Г. Г.* Информация. Общество. Человек. — М.: Дата+, 2003.

Описание экспериментальных установок (лабораторного оборудования)
Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента
Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности
Для выполнения практического занятия студент должен:

1 Ознакомиться с методикой и порядком выполнения работы.
2 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.
3 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

- работать без соответствующего освещения и вентиляции рабочего места;
- работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;
- передвигаться по аудитории без разрешения преподавателя;
- работать в специализированных аудиториях без сменной обуви;
- работать на одном рабочем месте более двух человек.

4 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.
5 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы
Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов

Не требуется

Порядок оформления отчета по практическому занятию и его защиты Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на вопросы для контроля владения
компетенциями работы.

Рекомендации для преподавателей по проведению занятия
К защите требуется отчет с подробными ответами на вопросы.

Задания для контроля владения компетенциями:

1. Раскройте содержание обеспечения информационной безопасности организации.
2. Перечислите наиболее важные объекты информационной безопасности организации и угрозы безопасности этих объектов.
3. Опишите структуру системы обеспечения информационной безопасности организации.
4. Раскройте содержание информационной безопасности Российской Федерации.
5. Перечислите наиболее важные объекты информационной безопасности Российской Федерации и основные угрозы их безопасности.
6. Перечислите принципы обеспечения информационной безопасности Российской Федерации и раскройте их содержание.
7. Перечислите основные виды обеспечения информационной безопасности и раскройте их содержание.

Содержание отчета о практическом задании
По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 20.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 20
Организационные структуры системы обеспечения безопасности информации

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 90 мин
Вступительная часть 2 мин
Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Учебная и воспитательная цели:

Изучить организационные структуры государственной системы обеспечения информационной безопасности. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

1 **Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти**
2 **Организационные структуры системы обеспечения информационной безопасности предприятия (организации)**

Краткие теоретические или справочно-информационные материалы 1 Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти

Наиболее развитой составляющей отечественного комплекса обеспечения информационной безопасности является **государственная система защиты информации,** в составе которой можно выделить такие **типовые организационные структуры,** как: служ**бы** контроля, надзора и обеспечения безопасности органов исполнительной власти; специализированные предприятия и организации — лицензиаты в различных областях компетенции уполномоченных органов исполнительной власти, которые являются разработчиками средств и поставщиками услуг по защите информации; сертификационно-испытательные центры; аттестационные центры; службы безопасности и защиты информации предприятий и организаций, независимо от их формы собственности.

Службы контроля и надзора органа исполнительной власти ***не***,сут основную нагрузку по формированию и развитию системы защиты информации в соответствующем органе власти. Такие службы входят в состав административного аппарата органов исполнительной власти и, как правило, в их функции входят:

- разработка нормативно-методических документов отраслевого (ведомственного) уровня по выполнению требований обеспечения безопасности и защиты информации;
- разработка, организация и проведение контрольных и надворных мероприятий в пределах установленной сферы компетентности органа государственной власти и оформление результатов ^проведения таких мероприятий;
- - выдача предписаний об устранении нарушений требований - Нормативных документов;
- подготовка мотивированных предложений о полном или частичном прекращении деятельности подведомственных организаций в случае, если иными мерами нарушения требований нормативных документов не могут быть устранены;
- проведение в ходе государственного контроля (надзора) разъяснительной работы по выполнению требований нормативных актов в области обеспечения безопасности и защиты информации.

Выполнение указанного перечня функций обеспечивают специалисты, соответствующие следующей **номенклатуре основных должностей:** руководитель управления, службы; руководитель отдела, сектора; специалист по направлению деятельности службы безопасности; инженер-метролог (нормоконтролер технической и организационно-распорядительной

документации).

Особое место в государственной системе защиты информации занимают **специализированные предприятия — разработчики комплексов и средств обеспечения,** а также поставщики услуг в области безопасности и защиты информации. Именно от степени их развития, уровня и качества поставляемой продукции и услуг зависит безопасность, устойчивость и надежность функционирования всей инфраструктуры информационной безопасности. Поэтому недаром одним из обязательных требований к указанным предприятиям и организациям является лицензирование их деятельности уполномоченным органом исполнительной власти в соответствии с законодательством о государственном регулировании отдельных видов деятельности.

Предлагаемые на рынке этими предприятиями **услуги организационно-технологического характера** можно классифицировать в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности:

- **обследование** — услуга, которая может включать анализ защи- щенности используемых информационных технологий, обследование системы документооборота, обследование организации в целом (т.е. анализ влияния существующего документооборота на защищенность бизнес-процессов), проверку деятельности организации в соответствии с требованиями нормативно- правовых документов и тому подобное;
- **проектирование комплексной системы обеспечения,** при котором должен быть охвачен не только технический уровень, но и все механизмы защиты, включая организационно-правовые;
- **внедрение системы защиты информации** на договорной основе с использованием специализированных подрядных организаций, имеющих соответствующую лицензию (может дать большой эффект за счет высокой квалификации привлекаемых специалистов);
- **сопровождение систем информационной безопасности и работ по защите информации третьими лицами (аутсорсинг**), т.е. оказание специализированной оперативной помощи в случае внештатных ситуаций, периодическое обновление специального и обшесистемного программного обеспечения в случае появления новых атак и уязвимостей.

Организация и технологии разработки специализированных комплексов, систем и средств зашиты информации принципиально не отличаются от используемых в других отраслях создания высокотехнологичной продукции, в частности средств вычислительной техники. Основная номенклатура

должностей традиционна для высокотехнологичных предприятий: конструктор по наладке и испытаниям; конструктор по стандартизации; программист; технолог; электроник; техник по наладке и испытаниям.

Бурный процесс информатизации и, как следствие, все возрастающая актуальность обеспечения требований информационной безопасности приводят к необходимости видоизменения и дополнения номенклатуры специалистов. Широкое распространение общепризнанной международной практики проведения такого вида услуги, как аудит информационной безопасности, привело к появлению специалистов нового профиля — аудиторов, которые осуществляют свою деятельность в соответствии с рекомендациями **отечественных и международных стандартов.** К таким стандартам относятся:

- ГОСТ Р ИСО/МЭК 17799—2005 «Информационная технология — Практические правила управления информационной безопасностью»;
- ИСО/МЭК 17799—2000 «Информационная технология. Кодекс установившейся практики для менеджмента информационной безопасностью»;
- В5 7799 «Управление информационной безопасностью. Практические правила»;
- вторая часть В5 7799-2:2002 «Системы управления информационной безопасностью — спецификация с руководством по использованию».

Сертификационно-испытательные центры и лаборатории занимают особое место среди предприятий и организаций — лицензиатов в области обеспечения безопасности и защиты информации. Эти организационные структуры обеспечивают необходимую поддержку такой функции государственно-общественного регулирования в области информационной безопасности, как сертификацию средств и оценки качества оказания услуг по защите /информации.

Наряду с лицензированием своей деятельности в области защиты информации указанные центры и лаборатории должны пройди дополнительно обязательную организационно-правовую процедуру — аккредитацию в качестве сертификационно-испытательных структур, которая в настоящее время осуществляется исключительно уполномоченными органами исполнительной власти. Реформа законодательства о техническом регулировании пока не дает четкой правовой основы использования обязательной сертификации как

механизма независимого подтверждения качества продукции и услуг в области информационной безопасности, но и не отменяет возможность применения такого механизма, по крайней мере в системе сертификации продукции, работ и услуг, средств и комплексов защиты сведений, составляющих государственную тайну. Наработанные практикой за более чем десятилетний период организационно-технологические процедуры в целом могут также с успехом применяться в системах добровольной сертификации. Поэтому существующие сертификационно-испытательные центры (лаборатории) по-прежнему будут играть ключевую роль в процессах подтверждения соответствия средств, комплексов и систем защиты установленным требованиям по безопасности информации. Номенклатура указанных должностей подобных структур также может быть дополнена новой категорией специалистов, например, «оценщик», или специалист по оценке защищенности информационных технологий, предусмотренной стандартом ГОСТ Р ИСО/МЭК 15408-2002 «Общие критерии оценки безопасности информационных технологий».

Аттестационные центры наряду с сертификацией средств, работ и услуг в области обеспечения информационной безопасности осуществляют относительно похожие процедуры подтверждения соответствия, называемые аттестацией объектов информатизации.

Как правило, по объему и характеру работ традиционные аттестационные центры (лаборатории) не имеют существенных отличительных особенностей по сравнению с сертификационно-испытательными центрами, а наиболее известные отечественные компании — поставщики услуг в области защиты информации — имеют аккредитацию по обоим видам деятельности и, соответ- ственно, примерно одинаковую номенклатуру основных должностей.

Активно развивается также рынок образовательных услуг в области информационной безопасности по повышению квалификации специалистов, руководителей служб безопасности, руководителей 1Т-подразделений, пользователей средств защиты, так как необходимым условием для получения лицензии на деятельность в области защиты информации является наличие

персонала необходимого уровня квалификации и подготовки. Однако система дополнительного образования в области информационной безопасности пока находится в стадии формирования, что затрудняет выделение ее типовых элементов.

Службы безопасности и защиты информации предприятий и организаций независимо от вида деятельности и форм собственности являются самой распространенной организационной структурой в рассматриваемой области общественной деятельности и по существу составляют основу всей системы обеспечения информационной безопасности предприятий, организаций и страны в целом. Поэтому целесообразно рассмотреть вопросы их функциони- рования более подробно.

Непосредственная деятельность по организации функционирования и эксплуатации комплексов обеспечения информационной безопасности осуществляется штатными специалистами соответствующих структурных подразделений. Они должны иметь определенную квалификацию в соответствии с требованиями, установленными номенклатурой должностей и служащих. Типовые требования можно найти в квалификационном справочнике должностей руководителей, специалистов и других служащих, утвержденном Министерством труда и социального развития Российской Федерации в 2003 г.

2 Организационные структуры системы обеспечения информационной безопасности предприятия (организации)

Задачи и функции организационных структур, осуществляющих реализацию специальных защитных мероприятий (служб безопасности) на уровне предприятия (организации), определяются потребностями реальных бизнес-процессов, их спецификой и масштабами.

Традиционной задачей служб безопасности хозяйствующих субъектов является обеспечение так называемой физической защиты, под которой подразумевается охрана имущества, материальных и финансовых ценностей, а также в отдельных случаях защита персонала, прежде всего руководства, от

преступных посягательств. Для решения этой задачи **служба безопасности** должна обеспечить .выполнение следующих **функций:**

- организацию пропускного режима, разграничение физического доступа на защищаемые объекты;
- организацию инженерно-технической защиты охраняемых зданий и помещений объекта;
- обнаружение проникновения внешнего нарушителя на охраняемую территорию и принятие соответствующих мер противодействия;
- противодействие противоправным действиям внутренних нарушителей по отношению к имуществу и активам предприятия;
- организацию личной охраны персонала.

Менее традиционной является **задача обеспечения безопасности управления бизнес-процессами**, включающая защиту нематериальных активов и информационных ресурсов предприятия (информационная безопасность) и участие в управлении персоналом в части обеспечения лояльности и благонадежности. Реализация талой задачи **подразумевает выполнение следующих функций:**

- разведка и контрразведка, в том числе изучение криминальных аспектов рынка, организация противодействия экономическому шпионажу, сбор на законных основаниях информации о деловых партнерах и других лицах, имеющих контакты с предприятием;
- организация противодействия недобросовестной конкуренции, выявление фактов противоправного использования нематериальных активов и интеллектуальной собственности;
- организация секретного и конфиденциального делопроизводства и ведения конфиденциальных переговоров;
- обеспечение безопасности автоматизированных информационных технологий, а также информации, циркулирующей в компьютерных сетях;
- противодействие технической разведке, т.е. способам несан- кционированного съема информации с помощью технических средств;
- проведение служебных расследований обстоятельств разглашения сведений, составляющих коммерческую тайну и т.д.;
- оценка лояльности и благонадежности персонала путем проведения в рамках, установленных законом, оперативно-розыскных мероприятий и выявление неблагонадежных сотрудников (группы риска) с помощью различных методов тестирования;
- подготовка персонала, в том числе нештатных сотрудников, формирование правосознания и культуры поведения всех сотрудников предприятия по вопросам обеспечения его безопасности;
- оценка эффективности работы структурных подразделений,

входящих в состав службы безопасности и защиты информации.

В случае **создания полномасштабной собственной системы без- опасности и защиты информации** наиболее эффективной является трехуровневая структура стратегического, тактического и оперативного управления.

На уровне стратегического управления осуществляется формулирование конкретных интересов предприятия, его бизнес-процессов и критериев обеспечения их защищенности, выделение необходимого ресурсного обеспечения. Очевидно, что решение этих задач должно быть сосредоточено на уровне высшего руководства, в структуре топ-менеджмента предприятия, где происходит утверждение соответствующей концепции развития предприятия. Тактическое управление осуществляет руководитель службы безопасности или должностное лицо, на которое возложены соответствующие обязанности, его заместители и руководители структурных подразделений. Основная задача тактического управления — формирование корпоративной нормативно- методической базы требований по обеспечению безопасности, их реализация и контроль за их выполнением. Оперативное управление включает практическую реализацию защитных функций, в том числе эксплуатацию специализированных технических средств и проведение организационных процедур, и осуществляется как штатными, так и нештатными сотрудниками службы безопасности, выполняющими соответствующие функции наряду с основной деятельностью.

Полномасштабный комплекс обеспечения безопасности предприятия включает следующие штатные и нештатные структуры:

- совет или комиссии по различным вопросам обеспечения безопасности, возглавляемые топ-менеджментом предприятия;
- руководство службой безопасности и руководимые им консультативно-экспертные группы;
- охранное подразделение;
- инженерно-техническое подразделение;
- аналитическую группу;
- подразделение секретного делопроизводства и ведения конфиденциальных переговоров;

- подразделение противодействия технической разведке и т е х - нической защиты информации;
- подразделение администрирования информационно-управляющих систем по требованиям безопасности информации;
- подразделение оценки лояльности и благонадежности персонала, его подготовки в области обеспечения безопасности;
- подразделение аудита систем обеспечения безопасности и оценки их эффективности.

Конкретная реализация структуры службы безопасности находится в компетенции первого руководителя предприятия. Номенклатура штатных и нештатных должностей службы безопасности на уровне предприятия может включать все перечисленные должности специализированных организационных структур. Кроме этого, в подразделениях системы управления предприятием, не связанных напрямую с обеспечением безопасности, на практике часто вводится штатная либо нештатная должность администратора информационной безопасности. Основной обязанностью такого специалиста является обеспечение защиты информационных ресурсов и администрирование соответствующих средств защиты Информации на уровне конкретного подразделения.

Для **малых предприятий с небольшими объемами бизнеса и чис- ленностью работников** обязанности по выполнению ряда вышеперечисленных функций возлагаются на отдельных ответственных сотрудников. На предприятиях среднего масштаба создается отдельное относительно небольшое подразделение, координирующее и контролирующее выполнение функций по обеспечению безопасности другими подразделениями предприятия. Крупные фирмы и корпорации развивают службу безопасности до полномасштабной структуры, имеющей все необходимые полномочия Р ресурсы для решения поставленных задач. При этом следует иметь в виду, что выполнение охранных функций, в том числе защиту личного состава, в соответствии с действующим законодательством могут осуществлять либо вневедомственная охрана МВД России, либо частные охранные предприятия, действующие на основе законодательства о частной детективной и охранной деятельности. Частным охранным предприятиям разрешается оказывать различные услуги, в том числе

по вооруженной охране имущественных ценностей при транспортировке и по защите жизни и здоровья персонала. Кроме этого, охранные предприятия обеспечивают проектирование, монтаж и обслуживание средств охранно- пожарной сигнализации, консалтинговые услуги по вопросам правомерной защиты от противоправных посягательств.

Другой пример использования услуг третьих лиц по обеспечению требований информационной безопасности характерен для предприятий и организаций негосударственных форм собственности, не имеющих собственных подразделений по защите государственной тайны. По действующему законодательству они в случае необходимости могут заключать с государственными организациями договоры об использовании их режимно- секретных органов (РСО), обеспечивающих секретное делопроизводство и режимные мероприятия в соответствии с лицензией на проведение работ с ис- пользованием сведений, составляющих государственную тайну, и на оказание услуг по защите указанных сведений.

В ходе информатизации малые и средние предприятия все чаще используют такую форму договорных услуг, как аутсорсинг информационных технологий, включая вопросы обеспечения информационной безопасности.

Одной из распространенных форм организационного обеспечения безопасности предприятия, отражающей комплексный характер рассматриваемой проблемы и один из методов ее решения, является создание отдельных комиссий. Такие нештатные структуры выполняют на временной или постоянной основе отдельные экспертные или контрольно-ревизионные функции по обеспечению безопасности, в частности инвентаризацию имущественных ценностей, нематериальных активов и информационных ресурсов, экспертизу материалов, подготовленных к публикации в средствах массовой информации, аттестацию персонала. Включение в комиссии сотрудников различных подразделений структуры управления предприятием позволяет скоординировать их взаимодействие и в целом повысить эффективность совместной деятельности.

Решение задачи физической защиты предполагает проведение следующих специальных мероприятий и действий сотрудников службы по организации режимов обеспечения безопасности объекта:

- определение и категорирование охраняемых зон по уровню доступа;
- разработка заданий на укрепление периметров охраняемых зон (ограждение, решетки, замки и т.д.), контроль проектирования системы укрепленности периметра, прием и контроль хода эксплуатации системы;
- определение точек доступа в охраняемые зоны, разработка заданий по их оборудованию необходимыми техническими средствами, контроль проектирования и эксплуатации технических средств, разработка инструкций о порядке пропускного и внутриобъектового режимов;
- разработка заданий по применению средств охранно-пожарной сигнализации, систем видеонаблюдения, автоматизированных систем ограничения и контроля доступа в охраняемые зоны, прием и контроль эксплуатации;
- согласование порядка выноса (вноса) из охраняемых зон ма- териальных ценностей и других видов ресурсов;
- разработка заданий, контроль проектирования, прием и контроль эксплуатации систем специальной связи, оборудования комнат и порядка приема посетителей;
- категорирование информационных ресурсов по степени секретности и конфиденциальности как нормативной основы ограничения их обращения;
- определение возможных физических каналов утечки информации с ограниченным доступом, разработка заданий на проектирование систем противодействия технической разведке, прием и контроль их эксплуатации;
- разработка порядка проведения служебных расследований по фактам нарушения пропускного и внутриобъектового режимов, а также взаимодействия с правоохранительными органами.

Указанные мероприятия позволяют обеспечить реализацию такой важной характеристики защищенности, как **конфиденциальность информации,** путем использования тех или иных технологий ограничения доступа. Однако, как правило, решение проблемы повышения эффективности бизнес-процессов требует увеличения их открытости, непрозрачности как для внешней среды, так и для собственного управленческого персонала. Это позволяет в максимальной степени обеспечить масштабность производственной деятельности, ее настройку на быстро изменяющиеся условия рыночной и политической конъюнктуры. Поэтому не менее важными, а подчас и более актуальными задачами обеспечения информационной безопасности являются повышение доступности

и целостности информационных активов корпорации в условиях бурного внедрения компьютерных технологий. Реализация всех характеристик защищенности является также необходимым условием обеспечения качества бизнес-процессов за счет поддержания их непрерывности, под которой понимается и своевременное принятие управленческих решений.

Отчетность за занятие

1 Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.
2 Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

1 *Возженников А. В.* Национальная безопасность: теория, политика, стратегия. — М.: РАГС, 1998.
2 Основы национальной безопасности России / под ред. В. Л. Манилова. — М.: Друза. 1998.
3 *Прохожее А.А.* Национальная безопасность: основы теории, сущность, проблемы. — М.: РАГС, 1997.
4 *Прохожее А.А.* Человек и общество: законы социального развития и безопасности. — М.: РАГС, 2002.
5 *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методологические основы. — М.: МЦНМО, 2002.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности

1 Для выполнения практического занятия студент должен:
2 Ознакомиться с методикой и порядком выполнения работы.

3 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.

4 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

- работать без соответствующего освещения и вентиляции рабочего места;
- работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;
- передвигаться по аудитории без разрешения преподавателя;
- работать в специализированных аудиториях без сменной обуви;
- работать на одном рабочем месте более двух человек.

5 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.

6 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы
Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов
Не требуется

Порядок оформления отчета по практическому занятию и его защиты Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на вопросы для контроля владения
компетенциями работы.

Рекомендации для преподавателей по проведению занятия
К защите требуется отчет с подробными ответами на вопросы.

Задания для контроля владения компетенциями:

1 Какие типовые организационные структуры входят в государствен- ную систему защиты информации?

2 Какие функции в области обеспечения безопасности и защиты ин- формации выполняют службы контроля и надзора органа государственной власти?

3 В чем состоит специфика государственного регулирования деятель- ности специализированных предприятий — разработчиков комплексов и средств обеспечения безопасности?

4 Как классифицируются услуги организационно-технологического характера в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности?

5 В чем состоит специфика деятельности сертификационно-испыта тельных центров (лабораторий) и механизмов ее государственного ре- гулирования?

6 Какие функции выполняет служба безопасности предприятия для решения задачи физической защиты?

7 Какие функции выполняет служба безопасности предприятия для решения задачи обеспечения информационной безопасности?

8 Как строится структура полномасштабной системы обеспечения безопасности и защиты информации?

9 Какова специфика организации и выполнения охранных функций'

10 Какие специальные мероприятия и действия должны предприни- мать сотрудники службы безопасности по организации объектовых режимов

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 21.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 21

Разработка модели информационных потоков предприятия (организации) с использованием программного комплекса гриф-2006

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 90 мин
Вступительная часть 2 мин
Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Цель и содержание

Целью данного раздела практического занятия является анализ уровня защищенности всех ценных ресурсов компании, оценка возможного ущерба, который понесет компания в результате реализации угроз информационной безопасности, позволить эффективно управлять рисками при помощи выбора контрмер, наиболее оптимальных по отношению цена - качество.

Краткие теоретические или справочно-информационные материалы

При проектировании системы информационной безопасности целесообразно руководствоваться следующими положениями:
Необходимо предварительно проанализировать информацию, которая циркулирует в учреждении, выделить информацию ограниченного доступа определить круг информации, составляющей государственную тайну, оценить коммерческую важность информации. Все это, в итоге, позволит диф- ференцировать круг мероприятий по обеспечению безопасности информации и, тем самым, сократить расходы. Необходимо разработать и утвердить перечень сведений, составляющих коммерческую тайну, и ознакомить с ним исполнителей.
До начала построения системы безопасности учреждения в целом и

безопасности информации, в частности, следует убедиться в лояльности сотрудников и, особенно, сотрудников службы безопасности. При этом необходимо руководствоваться принципом «доверяй, но проверяй». Следует принять необходимые меры морального и материального плана для поощрения лояльности сотрудников - это укрепит уверенность в том, что в критический момент система безопасности не подведет. Принимая сотрудника на работу, желательно всеми доступными средствами навести о нем справки. Можно применить специальные психологические тесты, которые помогут оценить его личностные качества. В контракте с сотрудником следует обязательно оговорить условия конфиденциальности не только на период совместной работы, но и на определенный срок после завершения взаимоотношений с ним.

Первым шагом к решению проблемы защиты информации должно стать создание концепции информационной безопасности и ее увязывание с общей концепцией безопасности учреждения. Концепция представляет собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности. Следует помнить, что основным принципом создания системы безопасности должно стать обеспечение заданного уровня защищенности от возможных угроз при минимальной стоимости средств и систем защиты.

Работы в области защиты информации следует поручать только пред- приятиям и организациям, имеющим лицензию ФСТЭК Российской Федерации - это дает надежную гарантию высокого качества работ и позволит, в случае необходимости, применить юридические санкции. Для обработки информации ограниченного доступа необходимо применять такие аппаратные средства и программные продукты, не использующие методы криптографии, которые имеют сертификат, выданный ФСТЭК. Для средств защиты с применением криптографии необходим сертификат ФАПСИ. Перечни средств защиты, прошедших сертификацию, постоянно обновляются и рассылаются ФСТЭК во все администрации регионов России и заинтересованные ведомства. Подобная информация есть и в Госстандарте России, который ведет сводный перечень средств, имеющих различные сертификаты.

Необходимо убедиться в достаточности принятых мер, проведя про- верку эффективности средств защиты. Следует помнить, что информационная безопасность любой организации зависит не только, а подчас — не столько от технических средств, но и от людей, их использующих. При этом необходимо, во-первых, научить сотрудников пользоваться защитными средствами. На каждом рабочем месте должны быть инструкции и памятки, в доступной форме информирующие персонал об обязательных мерах по поддержанию информационной безопасности. Во-вторых, необходимо тщательно подобрать и подготовить специалистов, способных грамотно обслуживать систему защиты.

Необходимо организовать подготовку персонала по вопросам защиты информации, разработать и довести до каждого правила информационной безопасности.

В результате выполнения предложенных организационных мероприятий следует ожидать качественно более высокого уровня безопасности, снижения страховых платежей за счет повышения защищенности повседневной профессиональной деятельности от различных видов угроз, предотвращения ущерба от противоправных действий злоумышленников.

В руководящем документе Госехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», указывается, что организационные мероприятия в рамках системы защиты информации от несанкционированного доступа в автоматизированных системах, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

Методика построения корпоративной системы защиты информации

Большинство директоров служб автоматизации (CIO) и информационной безопасности (CISO) российских компаний наверняка задавалось вопросом: “Как оценить уровень защищенности информационных активов компании и определить перспективы развития корпоративной системы защиты информации?” Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому решение вопроса об оценке уровня защищенности информационных активов компании обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, Конституции и федеральным законам, руководящим документам Гостехкомиссии России и ФАПСИ, приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, таких, как ISO 17799, 9001, 15408, BSI и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации компании.

Использование аналитических методов при определении объектов и субъектов защиты, их взаимоотношений

Современные методики управления рисками, проектирования и сопровождения корпоративных систем защиты информации должны позволять решить ряд задач перспективного стратегического развития компании.

Во-первых, количественно оценить текущий уровень информационной безопасности компании, что потребует выявления рисков на правовом, организационно-управленческом, технологическом, а также техническом

уровнях обеспечения защиты информации.

Во-вторых, разработать и реализовать комплексный план совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании. Для этого необходимо:

- обосновать и произвести расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности компании, создать необходимый пакет организационно-распорядительной документации;
- разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;
- обеспечить поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительнойдокументации, модификацией технологических процессов и модернизацией технических средств защиты.

Решение названных задач открывает новые широкие возможности перед должностными лицами разного уровня.

Руководителям верхнего звена это поможет объективно и независимо оценить текущей уровень информационной безопасности компании, обеспечить формирование единой концепции безопасности, рассчитать, согласовать и обосновать необходимые затраты на защиту компании. На основе полученной оценки начальники отделов и служб смогут выработать и обосновать необходимые организационные меры (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действия в нештатных ситуациях). Менеджеры среднего звена смогут обоснованно выбрать средства защиты информации, а также адаптировать и использовать в своей работе количественные показатели оценки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической эффективности компании.

Практические рекомендации по нейтрализации и локализации выявленных уязвимостей системы, полученные в результате аналитических исследований, помогут в работе над проблемами информационной безопасности на разных уровнях и, что особенно важно, определить основные зоны ответственности, в том числе материальной, за ненадлежащее использование информационных активов компании. При определении

масштабов материальной ответственности за ущерб, причиненный работодателю, в том числе разглашением коммерческой тайны, следует руководствоваться положениями гл. 39 Трудового кодекса РФ.

Субъекты безопасности предприятия

Обеспечением безопасности предприятия занимаются две группы субъектов. Первая группа занимается этой деятельностью непосредственно на предприятии и подчинены его руководству. Среди этой группы можно выделить специализированные субъекты (совет или комитет безопасности предприятия, служба безопасности, пожарная часть, спасательная служба и т.д.), основным предназначением которых является постоянная профессиональная деятельность по обеспечению безопасности предприятия (в рамках своей компетенции). Другую часть субъектов этой группы условно можно назвать полуспециализированной, т.к. часть функций этих субъектов предназначена для обеспечения безопасности предприятия (медицинская часть, юридический отдел и т.д.). Наконец, к третьей части этой группы субъектов относится весь остальной персонал и подразделения предприятия, которые в рамках своих должностных инструкций и положений о подразделениях обязаны принимать меры к обеспечению безопасности. Следует иметь в виду, что эффективно обеспечивать безопасность предприятия эти субъекты могут только в том случае, если цели, задачи, функции, права и обязанности будут распределены между ними таким образом, чтобы они не пересекались друг с другом.

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

- законодательные органы. Принятые на уровне Российской Федерации и субъектов Федерации законы составляют правовую основу деятельности по обеспечению безопасности предприятия;
- органы исполнительной власти. Принятые на уровне этих органов подзаконные акты во многом дополняют, уточняют, детализируют требования законов;
- суды. Судебные органы обеспечивают соблюдение законных прав и интересов предприятия, в т.ч. в сфере безопасности;
- правоохранительные органы. Такие органы осуществляют борьбу с правонарушениями, которые отрицательным образом влияют на состояние безопасности предприятия;
- научно-образовательные учреждения. Последние (особенно негосударственные образовательные учреждения для подготовки частных охранников и детективов) призваны обеспечить научно-методическую проработку проблем безопасности предприятия и подготовку соответствующих специалистов в сфере безопасности предприятий.

Совершенно очевидно, что субъекты второй группы по своей

инициативе подключаются эпизодически (или никогда) к деятельности предприятия по обеспечению своей безопасности. Организационной формой такого подключения может стать комплексная программа безопасности предприятия, в которой необходимо предусмотреть формы и методы этой работы. Кроме того, можно рекомендовать разработку планов структурных подразделений и всего предприятия в целом по организации взаимодействия с вышеуказанными органами и организациями.

Разновидности аналитических работ по оценке защищенности

Аналитические работы в области информационной безопасности могут проводиться по следующим направлениям:

- комплексный анализ информационных систем (ИС) компании и подсистемы информационной безопасности на правовом, методологическом, организационно-управленческом, технологическом и техническом уровнях. Анализ рисков;
- разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-аппаратному обеспечению режима ИС компании;
- организационно-технологический анализ ИС компании;
- экспертиза решений и проектов;
- работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации;
- работы, поддерживающие практическую реализацию плана защиты;
- повышение квалификации и переподготовка специалистов. Кратко рассмотрим каждое из них.

Исследование и оценка состояния информационной безопасности ИС и подсистемы информационной безопасности компании предполагают проведение их оценки на соответствие типовым требованиям руководящих документов Гостехкомиссии при Президенте РФ, типовым требованиям международных стандартов ISO и соответствующим требованиям компании- заказчика. К первой области также относятся работы, проводимые на основе анализа рисков, инструментальные исследования (исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы на наличие уязвимостей, исследование защищенности точек доступа в Internet). Данный комплекс работ также включает в себя и анализ документооборота, который, в свою очередь, можно выделить и как самостоятельное направление.

Рекомендации могут касаться общих основополагающих вопросов обеспечения безопасности информации (разработка концепции информационной безопасности, разработка корпоративной политики охраны информации на организационно-управленческом, правовом, технологическом и техническом уровнях), применимых на многих компаниях. Также рекомендации могут быть вполне конкретными и относится к деятельности одной единственной компании (план защиты информации, дополнительные

работы по анализу и созданию методологического, организационно-управленческого, технологического, инфраструктурного и технического обеспечения режима информационной безопасности компании).

Организационно-технологический анализ ИС компании в основном предполагает проведение оценки соответствия типовым требованиям руководящих документов РФ к системе информационной безопасности компании в области организационно-технологических норм и анализ документооборота компании категории “конфиденциально” на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям компании по обеспечению конфиденциальности информации. При этом собственно внутрифирменная концепция информационной безопасности (ИБ) и положение о коммерческой тайне должны соответствовать действующему законодательству, а именно требованиям Конституции РФ, ст.ст. 128 и 139 Гражданского кодекса РФ, Федерального закона “Об информации, информатизации и защите информации”, Федерального закона “Об участии в международном информационном обмене”, других нормативных актов.

Правильная экспертиза решений и проектов играет важную роль в обеспечении функционирования всей системы информационной безопасности и должна соответствовать требованиям по обеспечению информационной безопасности экспертно-документальным методом. Экспертиза проектов подсистем – требованиям по безопасности экспертно-документальным методом.

Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации, как правило, включают два направления:

- анализ документооборота компании категории “конфиденциально” на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям компании по обеспечению конфиденциальности информации;
- поставку комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ компании на организационно-управленческом и правовом уровне.

Работы, поддерживающие практическую реализацию плана информационной безопасности, в частности, заключаются в следующем:

- разработка технического проекта модернизации средств защиты ИС, установленных на фирме по результатам проведенного комплексного аналитического исследования корпоративной сети;
- подготовка компании к аттестации (к аттестации объектов информатизации заказчика на соответствие требованиям руководящих документов Гостехкомиссии при Президенте РФ, а также на соответствие требованиям безопасности международных стандартов ISO 15408, ISO 17799, стандарта ISO 9001 при обеспечении требований информационной безопасности компании);

- разработка расширенного перечня сведений ограниченного распространения как части политики безопасности;
- разработка пакета организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ компании на организационно-управленческом и правовом уровне;
- поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ компании на организационно-управленческом и правовом уровнях.

Уровень информационной безопасности компании во многом зависит от квалификации специалистов. В целях повышения квалификации и переподготовки кадров рекомендуется проводить тренинги по применению средств защиты информации, технологии защиты информации, обучать сотрудников основам экономической безопасности.

Немаловажную роль играет и ежегодная переоценка состояния информационной безопасности компании.

Методика построения корпоративной системы защиты информации

Федеральный Закон «Об информации, информационных технологиях и о защите информации» гласит, что целями защиты информации являются: предотвращение утечки, хищения, утраты, искажения, подделки информации, несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, а также других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Основная задача любой системы информационной безопасности заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом РФ, обеспечении нормальной производственной деятельности всех подразделений объекта.

Другая задача сводится к повышению качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов**.**

Для этого необходимо:

- отнести информацию к категории ограниченного доступа (служебной тайне);
- прогнозировать и своевременно выявлять угрозы безопасности информационным ресурсам, причины и условия, способствующие нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создать условия функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
- создать механизм и условия оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в

функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

создать условия для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, и тем самым ослабить возможное негативное влияние последствий нарушения информационной безопасности.

При выполнении работ можно использовать следующую модель построения корпоративной системы защиты информации (рисунок 1), основанную на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799). Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 “Информационная технология – методы защиты – критерии оценки информационной безопасности”, стандарту ISO/IEC 17799 “Управление информационной безопасностью” и учитывает тенденции развития отечественной нормативной базы (в частности, Гостехкомиссии РФ) по вопросам защиты информации.

Рисунок 1 - Модель построения корпоративной системы защиты информации

Представленная модель защиты информации – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

- угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
- уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
- риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается первоначально:

- провести анализ рисков в области информационной безопасности;
- определить оптимальный уровень риска для организации на основе заданного критерия;
- систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемая методика проведения аналитических работ позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также в соответствии со ст. 2 Федерального закона “Об информации, информационных технологиях и о защите информации” – информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов являются сети связи, внешние сервисы и т.п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель (модель угроз и уязвимостей), в соответствии с предлагаемой методикой, строится следующим образом:

- для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д.;
- описываются взаимосвязи ресурсов;
- определяются угрозы безопасности;
- оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки безопасности основана на:

- вовлечении в процесс оценки большего числа элементов информационной среды объекта;
- глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения,
- строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Формирование организационной политики безопасности

Прежде чем предлагать какие-либо решения по системе информационной безопасности, предстоит разработать политику безопасности. Организационная политика безопасности описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения организационной

политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Организационная политика безопасности оформляется в виде отдельного документа, который согласовывается и утверждается Заказчиком.

Прежде всего, необходимо составить детализированное описание общей цели построения системы безопасности объекта, выражаемое через совокупность факторов или критериев, уточняющих цель. Совокупность факторов служит базисом для определения требований к системе (выбор альтернатив). Факторы безопасности, в свою очередь, могут распределяться на правовые, технологические, технические и организационные.

Требования гарантии достигаемой защиты выражаются через оценки функций безопасности СИБ объекта. Оценка силы функции безопасности выполняется на уровне отдельного механизма защиты, а ее результаты позволяют определить относительную способность соответствующей функции безопасности противостоять идентифицированным угрозам. Исходя из известного потенциала нападения, сила функции защиты определяется, например, категориями “базовая”, “средняя”, “высокая”. Потенциал нападения определяется путем экспертизы возможностей, ресурсов и мотивов побуждения нападающего.

Перечень требований к системе информационной безопасности, эскизный проект, план защиты (далее – техническая документация, ТД) содержит набор требований безопасности информационной среды объекта, которые могут ссылаться на соответствующий профиль защиты, а также содержать требования, сформулированные в явном виде.

В общем виде разработка технической документации (ТД) включает:

- уточнение функций защиты;
- выбор архитектурных принципов построения СИБ;
- разработку логической структуры СИБ (четкое описание интерфейсов);
- уточнение требований функций обеспечения гарантоспособности СИБ;
- разработку методики и программы испытаний на соответствие сформулированным требованиям.

На этапе оценки достигаемой защищенности производится оценка меры гарантии безопасности информационной среды. Мера гарантии основывается на оценке, с которой после выполнения рекомендованных мероприятий можно доверять информационной среде объекта. Базовые положения данной методики предполагают, что степень гарантии следует из эффективности усилий при проведении оценки безопасности. Увеличение усилий оценки предполагает:

- значительное число элементов информационной среды объекта, участвующих в процессе оценивания;

- расширение типов проектов и описаний деталей выполнения при проектировании системы обеспечения безопасности;
- строгость, заключающуюся в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

В целом рассмотренная выше методика позволяет оценить или переоценить уровень текущего состояния защищенности информационных активов компании, а также выработать рекомендации по обеспечению (повышению) информационной безопасности компании. В том числе снизить потенциальные потери компании путем повышения устойчивости функционирования корпоративной сети, разработать концепцию и политику безопасности компании. Также рассмотренная методика позволяет предложить планы защиты конфиденциальной информации компании, передаваемой по открытым каналам связи, защиты информации компании от умышленного искажения (разрушения), несанкционированного доступа к ней, ее копирования или использования.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

1 *Возженников А. В.* Национальная безопасность: теория, политика, стратегия. — М.: РАГС, 1998.
2 Основы национальной безопасности России / под ред. В. Л. Манилова. — М.: Друза. 1998.
3 *Прохожее А.А.* Национальная безопасность: основы теории, сущность, проблемы. — М.: РАГС, 1997.
4 *Прохожее А.А.* Человек и общество: законы социального развития и безопасности. — М.: РАГС, 2002.
5 *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методологические основы. — М.: МЦНМО, 2002.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ с использованием программных комплексов «ГРИФ», «КОНДОР».

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на Задания для контроля владения компетенциями данной

Практического занятия.

Техника безопасности

Для выполнения Практического занятия студент должен: Ознакомиться с методикой и порядком выполнения работы.

Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.

После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

- работать без соответствующего освещения и вентиляции рабочего места;
- работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;
- передвигаться по аудитории без разрешения преподавателя;
- работать в специализированных аудиториях без сменной обуви;
- работать на одном рабочем месте более двух человек.

После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.

Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы

Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов

Представление отчетов.

Порядок оформления отчета по практическому занятию и его защиты

Отчет по результатам выполнения Практического занятия оформляется в тетради и должен содержать ответы на Задания для контроля владения компетенциями работы.

Рекомендации для преподавателей по проведению занятия

К защите требуется отчет с подробными ответами на вопросы к ПЗ.

Методика и порядок выполнения работы

Задание № 1. Построить полную модель информационной системы

компании, создав:

- отделы (структурное подразделение организации, например, отдел кадров, бухгалтерия и т.д.);
- сетевые группы (например, сервер и 1 рабочая станция);
- ресурсы (объект хранения ценной информации, например, твердая копия, рабочая станция, сервер);
- сетевые устройства (устройства, с помощью которых осуществляются связи между ресурсами сети, например, точка доступа, маршрутизатор и т.д.);
- виды информации (вид ценной информации, хранимой и обрабатываемой на ресурсе, например, бухгалтерская информация, информация о ценовых предложениях и т.д.);
- группы пользователей (группы пользователей, имеющих одинаковый класс и средства защиты, обладающих одинаковыми правами доступа к ценной информации, например, офицеры безопасности, топ - менеджеры и т.д.);
- бизнес – процесс (производственные процессы, в которых обрабатывается данная информация, например, внесение изменений, охрана предприятия и т.д.).

Для того чтобы наиболее полно охватить все угрозы, действующие на информационные ресурсы организации, вводится раздел «Политика безопасности», который содержит вопросы, ответы на которые влияют на эффективность средств защиты и изменяют риск реализации угроз информационной безопасности. Разделы, по которым проектируется политика безопасности:

- организационные меры;
- безопасность персонала;
- физическая безопасность;
- управление коммуникациями и процессами;
- контроль доступа;
- разработка и сопровождение систем;
- непрерывность ведения бизнеса;
- соответствие системы требованиям.

Ответ на каждый вопрос необходимо утвердить нажатием клавиши «Принять».

Далее производится работа с разделом «Связи», в котором определяются связи между объектами, занесенными в разделе «Моделирование системы». При выборе отдела рабочее поле отображает все ресурсы, принадлежащие данному отделу. Пользователь может просмотреть свойства ресурсов и при необходимости отредактировать их. При выборе ресурса рабочее поле отображает закладки для определения связей между данным ресурсом и остальными элементами информационной системы. Количество закладок зависит от типа ресурса. В этом разделе рассматриваются следующие закладки:

- виды информации (определяется ценная информация, используемая на ресурсах);
- группы пользователей (определяются пользователи, имеющие доступ к ценной информации на ресурсах);
- каналы связей (определяется, с помощью каких сетевых устройств осуществляется доступ к ресурсу «сервер» группами пользователей);
- бизнес-процессы (определяется, в каких бизнес-процессах используется ценная информация);
- средства защиты (определяется, какие средства защиты применяются для ресурсов);
- средства защиты информации (определяется, какие средства защиты применяются для ценной информации на ресурсах).

Окно «Отчет» позволяет просмотреть созданные отчеты. Каждый отчет располагается на отдельной закладке. При нажатии на «Создать отчет» появляется окно «Конфигурация отчета», которая может быть практически любой, позволяя создавать как краткие отчеты для руководства, так и детальные отчеты для дальнейшей работы с результатами. Нажать «Открыть отчет». После просмотра отчета перенести проект с сетевого сервера на локальный, для чего необходимо войти в систему как пользователю, обладающему правом на чтение данного проекта. Здесь свой проект следует
«сохранить как…», приложить к отчету о практическому занятию.

Варианты заданий для самостоятельного выполнения

Создать проект модели информационных потоков на конкретном предприятии, выпускающем конкретную продукцию.

До начала построения системы безопасности учреждения в целом и безопасности информации, в частности, следует убедиться в лояльности со- трудников и, особенно, сотрудников службы безопасности. При этом необ- ходимо руководствоваться принципом «доверяй, но проверяй». Следует принять необходимые меры морального и материального плана для поощ- рения лояльности сотрудников - это укрепит уверенность в том, что в кри- тический момент система безопасности не подведет. Принимая сотрудника на работу, желательно всеми доступными средствами навести о нем справки. Можно применить специальные психологические тесты, которые помогут оценить его личностные качества. В контракте с сотрудником следует обязательно оговорить условия конфиденциальности не только на период совместной работы, но и на определенный срок после завершения взаимоотношений с ним.

Первым шагом к решению проблемы защиты информации должно стать создание концепции информационной безопасности и ее увязывание с общей концепцией безопасности учреждения. Концепция представляет собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности. Следует помнить, что основным принципом создания системы безопасности должно стать обеспечение заданного уровня защищенности от возможных угроз при минимальной

стоимости средств и систем защиты.

Работы в области защиты информации следует поручать только предприятиям и организациям, имеющим лицензию ФСТЭК Российской Федерации - это дает надежную гарантию высокого качества работ и позволит, в случае необходимости, применить юридические санкции. Для обработки информации ограниченного доступа необходимо применять такие аппаратные средства и программные продукты, не использующие методы криптографии, которые имеют сертификат, выданный ФСТЭК. Для средств защиты с применением криптографии необходим сертификат ФАПСИ. Перечни средств защиты, прошедших сертификацию, постоянно обновляются и рассылаются ФСТЭК во все администрации регионов России и заинтересованные ведомства. Подобная информация есть и в Госстандарте России, который ведет сводный перечень средств, имеющих различные сертификаты.

Необходимо убедиться в достаточности принятых мер, проведя проверку эффективности средств защиты. Следует помнить, что информационная безопасность любой организации зависит не только, а подчас

— не столько от технических средств, но и от людей, их использующих. При этом необходимо, во-первых, научить сотрудников пользоваться защитными средствами. На каждом рабочем месте должны быть инструкции и памятки, в доступной форме информирующие персонал об обязательных мерах по поддержанию информационной безопасности. Во-вторых, необходимо тщательно подобрать и подготовить специалистов, способных грамотно обслуживать систему защиты.

Необходимо организовать подготовку персонала по вопросам защиты информации, разработать и довести до каждого правила информационной безопасности.

В результате выполнения предложенных организационных мероприятий следует ожидать качественно более высокого уровня безопасности, снижения страховых платежей за счет повышения защищенности повседневной профессиональной деятельности от различных видов угроз, предотвращения ущерба от противоправных действий злоумышленников.

В руководящем документе Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», указывается, что организационные мероприятия в рамках системы защиты информации от несанкционированного доступа в автоматизированных системах, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

Задание № 2. Построить полную модель угроз и уязвимости компании, создав:

отделы (структурное подразделение организации, например, отдел

кадров, бухгалтерия и т.д.);

- сетевые группы (например, сервер и 1 рабочая станция);
- ресурсы (объект хранения ценной информации, например, твердая копия, рабочая станция, сервер);
- сетевые устройства (устройства, с помощью которых осуществляются связи между ресурсами сети, например, точка доступа, маршрутизатор и т.д.);
- виды информации (вид ценной информации, хранимой и обрабатываемой на ресурсе, например, бухгалтерская информация, информация о ценовых предложениях и т.д.);
- группы пользователей (группы пользователей, имеющих одинаковый класс и средства защиты, обладающих одинаковыми правами доступа к ценной информации, например, офицеры безопасности, топ - менеджеры и т.д.);
- бизнес – процесс (производственные процессы, в которых обрабатывается данная информация, например, внесение изменений, охрана предприятия и т.д.).

Для того чтобы наиболее полно охватить все угрозы, действующие на информационные ресурсы организации, вводится раздел «Политика безопасности», который содержит вопросы, ответы на которые влияют на эффективность средств защиты и изменяют риск реализации угроз информационной безопасности. Разделы, по которым проектируется политика безопасности:

- организационные меры;
- безопасность персонала;
- физическая безопасность;
- управление коммуникациями и процессами;
- контроль доступа;
- разработка и сопровождение систем;
- непрерывность ведения бизнеса;
- соответствие системы требованиям.

Ответ на каждый вопрос необходимо утвердить нажатием клавиши «Принять».

Далее производится работа с разделом «Связи», в котором определяются связи между объектами, занесенными в разделе «Моделирование системы». При выборе отдела рабочее поле отображает все ресурсы, принадлежащие данному отделу. Пользователь может просмотреть свойства ресурсов и при необходимости отредактировать их. При выборе ресурса рабочее поле отображает закладки для определения связей между данным ресурсом и остальными элементами информационной системы. Количество закладок зависит от типа ресурса. В этом разделе рассматриваются следующие закладки:

- виды информации (определяется ценная информация, используемая на ресурсах);

- группы пользователей (определяются пользователи, имеющие доступ к ценной информации на ресурсах);
- каналы связей (определяется, с помощью каких сетевых устройств осуществляется доступ к ресурсу «сервер» группами пользователей);
- бизнес-процессы (определяется, в каких бизнес-процессах используется ценная информация);
- средства защиты (определяется, какие средства защиты применяются для ресурсов);
- средства защиты информации (определяется, какие средства защиты применяются для ценной информации на ресурсах).

Окно «Отчет» позволяет просмотреть созданные отчеты. Каждый отчет располагается на отдельной закладке. При нажатии на «Создать отчет» появляется окно «Конфигурация отчета», которая может быть практически любой, позволяя создавать как краткие отчеты для руководства, так и детальные отчеты для дальнейшей работы с результатами. Нажать «Открыть отчет». После просмотра отчета перенести проект с сетевого сервера на локальный, для чего необходимо войти в систему как пользователь, обладающий правом на чтение данного проекта. Здесь свой проект следует
«сохранить как…», распечатать, приложить к отчету о практическому занятию.
Варианты заданий для самостоятельного выполнения
Создать проект модели угроз и уязвимости на конкретном предприятии.

Содержание отчета и его форма

Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать: ответы на Задания для контроля владения компетенциями работы.

Задания для контроля владения компетенциями:

1 Задачи перспективного развития компании.
2 Необходимые шаги для реализации комплексного плана совершенствования корпоративной системы защиты информации.
3 Направления аналитической работы в области информационной безопасности.
4 Двеосновные задачи любой системы информационной безопасности.
5 Что необходимо делать для выполнения этих двух задач.
6 Изобразить модель построения корпоративной системы защиты информации.
7 Что такое модель защиты информации.
8 Угрозы
9 Уязвимости
10 Риск
11 Что необходимо сделать для построения сбалансированной

системы информационной безопасности.

12 Как строится модель угроз и уязвимостей.
13 Что необходимо определить по завершении работ.
14 На чем основана адекватность оценки безопасности.
15 При построении системы информационной безопасности создается техническая документация, включающая …

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 22.

Организация режимов безопасности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 90 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Учебная и воспитательная цели:

Изучить положения об отделе и секторе режима и охраны, должностные инструкции инспектора по режиму, коменданта здания, мастера по обучению вневедомственной охраны, положение о структуре службы безопасности предприятия и инструкцию о пропускном и внутриобъектовом режимах.. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

1 Примерные положения о режимах, об отделах и секторах режима и охраны, инструкции, должностные инструкции специалистов.

Краткие теоретические или справочно-информационные материалы

Примерное положение об отделе режима и охраны

Отдел режима и охраны является самостоятельным структурным подразделением службы безопасности и подчиняется начальнику службы безопасности.

В своей деятельности отдел руководствуется требованиями инструкции по организации режима и охране.

Задачи

1 Организация и осуществление мер по обеспечению безопасности деятельности и защите сведений, составляющих государственную и коммерческую тайну.
2 Разработка и совершенствование системы предотвращения несанкционированного допуска и доступа к сведениям, составляющим коммерческую тайну.
3 Организация и поддержание пропускного и внутриобъектного режима.
4 Организация охраны аттестованных по режиму конфиденциальности помещений.
5 Организация личной охраны руководителей и ведущих сотрудников.
6 Организация и установление мер физической и технической защиты зданий и помещений.
7 Организация, разработка и контроль системы безопасности в повседневных и особых условиях (стихийные бедствия, поломки, аварии, беспорядки и т.п.).

Структура

В составе отдела режима и охраны имеются следующие структурные единицы:

1 Сектор режима.
2 Сектор охраны.
3 Функции Функции

1 Организует работу по выполнению решений, приказов и распоряжений руководства фирмы по обеспечению защиты коммерческих секретов и обеспечению безопасности деятельности.
2 Определяет единство действий и организует защиту, безопасность, сохранность документов и ценностей в обычных и особых условиях.
3 Разрабатывает, обновляет и дополняет инструкции, положения и иные нормативные материалы по режиму и охране.
4 Осуществляет руководство работой по установлению степени конфиденциальности сведений, содержащихся в документах. Совместно с основными подразделениями проводит систематическую работу по анализу практики применения перечня сведений, составляющих коммерческую тайну, по подготовке и внесению в него в установленном порядке необходимых изменений и дополнений, а также организует его переработку и переиздание.
5 Организует разработку и контроль за эффективностью действующей разрешительной системы допуска сотрудников, компаньонов и клиентов к ознакомлению и работе с документами конфиденциального характера, с целью исключения возможности ознакомления со сведениями, не относящимися к выполняемой ими работе.
6 Разрабатывает и рассматривает совместно со специальным

отделом и подразделениями предложения по совершенствованию делопроизводства с грифом "Коммерческая тайна", предотвращению фактов включения в документы секретного и несекретного характера излишнего объема сведений, являющихся коммерческой тайной, сокращению издаваемых или разрабатываемых документов конфиденциального характера, неоправданной их рассылки.

7 Организует и обеспечивает систему контролируемого доступа и специального пропускного режима в здания и помещения.

8 Организует, обеспечивает и контролирует выполнение требований внутриобъектового режима.

9 Определяет систему охраны и участвует в ее организации и обеспечении работы выделенных помещений.

10 Организует разработку тактических принципов использования средств автоматизации, сигнализации, связи и охраны.

11 Организует охрану, пропускной, допускной и внутриобъектовый режим и осуществляет оперативно-методическое руководство работами по защите выделенных помещений и информации, обрабатываемой и передаваемой с использованием технических средств.

12 Осуществляет руководство и режим защиты коммерческих сведений в работе по отбору, хранению и использованию архивных материалов.

13 Осуществляет методическое руководство и принимает непосредственное участие в проведении предупредительно- профилактической работы с исполнителями работ и документов конфиденциального характера.

14 Организует проведение служебных расследований по фактам утраты конфиденциальных документов, разглашения охраняемых сведений, нарушений охраны и пропускного режима, необоснованного ознакомления сотрудников и командированных лиц со сведениями, составляющими государственную и коммерческую тайну, и по Другим фактам, которые привели к утечке или создали условия, способствующие утечке конфиденциальной информации.

15 Обеспечивает личную охрану руководства и сотрудников. Права начальника отдела

1 На основе единоначалия руководит деятельностью отдела по режиму и охране в соответствии с возложенными на отдел задач и функций.

2 Назначает проведение проверок состояния и эффективности работы по обеспечению сохранения коммерческих секретов, режима безопасности, охраны и технического ее обеспечения.

3 Требует от сотрудников предоставления объяснений по фактам, которые привели или могли привести к утечке информации, составляющей коммерческую тайну.

4 Ходатайствует о поощрении сотрудников, активно участвующих в работе по предупреждению утечки охраняемых сведений, выполнении требований режима и охраны.

Ответственность

Всю ответственность за качество, объем и своевременность выполнения возложенных настоящим положением на отдел задач и функций несет начальник отдела.

Примерное положение о секторе режима

Сектор режима является подразделением отдела режима и охраны службы безопасности и подчиняется непосредственно начальнику отдела.

В своей деятельности сектор руководствуется требованиями инструкции по режиму и охране в части режима.

Задачи

1 Организация пропускного и внутриобъектового режима.

2 Разработка разрешительной системы и обеспечение допуска сотрудников к документам, материалам и сведениям, составляющим коммерческую тайну.

3 Контроль за соблюдением режима допуска к сведениям и документам.

4 Совершенствование системы пропускного и внутриобъектового режима.

5 Участие в разработке перечня сведений, составляющих коммерческую тайну.

Структура

В составе сектора режима выделяются следующие штатные должности:

- заведующий сектором режима;
- старший инспектор по режиму — начальник бюро пропусков;
- инспектор по режиму;
- инспектор по работе с персоналом, допущенным к сведениям, составляющим коммерческую тайну.

Функции

В части обеспечения режима основными функциями сектора являются разработка, осуществление основных положений системы получения разрешений на доступ к информации, являющейся коммерческой тайной, в том числе:

- права, обязанности и ответственность сотрудников, допущенных к работе с документами, содержащими коммерческую тайну;
- схема выдачи разрешений на доступ сотрудников к сведениям, составляющим коммерческую тайну;
- порядок доступа на совещания по вопросам, содержащим сведения, являющиеся коммерческой тайной;
- порядок и контроль доступа к сведениям, составляющим коммерческую тайну, представителей других фирм и государственных органов;
- ведение, уточнение и изменение перечня сведений, составляющих коммерческую тайну;

- учет сотрудников, допущенных к работам с документами и материалами, содержащими сведения, составляющие коммерческую тайну;
- учет и анализ нарушений режима работы с документами, содержащими коммерческую тайну, различного рода попыток несанкционированного доступа к конфиденциальным документам традиционного и автоматизированного исполнения (базы данных, персональные файлы и др.), случаев телефонных переговоров, содержащих конфиденциальную информацию;
- организация и проведение деловых совещаний, переговоров и встреч с обсуждением вопросов, связанных с коммерческой тайной;
- организация и обеспечение пропускного и внутриобъектового режима: выдача пропусков (постоянных, временных, разовых); порядок посещения, учет посетителей;
- определение выделенных помещений, проведение их паспортизации, обеспечение их защиты совместно с группой инженерно- технической защиты информации.

В части работы с персоналом учитывается, что сотрудники — главный источник утечки конфиденциальной информации. С учетом этого функции группы составляют:

- беседы с поступающими на работу в подразделения, работа которых связана с коммерческой тайной, с целью установления их пригодности для этой работы;
- изучение прошлой трудовой деятельности поступающего на работу;
- оформление обязательств о неразглашении сведений, составляющих коммерческую тайну;
- анализ служебной осведомленности сотрудников;
- анализ и учет трудовой удовлетворенности с целью предупреждения увольнения сотрудников, допущенных к сведениям, составляющим коммерческую тайну;
- ведение досье на сотрудников, допущенных к документам с коммерческой тайной;
- организация обучения сотрудников по вопросам защиты коммерческой тайны;
- беседы с увольняющимися и оформление обязательства не разглашать коммерческие секреты.

Кроме того, сектор в тесном взаимодействии с отделом кадров:

- разрабатывает планы комплектования кадрами;
- оформляет прием, перевод и увольнение сотрудников, допущенных к коммерческой тайне;
- готовит материалы для представления сотрудников к поощрениям и должностным перемещениям.

Права

1 Проводить беседы с поступающими на работу и увольняющимися

и оформлять обязательства о неразглашении сведений, составляющих коммерческую тайну.

2 Требовать от сотрудников и клиентов строгого выполнения установленного пропускного и внутриобъектового режима.

3 Проводить проверку состояния и организации работы по обеспечению режима работы с документами, составляющими коммерческую тайну.

4 Требовать от сотрудников письменных объяснений по фактам нарушения пропускного и внутриобъектового режима.

5 Возбуждать ходатайства перед руководством о привлечении к дисциплинарной ответственности лиц, допустивших нарушения режима.

6 Представлять к поощрениям сотрудников, добросовестно выполняющих обязанности по сохранению в тайне секретных сведений.

7 Ответственность

8 Всю полноту ответственности за выполнение задач и функций по режиму и работе с персоналом несет заведующий сектором режима.

9 Степень ответственности других сотрудников сектора устанавливается должностными инструкциями.

Примерное положение о секторе охраны

Сектор охраны является структурной единицей отдела режима и охраны и подчиняется непосредственно начальнику этого отдела.

В своей деятельности сектор руководствуется требованиями инструкции по организации режима и охраны в части охраны.

Задачи

Обеспечение надежной охраны зданий, помещений, оборудования, валютных и материальных ценностей, а также личной охраны руководящего состава в обычных и экстремальных условиях.

Структура

1 Сектор охраны состоит из:

~ комендантской службы;

~ группы охраны.

2 Комендантская служба может состоять из коменданта здания, дежурного мастера по вневедомственной и объектовой технической охране и дежурного мастера по противопожарной охране.

Функции

1 Сектор охраны осуществляет охрану зданий, помещений, оборудования, линий связи и перевозок, пожарную охрану, а также личную охрану руководящего состава.

2 Сектор охраны обеспечивает необходимые условия, исключающие несанкционированный доступ в охраняемые здания, помещения, отдельные конфиденциальные участки и зоны территории и служебных помещений.

Особое внимание уделяется критическим условиям, связанным со стихийными бедствиями, поломками, авариями.

3 Сектор охраны:

- реализует учет, контроль и наблюдение за охраняемыми зонами, помещениями и хранилищами;
- обеспечивает установку и работу на местах технических средств охраны, охранной и пожарной сигнализации;
- осуществляет прием под охрану и сдачу в эксплуатацию охраняемых помещений, проверяя при этом надежное срабатывание средств охраны, делая соответствующую запись в журнале приема и сдачи под охрану;
- принимает меры по ликвидации возможных пожаров и других аварийных ситуаций.
- в части личной охраны руководства сектор руководствуется отдельным положением, разрабатываемым службой безопасности с учетом конкретных условий ее деятельности.

Права

1 Проверять наличие, состояние и функционирование технических средств охраны, охранной и пожарной сигнализации.
2 Требовать строгого соблюдения установленного внутриобъектового режима и правил трудового распорядка.
3 Участвовать в разработке мероприятий по усилению безопасности и сохранности имущества, средств, зданий и помещений.
4 Не допускать случаев использования неисправного оборудования охранной и пожарной техники.
5 Принимать меры воздействия к сотрудникам, допускающим порчу или неправильную эксплуатацию охранно-пожарной техники.
6 Требовать своевременного ремонта и профилактики технических средств охраны и пожарной сигнализации.

5 Ответственность

Всю полноту ответственности за качество и своевременность выполнения возложенных на сектор настоящим положением задач и функций несет заведующий сектором.

Примерная должностная инструкция инспектора по режиму

Инспектор по режиму подчиняется начальнику сектора по режиму.

В своей работе руководствуется инструкцией по организации режима и охраны.

Обязанности

Инспектор по режиму обязан:

- твердо знать и правильно выполнять инструкцию и правила по организации пропускного и внутриобъектового режима;
- вести журнал учета бланков удостоверений, постоянных и временных пропусков;
- принимать от подразделений фирмы заявки на оформление удостоверений и пропусков;
- вести карточки учета сотрудников фирмы, получивших удостоверения;

~ вести делопроизводство в секторе режима. Права

Имеет право:

— требовать своевременно представлять заявки на разовые пропуски для посетителей и командированных;
— контролировать наличие и срок действия постоянных пропусков и удостоверений.

Ответственность

Инспектор по режиму несет ответственность за:

— оформление и выдачу удостоверений личности;
— хранение и учет бланков удостоверений, постоянных пропусков;
— ведение картотеки выданных удостоверений и пропусков.

Примерная должностная инструкция инспектора сектора режима по работе с персоналом, допущенным к материалам с грифом

Инспектор по работе с персоналом, допущенным к сведениям, составляющим коммерческую тайну, непосредственно подчиняется заведующему сектором режима в части специальной работы, а по общим кадровым вопросам выполняет требования отдела кадров.

Обязанности

1 Проводить беседы с поступающими на работу в подразделения, в которых обрабатываются сведения, составляющие коммерческую тайну.
2 Изучать поступающего на работу сотрудника в части его прошлой трудовой деятельности.
3 Оформлять обязательства о неразглашении сведений, составляющих коммерческую тайну.
4 Анализировать служебную осведомленность сотрудников, работающих со сведениями, составляющими коммерческую тайну.
5 Изучать состояние трудовой удовлетворенности сотрудников, допущенных к работе с конфиденциальной информацией, с целью предупреждения их увольнения.
6 Вести досье на сотрудников, допущенных к документам с грифом «Коммерческая тайна».
7 Участвовать в обучении сотрудников по вопросам защиты коммерческой тайны.
8 Вести беседы с увольняющимися и оформлять обязательства о неразглашении коммерческих секретов.
9 Участвовать в разработке планов комплектования кадрами подразделений, работающих с конфиденциальными документами.
10 Оформлять прием, перевод и увольнение сотрудников, допущенных к сведениям, составляющим коммерческую тайну.
11 Готовить материалы для представления сотрудников к поощрениям и должностным перемещениям.

Права

1 Проводить беседы с поступающими на работу и увольняющимися

и оформлять обязательства о неразглашении сведений, составляющих коммерческую тайну.

2 Требовать от сотрудников письменных объяснений по фактам нарушения требований сохранности конфиденциальной информации.

3 Возбуждать ходатайство перед руководством о привлечении к дисциплинарной ответственности лиц, допускающих нарушения режима.

Ответственность

Несет всю полноту ответственности за подбор и расстановку кадров в рамках данной должностной инструкции.

Примерная должностная инструкция инженера сектора охраны

Инженер сектора охраны подчиняется начальнику сектора и в своей работе руководствуется требованиями инструкции по режиму и охране в части охраны.

Обязанности

Инженер сектора охраны обязан:

~ твердо знать состав и порядок работы используемых на предприятии технических средств пожарной сигнализации и систем охраны;

~ систематически проверять, глубоко анализировать и обобщать практику работы по обеспечению охранного, пропускного и внутриобъектового режима, допуска лиц на предприятие, вырабатывать рекомендации и предложения по их выполнению;

~ вносить предложения по внедрению на предприятии новых технических средств охранной сигнализации.

Права

Инженер сектора охраны имеет право:

— проверять правильность работы средств охранной сигнализации;

— требовать от сотрудников бережного отношения к техническим средствам охраны помещений;

— докладывать руководству о случаях выхода из строя охранных систем и принимать меры по обеспечению их работоспособности.

Ответственность

Инженер сектора охраны несет ответственность за надежную работу охранных и охранно-пожарных технических средств.

Примерная должностная инструкция коменданта здания

Комендант здания подчиняется заведующему сектором охраны.

На время исполнения комендантом здания своих служебных обязанностей ему подчиняются инспектор пожарного надзора, дежурные электро- и сантехнической службы, плотники и уборщицы помещений.

Обязанности

1 Знать требования инструкции по организации пропускного и внутриобъектового режима в зданиях и помещениях и правила внутреннего трудового распорядка работы структурных подразделений и дежурных служб.

2 Знать порядок закрытия и открытия служебных помещений, в том

числе и сдаваемых под вневедомственную и внутриобъектовую охрану, а также организацию хранения и выдачи ключей сотрудникам, ответственным за охраняемые помещения.

3 Ежедневно, по окончании работы подразделений с клиентами и закрытию входа в здание, осуществлять осмотр помещений на предмет возможного выявления посторонних предметов, подозрительных на взрывание, зажигательные и другие устройства, представляющие опасность как для жизни и здоровья сотрудников, так и для безопасности.

4 По окончании рабочего дня, в ходе уборки помещений, совместно с инспектором пожарного надзора, и при необходимости с дежурными электриками и сантехниками, обходом проверять состояние помещений.

5 Рабочие ключи и контрольные экземпляры от всех служебных помещений, запасных входов и выходов хранить в комнате коменданта в сейфе, в опечатанном виде. Выдачу ключей производить под расписку в специальной книге. Дубликат ключа от сейфа должен быть и у инспектора пожарного надзора.

6 После 20.00 часов удалять из здания всех сотрудников, оставив только уборщиц, дежурную службу, а также лиц, имеющих на то разрешение руководства или работающих по специальному графику.

7 В предвыходные и предпраздничные дни осмотр помещений здания осуществлять совместно с инспектором пожарного надзора и начальником караула вневедомственной охраны в обязательном порядке.

8 Во всех случаях обнаружения открытых без соответствующего разрешения помещений, а также выявления поврежденных печатей, запирающих устройств, хищения и порчи имущества комендант совместно с начальником караула вневедомственной охраны составляют акт и доклад руководству службы безопасности.

Права

1 Проверять помещения зданий на наличие, состояние и функционирование средств охраны, охранной и пожарной сигнализации.

2 Проверять порядок эвакуации сотрудников и технических средств в чрезвычайных обстоятельствах.

3 Участвовать в выработке мероприятий по усилению безопасности зданий и помещений.

Ответственность

Комендант здания несет личную ответственность за состояние охраны, охранной и пожарной сигнализации здания и помещений.

Примерная должностная инструкция мастера по обеспечению вневедомственной охраны

Дежурный мастер по эксплуатации охранно-пожарной сигнализации подчиняется начальнику отдела режима и охраны.

Обязанности

1 В день заступления на дежурство прибыть на объект к 7 час. 30 мин., произвести внешний осмотр охраняемого объекта и при отсутствии

нарушения снять его с охраны пульта ВВО. При наличии нарушений, т.е. повреждений в системе охранно-пожарной сигнализации, вызвать техника отдела охраны и вместе с ним обследовать помещения, выявить — было ли проникновение в здание.

2 После этого разрешить сотрудникам вход в помещение.

3 Перед окончанием рабочего дня обойти подконтрольные помещения, потребовать от сотрудников подготовить помещения к сдаче под охрану (закрыть все форточки, окна, двери и т.д.) и сдаче ключей от комнат в шкаф.

4 По имеющимся у него пультовым номерам сообщить на пульт о сдаче и получить в ответ фамилию принявшего и пароль.

5 В отношении пультового номера кассы осуществлять контроль по обязательной и своевременной сдаче на пульт охраны.

6 Свою работу в день дежурства четко согласовать с оперативным дежурным предприятия.

Права

Имеет право требовать от сотрудников своевременной сдачи охраняемых помещений и выполнения ими установленного порядка сдачи и приема помещений под охрану.

Ответственность

Несет ответственность за работоспособность технических средств охраны помещений.

Положение о структуре службы безопасности предприятия

Многогранность сферы обеспечения безопасности и защиты информации требует создания специальной службы, осуществляющей реализацию специальных защитных мероприятий.

Структура, численность и состав службы безопасности предприятия (фирмы, компании и т.д.) за рубежом определяются реальными потребностями предприятия и степенью конфиденциальности ее информации. В зависимости от масштабов и мощности организации деятельность по обеспечению безопасности предприятия и защиты информации может быть реализована от абонентного обслуживания силами специальных центров безопасности до полномасштабной службы компании с развитой штатной численностью. В зарубежных источниках, например, рассматривается следующая структура службы безопасности фирмы: возглавляется начальником службы безопасности, которому подчинены служба охраны, инспектор безопасности, консультант по безопасности и служба противопожарной охраны.

С учетом накопленного зарубежного и отечественного опыта и особенностей рыночной экономики предлагается рабочий вариант службы безопасности предприятия среднего масштаба производства, ее структура и должностные инструкции.

Общие положения

Основными задачами службы безопасности предприятия являются обеспечение безопасности предприятия, производства, продукции и защита коммерческой, промышленной, финансовой, деловой и другой информации,

независимо от ее назначения и форм при всем многообразии возможных каналов ее утечки и различных злонамеренных действий со стороны конкурентов.

Правовые основы деятельности службы безопасности

Основные положения, состав и организация службы безопасности имеют юридическую силу в том случае, если они зафиксированы в основополагающих правовых, юридических и организационных документах предприятия.

В основу деятельности службы безопасности положены:

- Закон Российской Федерации «О безопасности»;
- Законы и регламенты России, обеспечивающие безопасность деятельности и сохранность коммерческой тайны;
- Закон о предприятиях и предпринимательской деятельности;
- Кодекс законов о труде (КЗОТ);
- Устав предприятия, коллективный договор, трудовые договоры, правила внутреннего трудового распорядка сотрудников, должностные обязанности руководителей, специалистов, рабочих и служащих.

Основные задачи службы безопасности

- 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.

Общие функции службы безопасности

- 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 обеспечение безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
- разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организует и контролирует выполнение требований «ИНСТРУКЦИИ по защите коммерческой тайны»;
- изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций о деятельности предприятия и его клиентов, партнеров, смежников;
- организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;
- разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие
- нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
- обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;
- осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны;
- организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был глубоко осознанный подход;
- ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;
- ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
- поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения

криминогенной обстановки в районе (зоне).

Состав службы безопасности

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия.

Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности.

Организационно служба безопасности состоит из следующих структурных единиц:

- отдела режима и охраны, в составе сектора режима и сектора охраны;
- специальногоотдела в составе сектора обработки секретных документов и сектора обработки документов с грифом «Коммерческая тайна»;
- инженерно-технической группы;
- группы безопасности внешней деятельности.

Права, обязанности и ответственность сотрудников службы безопасности

Сотрудники подразделений службы безопасности в целях обеспечения защиты сведений, составляющих коммерческую тайну, имеют право:

- требовать от всех сотрудников предприятия, партнеров, клиентов строгого и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите коммерческой тайны;
- вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.

Сотрудники службы безопасности обязаны:

- осуществлять контроль за соблюдением «инструкции по защите коммерческой тайны;
- докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действий, могущих привести к утечке конфиденциальной информации или утрате документов или изделий;
- не допускать неправомерного ознакомления с документами и материалами с грифом «Коммерческая тайна» посторонних лиц.

Сотрудники службы безопасности несут ответственность

- за личное нарушение безопасности коммерческой тайны и
- за неиспользование своих прав при выполнении функциональных обязанностей по защите конфиденциальных сведений сотрудниками предприятия.

Нештатные структуры службы безопасности

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства предприятия и службы безопасности могут создаваться отдельные комиссии, решающие определенные контрольно-ревизионные функции на временной или постоянной основе, такие как:

- квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей);

- комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и телевидении, семинарах, симпозиумах, конференциях и т.п.;
- периодические проверочные комиссии для проверки знаний и умений выполнять требования нормативных документов по защите коммерческой тайны, а также по оценке эффективности и надежности защитных мероприятий по обеспечению безопасности предприятия.

Инструкция о пропускном и внутриобъектовом режимах (на примере Московской Западной таможни)

Настоящая Инструкция определяет основные требования и порядок организации пропускного и внутриобъектового режимов на объектах Московской западной таможни.

Выполнение требований настоящей Инструкции обязательно для всех сотрудников, постоянно или временно работающих в таможне, всех юридических и физических лиц, осуществляющих свою деятельность на данных объектах или предоставляющих свои помещения для деятельности структурных подразделений таможни.

Пропускной режим - совокупность мероприятий и правил, исключающих возможность несанкционированного прохода лиц, проезда транспортных средств, проноса (провоза) имущества на объект и с объекта.

Внутриобъектовый режим - совокупность мероприятий и правил, выполняемых сотрудниками таможни и посетителями, находящимися на охраняемых объектах, в соответствии с требованиями внутреннего распорядка работы таможни и пожарной безопасности.

Объект - здание (строение, сооружение, помещение), в котором размещается таможенный орган (подразделение) и прилегающая к нему территория, а также зона таможенного контроля (оформления), площадки, содержащие охраняемые предметы.

Ответственность за организацию пропускного и внутриобъектового режимов на объектах возлагается на начальников подразделений таможни, в ведении которых находится данный объект.

Пропускной и внутриобъектовый режимы в этих зданиях (помещениях) обеспечивают специально подготовленные и назначенные в соответствии с графиком дежурств, утвержденным старшим таможенного объекта, сотрудники подразделений таможни.

Ответственность за обеспечение пропускного и внутриобъектового режимов на объектах, где выставляются наряды таможенной охраны, возлагается на начальника отряда таможенной охраны.

Организация пропускного и внутриобъектового режимов на территории зон таможенного контроля, таможенных складов и складов временного хранения, где по роду своей деятельности располагаются подразделения таможни, осуществляется владельцами склада в соответствии с требованиями, предъявляемыми к оборудованию и обустройству зон таможенного контроля,

СВХ (ТС) и согласованными с руководством таможни, при получении лицензии на право владения складом.
Начальник таможни (заместитель начальника таможни) при согласовании инструкций о пропускном режиме на складах устанавливает конкретные требования к администрации склада по обеспечению пропускного режима, охране объекта, помещений и сотрудников таможни.
Для организации пропускного и внутриобъектового режимов на объектах, складах и складах временного хранения, где располагаются отдельные структурные подразделения таможни, разрабатываются инструкции по организации пропускного и внутриобъектового режимов (инструкции разрабатывают начальники данных подразделений, их согласовывают со службой собственной безопасности, подразделением таможенной охраны и владельцем объекта) и утверждаются начальником таможни или его заместителем.
Контроль за соблюдением пропускного и внутриобъектового режимов на объектах, находящихся под таможенной охраной, а также за его организацией на территории зон таможенного контроля и в помещениях, занимаемых отдельно размещенными подразделениями таможни, осуществляют заместители начальника таможни, курирующие таможенный пост, в состав которого входит данное подразделение, и начальник отряда таможенной охраны.
Виды пропусков и отличительных шифров
В качестве пропускных документов могут быть: удостоверения, пропуска. В свою очередь пропуска (Рисунок 2) бывают двух видов: для сотрудников (посетителей) и материальные.

Пропуска			
Для сотрудников и посетителей			Для автотранспорта
Разовые	Временные	Постоянные	Материальные

Рисунок 2 – Виды пропусков

Сотрудникам (посетителям) могут выдаваться пропуска 3-х видов:
- разовые;
- временные;
- постоянные.

Разовые пропуска выдаются, как правило, посетителям. Они действительны в течение 30 минут с момента их выдачи до прохода контрольно-пропускного поста (КПП) и в течение 15 минут после отметки о времени ухода посетителя. Отметка о времени ухода посетителя делается на обратной стороне разового пропуска руководителем подразделения, которое посещал посетитель. Разовые пропуска для посетителей оформляются в бюро пропусков по письменным заявкам. Заявки на оформление и выдачу разовых пропусков составляются по установленной форме (приложение) и подаются в

отряд таможенной охраны (бюро пропусков) накануне дня посещения, в исключительных случаях - в день посещения. Право подписи письменных заявок на оформление разовых пропусков имеют начальники структурных подразделений таможни и их заместители. Если посетитель имеет на руках направление установленной формы с таможенного поста или функционального отдела, наличие заявки на выдачу разового пропуска не требуется. Разовые пропуска оформляются с регистрацией в книге посетителей, только при предъявлении участником ВЭД или посетителем паспорта или удостоверения личности, выданного государственными учреждениями, ведомствами. Если посетитель имеет портфель, папку и т.д., то в разовом пропуске делается отметка: «С портфелем», «С папкой», «С пакетом» и т.д. Посетители проходят по разовым пропускам только в рабочее время, определенное регламентом служебного времени. Сотрудник подразделения, принимающего посетителя, сопровождает его от КПП и обратно.

Примечание. Не действительны водительское удостоверение и удостоверения, выданные коммерческими структурами. Разовые пропуска выдаются посетителю на одно посещение и дают право прохода только в те структурные подразделения, которые указаны в пропуске. Разовые и временные пропуска действительны только при предъявлении участником ВЭД или посетителем паспорта или удостоверения личности, выданного государственными учреждениями, ведомствами.

Прикомандированным сотрудникам, либо сотрудникам, работающим временно, выдаются временные пропуска. Временные пропуска могут быть с фотографиями и без них. С фотографиями временные пропуска выдаются - на срок до 3-х месяцев, без фотографий на срок до 1 месяца. Основанием для оформления (продления) временного пропуска является письменная заявка за подписью руководителя учреждения, подаваемая через отряд документационного обеспечения на имя первого заместителя начальника таможни. Временные пропуска действительны в течение срока, указанного в них, только на территории указанного объекта (объектов) и при предъявлении документа, удостоверяющего личность.

Удостоверения и постоянные пропуска выдают на срок до нескольких лет. Через 1-2 года осуществляется их перерегистрация путем проставления соответствующей отметки.

Материальные пропуска выдаются на внос (вынос), либо ввоз (вывоз) материальных ценностей. По срокам действия они приравниваются к разовым пропускам. Для повышения эффективности службы пропускного режима в настоящее время широкое применение находят технические средства, получившие название системы ограничения и контроля доступа (СО и КД).

Грамотное использование СО и КД позволит надежно обеспечить защиту от несанкционированного доступа не только на территорию фирмы, но и в выделенные помещения и на объекты вычислительной техники. То есть на объекты, где обрабатывается конфиденциальная информация. Структурная схема системы ограничения и контроля доступа показана на рисунке 3.

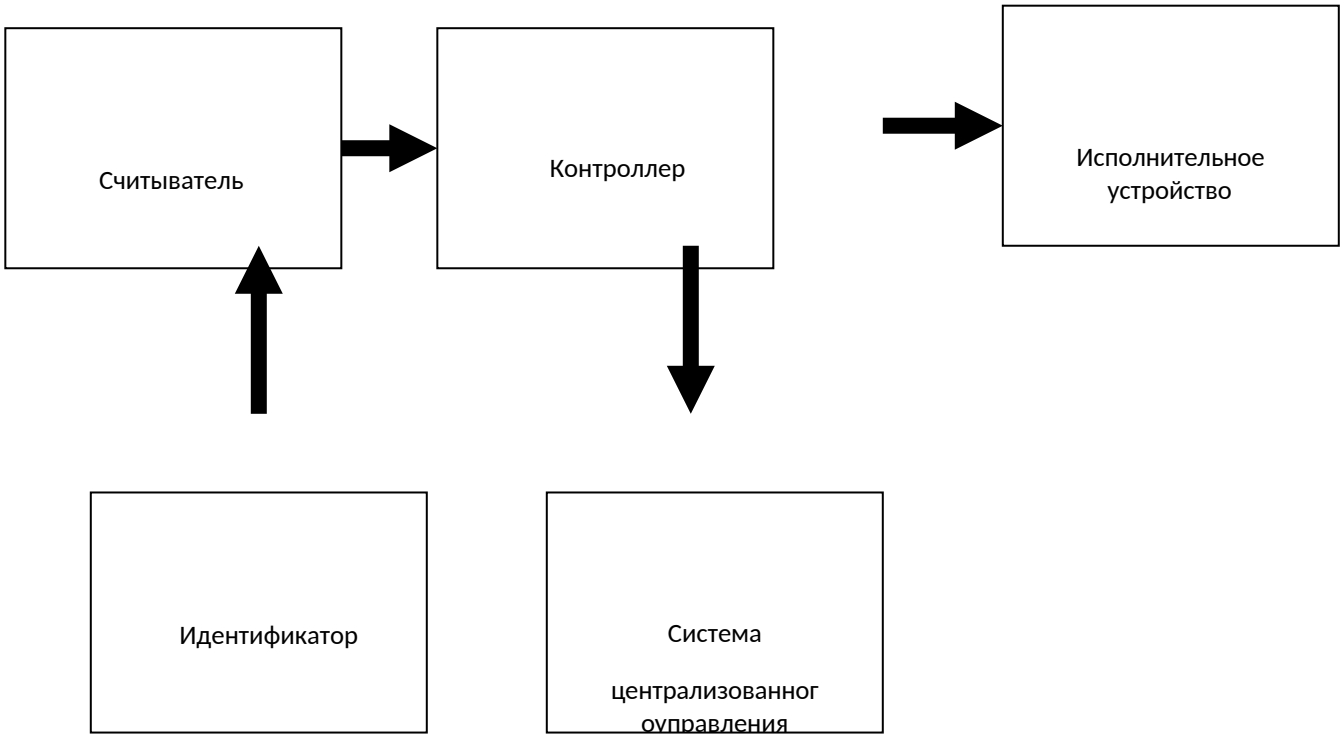

Рисунок 3 - Структурная схема системы ограничения и контроля доступа

Как видно из рисунка основными элементами СО и КД являются:

- считыватель;
- контроллер;
- исполнительное устройство.

Для более сложных систем применяются системы централизованного управления. Они состоят из компьютера (может быть система компьютеров, объединенных в локальную сеть) с мощным программным обеспечением.

Считыватель - это устройство (размещенное в двери или рядом с дверью), предназначенное для считывания специальной кодовой информации, записанной на идентификаторе и передаче этой информации в виде определенного сигнала в контроллер.

Контроллер предназначен для приема и анализа информации, переданной считывателем, сравнения этой информации с эталонной, принятие на этой основе решения о допуске посетителя и выдачи сигнала управления на исполнительное устройство и в систему централизованного управления (при ее наличии).

В качестве исполнительных устройств могут быть электромеханические (электромагнитные) замки, а также устройства управления калитками, воротами, турникетами и т.д. Для того, чтобы посетитель попал на объект (в помещение) он

должен предъявить считывателю свой идентификатор. Таким образом, идентификатор - это устройство, в которое записывается кодовая

информация, однозначно идентифицирующая его владельца.
Классификация идентификаторов, показана на рисунке 4. Идентификаторов бывает несколько видов: электронные ключи, карточки, биометрические.

Таблица 7 - Классификация идентификаторов

<table>
<tr><td colspan="6">Идентификаторы</td></tr>
<tr><td>Электронные ключи</td><td>Pin-код</td><td colspan="2">Карточки</td><td colspan="2">Биометрические</td></tr>
<tr><td>Touch Memory</td><td></td><td>Со штриховым кодом</td><td>Магнитные</td><td>Рисунок ладони</td><td>Голос</td></tr>
<tr><td></td><td></td><td>Перфорированные</td><td>Виганд-карточки</td><td>Отпечатки пальцев</td><td>Радужная оболочка глаза</td></tr>
<tr><td></td><td></td><td colspan="2">Бесконтактные</td><td colspan="2">Масса человека</td></tr>
</table>

Электронные ключи «Touch Memory» представляют собой микросхему, расположенную в прочном металлическом корпусе. Кодовая информация записывается в память данной схемы. Код с электронного ключа считывается при его касании считывателя.
Карточка со штриховымкодом представляет собой пластину с нанесенными на нее полосами черного цвета (штрихами). Кодовая информация содержится в изменяющейся ширине штрихов и расстоянии между ними. Код с такой карточки считывается оптическим считывателем. На магнитную карточку кодовая информация записывается на магнитной полосе.
Перфорированная карточка представляет собой пластину (пластмассовую или металлическую). Кодовая информация на перфорированную карточку наносится в виде отверстий, расположенных в определенном порядке. Код с карточек считывается механическими или оптическими считывателями.
Кодовая информация на Виганд-карточке представляет собой определенным образом расположенные тонкие металлические проволочки, приклеенные на карточке специальным клеем. Информация с карточки считывается электромагнитным считывателем.
Бесконтактная карточка (Proximity) кодовую информацию хранит в микросхеме. Кодовая информация с бесконтактных карточек считывается радиочастотным считывателем.
В последнее время находят применение так называемые биометрические идентификаторы. Хотя отношение к ним специалистов носит противоречивый

характер. В качестве идентификационных признаков могутбыть использованы: рисунок ладони;

- голос человека;
- отпечаток пальца;
- радужная оболочка глаза;
- вес человека и т.д.

Особое место среди идентификаторов занимают PIN-коды. Носителем кодовой информации является память человека. Сотрудник самостоятельно набирает на клавиатуре код и таким образом управляет исполнительным устройством (замком двери, например).

Используя на практике системы ограничения и контроля доступа (СО и КД) можно с большой эффективностью обеспечить пропускной режим, как на территорию фирмы, так и в ее отдельные помещения. Надежно решить, таким образом, проблему защиты от несанкционированного доступа злоумышленников в служебные помещения фирмы, а также проблему от несанкционированного выноса (вывоза) материальных ценностей фирмы.

С другой стороны системы ограничения и контроля доступа (СО и КД) позволит также эффективно решать задачи защиты конфиденциальной информации, обрабатываемой в некоторых помещениях фирмы. Это позволит не только повысить безопасность в целом фирмы как объекта, но и безопасность сведений, относящихся к коммерческой тайне фирмы, что в свою очередь снижает общие затраты на обеспечение безопасности фирмы.

Отчетность за занятие

1. Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.
2. Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

1. *Возженников А. В.* Национальная безопасность: теория, политика, стра- тегия. — М.: РАГС, 1998.
2. Основы национальной безопасности России / под ред. В. Л. Манилова. — М.: Друза. 1998.
3. *Прохожее А.А.* Национальная безопасность: основы теории, сущность, проблемы. — М.: РАГС, 1997.
4. *Прохожее А.А.* Человек и общество: законы социального развития и безопасности. — М.: РАГС, 2002.
5. *Стрельцов А.А.* Обеспечение информационной безопасности России. Теоретические и методологические основы. — М.: МЦНМО, 2002.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM-

совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности

Для выполнения практического занятия студент должен:

1 Ознакомиться с методикой и порядком выполнения работы.

2 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.

3 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

~ работать без соответствующего освещения и вентиляции рабочего места;

~ работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;

~ передвигаться по аудитории без разрешения преподавателя;

~ работать в специализированных аудиториях без сменной обуви;

~ работать на одном рабочем месте более двух человек.

4 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.

5 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы

Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов

Не требуется

Порядок оформления отчета по практическому занятию и его

защиты

Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на вопросы для контроля владения компетенциями работы.

Рекомендации для преподавателей по проведению занятия

К защите требуется отчет с подробными ответами на вопросы.

Задания для контроля владения компетенциями:

1 Назовите задачи структуру отдела режима и охраны.
2 Назовите обязанности инспектора по режиму.
3 Перечислите задачи и структуру сектора режима.
4 Перечислите задачи и структуру сектора охраны.
5 Назовите виды пропусков.
6 Изобразите структурную схему системы ограничения и контроля доступа.
7 Классифицируйте идентификаторы.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 23-24.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 23-24
Организация работы с персоналом

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 180 мин
Вступительная часть 2 мин
Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Учебная и воспитательная цели:

Изучить специальные психологические методики, некоторые уникальные психофизические методы и компьютерные психотехнологии при подборе персонала на работу с конфиденциальной информацией, средства и системы обучения, контроля, проверки и увольнения персонала, работающего с конфиденциальной информацией. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

1 Метапрограммы в подборе и оценке персонала.
2 Обзор методик, применяющихся в корпоративной практике тестирования персонала.
3 Персонал фирмы и его роль в утечке информации.
4 Основные принципы организации профессионального отбора персонала в учреждения и предприятия.
5 Основные рекомендации при организации проверки и отбора кандидатов на работу в организации и предприятия.
6 Процесс увольнения кадров из организации.

Краткие теоретические или справочно-информационные материалы

1 Метапрограммы в подборе и оценке персонала

Профессиональные рекрутеры или специалисты отдела HR часто сталкиваются с такой задачей: необходимо подобрать специалиста на рабочую вакансию, а претендентов несколько. И все очень приятные в общении люди, грамотно отвечающие на поставленные вопросы. По каким критериям выбрать из них подходящего?

Профессионалы, давно работающие в этой области, делают это легко и именуют свое мастерство интуицией. Но практически не могут передать свой опыт другим, так как его трудно формализовать. Начинающие же работу в этой области нарабатывают свой собственный опыт ценой проб и ошибок, часто приводящих к потерям собственного рабочего времени и лишним материальным затратам компании.

Итак, нужны система, структура построения интервью, четко разработанные критерии, простая и универсальная технология, которая обобщит и структурирует опыт. И нужен язык описания.

Хорошая новость заключается в том, что вся эта система уже существует. Она не противоречит действующим тестам и методикам, а легко интегрируется с ними. Кроме того, вы «встраиваете в себя» все необходимые тесты. Для ее освоения не обязательно быть психологом — вы становитесь психологом «по жизни». Система достаточно универсальна, чтобы использовать ее для разных задач — от создания модели компетенций, проведения структурированного диагностического интервью до оценки и мотивирования персонала, подбора команд и создания кадрового резерва. Эта система основана на теории метапрограмм человека.

Метапрограммы — это внутренние характеристики, способы мышления человека, на основании которых строится его поведение. Как человек мыслит, так он и действует. Если человек уверен в себе, в том, что мир вокруг него безопасен, то вы всегда заметите это в его поведении — скажем, в развороте плеч, наклоне головы — и даже говорить он будет особым образом. Если человек не уверен в себе, его беспокоят сомнения, то вы почувствуете это и в позе, и в речи. Мышление и поведение взаимосвязаны.

Метапрограммы выражаются не только в поведении, но и в речевых оборотах. Исследования в области психолингвистики (Ноам Хомский) показывают, что язык, как и внешнее поведение, отражает наше сознание. Но в обыденном общении мы часто обращаем внимание лишь на содержательную часть речи. Если мы будем обращать внимание на «форму» построения речи, то очень многое сможем узнать о человеке, ее произносящем.

Слушая, как говорит человек, наблюдая за его поведением (позы, мимика, скорость реакции, движения глаз и др.), мы можем определить его личностные особенности, которые, как правило, связаны и с профессиональными предпочтениями. Только слушать, слышать и наблюдать

нужно особенным образом. На чем строится подход?

Избирательность внимания. Ценности

Наше внимание устроено так, что оно само выбирает то, что ценно и полезно для человека в данном контексте.

Как это связано с приемом на работу? Задавая определенные вопросы, вы можете выявить зоны интересов претендентов на данную должность. Например, вы задаете вопрос трем претендентам «Что вам важно в вашей работе?» А они вам отвечают:

- первый — «Мне важно, чтобы я мог приносить стабильную прибыль себе и фирме»;
- второй — «Мне хотелось бы реализовать знания, полученные в институте…»,
- третий — «Ну чтоб интересно было, чтобы коллектив был хороший…»

Вслушиваясь в эти слова, вы понимаете, кто из них пришел за:

- финансовым результатом;
- самореализацией;
- развитием; общением.

Умение работать с чужими ценностями, учитывать их, присоединяться к ним — основа любой успешной коммуникации. Все успешные коммуникаторы, будь то управленцы, продавцы или специалисты по связям с общественностью, обладают высокой чуткостью и гибкостью в отношении ценностей своих сотрудников, клиентов или партнеров.

Человек бессознательно использует в речи и поведении привычные способы мышления.

Мы привыкли думать, что в бессознательном состоянии находимся, когда спим или медитируем. На самом деле мы многое делаем бессознательно. Например, «что» говорить — еще контролируем сознательно, а вот «как» — это больше бессознательный процесс. Человек в речи обычно проявляет свой привычный способ мышления, ценности, личные особенности, которые полезно учитывать при профессиональном отборе.

Существует несколько основных метапрограмм, с помощью которых мозг отдельного человека организует работу с входящей и исходящей информацией.

Метапрограммы удобнее рассматривать с помощью шкал с двумя полюсами. При собеседовании обычно используется от 7 до 12 таких шкал. Рассмотрим некоторые из них.

Активность — рефлективность

Всем памятна ситуация, когда на вопрос учителя быстро поднимаются руки — это самые активные ученики сигнализируют о готовности отвечать. Не всегда, правда, ответы бывают правильными. Но таковы уж ученики активные — они сначала действуют, а только потом думают. Люди (и не только дети) активного типа предпочитают действия размышлениям. Едва задача поставлена, они срываются с места и начинают ее выполнять. «Огонь в

глазах» — это про них. Их отличает неутомимость и неусидчивость. Скорость реакции на внешние стимулы у них очень высока. Такие люди, как правило, работают за четверых. Люди рефлективного типа предпочитают сначала размышлять, потом действовать. Они словно бы экономят энергию.

И как же нам по собеседованию определить активного и рефлективного? Задайте вопрос, например: «Чем вы занимались на своей предыдущей работе?» Проследите за построением предложения — в речи активного вы услышите: «Работал с клиентами, подписывал договоры, ездил на переговоры, следил за ассортиментом продукции в магазинах...» Рефлективный же скажет вам: «Вы знаете, в моей работе было очень важно постоянно сопоставлять ситуацию на рынке и учитывать эти изменения в отношениях с нашими клиентами, с которыми у нас постоянные контакты, потому что если бы мы не учитывали этих факторов…» Наблюдения показывают: чем короче предложения, тем активнее личность. Большое количество придаточных предложений свидетельствует о рефлективности.

Представим эту метапрограмму в виде шкалы:

Крайние значения (активный «мотор» или рефлективный «тормоз») встречаются довольно редко. Но предпочтения определить все-таки можно. Статистики подсчитали, что граждан рефлективного типа раз в пять больше, чем активного. А в нашей стране — раз в шесть. Это связано с историческими особенностями, например, во времена сталинских репрессий условием выживания становилось такое личное качество людей, как рефлективность:

«не высовывайся» (запрет активности) — было условием выживания, и оно передалось следующим поколениям. Времена изменились — нужны активные, смелые, предприимчивые. Но память поколений жива, активных — не так много.

Принадлежность к тому или другому типу ничего не говорит об эффективности специалиста, о качестве его работы. Хороших результатов в равной степени может достигать и активный, и рефлективный. Другой вопрос

— на каких должностях: туда, где нужно быстро действовать по ситуации (например, торговый представитель, тренер, руководитель), полезно набирать активных. А в работе финансового аналитика, бухгалтера, эксперта лучше не торопиться — здесь как раз подойдут рефлективные сотрудники.

Референция внутренняя — референция внешняя

Эта пара метапрограмм имеет отношение к тому, кто принимает решение в жизни человека и кто оценивает — сам человек, его воля или обстоятельства и другие люди.

Спросите пришедшего на собеседование: «Когда вы решали для себя, поменять работу или нет,— что на вас влияло, как вы принимали решение?»

~ Одни ответят, что на решение повлияли другие люди: «Мой муж считает, что если я не пойду работать, то потеряю квалификацию…» или обстоятельства: «Ситуация в стране заставила меня искать новую работу…» Это — внешнереферентные. Они постоянно нуждаются в поддержке и внешней оценке.

~ Внутреннереферентный скажет: «Я проанализировал ситуацию,

взвесил все обстоятельства и принял решение о новой работе». Этот контингент имеет свой собственный «волевой центр», который принимает решения и берет ответственность на себя.

- Задайте вопрос: «Как вы поймете — хорошо или плохо выполнена ваша работа?»
- Внутреннереферентный скажет: «Если у меня есть внутреннее чувство удовлетворения, значит работа сделана хорошо». Эти люди хороши на руководящих должностях, на проектах, связанных с ответственностью.
- Внешнереферентный сошлется: «Если начальник принял отчет, если от клиентов не поступило ни одной жалобы — значит, я работаю хорошо». Эти специалисты подходят только для исполнительских должностей.
- Есть еще люди, ориентированные на контекст. Это также внешняя референция, но она связана не с людьми, а с обстоятельствами: человек сошлется на отчеты, нормы, графики, сроки и т.п. Опыт показывает, что хорошие топ-менеджеры второго уровня и специалисты, работающие с финансами, довольно часто узнают о том, как они поработали, глядя на цифры.

Конечно, сделать точное заключение о годности человека для работы можно, только имея метапрограммный профиль конкретной вакансии и конкретного кандидата.

Мотивация избегания — мотивация достижения

У каждого человека есть в жизни цели. И есть внутреннее «топливо» — мотивация — энергия, необходимая для достижения цели. Предположим, два сотрудника одной организации хотят купить машину.

- Один хочет купить машину, чтобы иметь возможность путешествовать, иметь свободу передвижения;
- другой — чтобы не ездить в час пик в метро и не таскать тяжелые грузы на себе.

Цель одинаковая — покупка машины. А направление мотивации разное.

- У одного — на достижение удовольствия и выгод, ему бесполезно будет объяснять, что случится, если он не выполнит ежемесячный план работы. Для таких людей нужны постоянные поощрения.
- у другого — на избегание дискомфорта, его бессмысленно завлекать перспективами развития будущего компании. Штрафы, рассчитаны именно на таких людей.

Хотя дело не столько в системе оплаты, сколько в том, как ее использовать с конкретными людьми, нельзя пренебрегать человеческим фактором.

- Одному стоит сказать: «Работай хорошо — получишь премию».
- А другому: «Смотри, будешь работать плохо — премии лишим!» Направление внимания на себя — на других

Эта пара метапрограмм формируется вокруг вопроса: чьи интересы — свои собственные или интересы других людей являются для человека более важными.

Есть люди, которые и позой, и голосом, и всеми мыслями выражают внимание к собеседнику. Когда они говорят, вы понимаете, что они говорят для вас. Когда слушают, вам понятно, что они действительно вас слушают. Они делают это естественно, и вам еще и еще раз хочется зайти к этому продавцу или агенту. Это то качество, которое мы называем
«клиентоориентированность».
А есть другие люди, разговаривая с которыми чувствуешь отстраненность и холодность, их внимание направлено целиком на себя. Понять, что они вообще вас слушают очень трудно. Специалистов с направлением внимания «на себя» не назовешь клиентоориентированными!
Как вы думаете, в каких профессиях полезно набирать сотрудников с вниманием «на других»? Конечно же, это продавец в торговом зале или человек, который работает с рекламациями и жалобами покупателей. А вот налоговому инспектору или контролеру на транспорте вряд ли полезно быть
«клиентоориентированным» — не соберут они налоги и штрафы, если будут сочувственно выслушивать должников…
Итак, в нашем подходе люди не рассматриваются как хорошие или плохие, каждое рабочее место уникально и требует соответствующего специалиста. Метапрограммный подход дает возможность соизмерить личные качества человека и качественные требования должности, что делает его удобным инструментом для составления модели компетенций, подбора и оценки персонала компании или команды, построения кадрового резерва, написания должностных инструкций. Понимание и учет особенностей и ценностей человека позволяют более точно мотивировать его к работе. Это важно в работе менеджера по персоналу или любого руководителя.

2 Обзор методик, применяющихся в корпоративной практике тестирования персонала

Отечественные компании предпочитают не покупать лицензий на западные тесты и опросники – даже самые популярные, а применять контрафактные. Неудивительно, что говорить об этом не хотят. Достоверными единственными источниками информации в этом случае являются приватные беседы со знакомыми HR-ами и консультантами.
Если компания не хочет пользоваться нелицензионным продуктом, у нее есть два выхода – купить тест у разработчика или разработать самим. Но разработка собственного психологического теста (в отличие от профессионального) – дело трудоемкое и доступно лишь крупным и состоятельным кампаниям, которые обычно тоже привлекают к этой работе провайдера.
Поэтому, можно считать, повезло транснациональным корпорациям, приходящим в Россию с арсеналом собственных тестовых методик и опросников. Так, у компании Procter & Gamble на одном из этапов отбора применяется так называемый Problem Solving Test (PST), который разработан сотрудниками компании P&G приблизительно 10 лет назад и с тех пор

периодически обновляется. Этот тест является стандартным рекрутинговым инструментом кампании и используется практически во всех странах, где работает P&G.

Многие отечественные корпорации сегодня открывают для себя технологии тестирования заново. После ажиотажного бума начала 1990-х годов, когда в страну стали массово привозить нелицензированные, а, вернее, краденые западные тесты, HR-ы столь же массово от них отказывались. Слишком много подделок, а значит, бесполезных результатов. Слишком много денег тратилось впустую.

Существуют две школы тестирования – отечественная и иностранная.

Основа первой – когорта выпускников факультета психологии МГУ. Их тесты и опросники больше годятся для оценки, при которой не важны бизнес- способности – например, при психодиагностике, выявлении отклонений».

Принципы другой привнесли сюда «импортные» компании вроде SHL – крупнейшего провайдера продуктов такого рода в России. Иностранцы изначально ориентировали все программы и линейки продуктов на нужды бизнеса, подобрали соответствующие батареи тестов и работают под заказ.

Российские разработки бизнес-тестов ничем не уступают западным. Просто у западных методик «упаковка» ярче. Но не всегда они адаптированы к российским условиям должным образом.

В соответствии с дилеммой «бизнес-практика – клиника» используемые компаниями тесты можно разделить на две группы:

- функциональные (тесты достижений, бизнес-тесты);
- психологические.

Функциональные специфичны для какой-либо отрасли либо профессии (например, тесты для бухгалтеров, программистов и т. п.). Иногда такие тесты и опросники разрабатываются самими корпорациями, однако возможно и сотрудничество с провайдерами или простая покупка – например, теста для бухгалтеров.

С психологическими тестами и опросниками все запутаннее – брэндированных методик на рынке очень много. Психологические тесты – самая многочисленная и самая разношерстная группа методик, применяющаяся в корпоративной практике тестирования персонала. Условно их можно разделить на 4 группы.

Интеллектуальные. – наиболее известны непосвященным. Знаменитый тест на IQ Айзенка – из этой плеяды. По идее, такие методики должны выявлять уровень интеллектуального развития человека. Однако в кадровом менеджменте практически бесполезны, так как не адаптированы к российским условиям и – кроме того – не дают представления об истинном уровне умственного развития. Опросник уровня субъективного контроля (УСК). Предназначен для того, чтобы определить, в какой степени человек готов брать на себя ответственность за то, что происходит с ним и вокруг него. Один из самых популярных методов оценки персонала при создании внутреннего резерва и составлении плана карьерного продвижения. Профессиограмма.

Социально-психологические. Дают представление о социальной

компетентности человека – конфликтности - неконфликтности, его ролевых качествах в группе. Например, склонных к соперничеству или, напротив, стремящихся к компромиссам. Эти тесты также помогают оценить степень адаптации каждого члена коллектива к совместной деятельности. Распространены достаточно широко. Здесь применяют детектор лжи, тест Кеттела, который позволяет проводить психодиагностические исследования личности, включает задания на диагностику уровня интеллектуального развития, однако, «все вопросы в нем «лобовые», слишком легко «читаются»». В России часто применяется аналогичная многофакторная методика Александра Шмелева. Опросник Томаса Включает 30 вопросов, позволяет выделить типичные способы реагирования сотрудников на конфликтные ситуации (сотрудничество, компромисс, уступчивость, избегание, доминирование). Тест Люшера. применяют в основном из-за простоты, отчасти – из-за «раскрученности». Позволяет по цветовым предпочтениям определять эмоциональное состояние, мотивационную сферу, а также особенности взаимоотношений с другими людьми. Тест Ку-сорт, Тест Розенцвейга**,** предназначенный для оценки развитости у человека черты личности «агрессивность», понимаемой как не вызванная объективными обстоятельствами и необходимостью тенденциями враждебно реагировать на большинство высказываний, действий и поступков окружающих людей. В этом тесте испытуемый получает 24 разных рисунка. На них представлены люди в различных эмоциогенных, близких к стрессовым, ситуациях. Общим для всех рисунков является то, что один человек в них проявляет в отношении другого такие действия, которые вторым человеком могут быть приняты по- разному: как агрессивные, преднамеренно вызывающие или оскорбительные, или случайные, совершенные неумышленно, по незнанию, без желания навредить или унизить человека.

Личностные. В этой группе – знаменитый опросник MMPI (Minnesota Multiphasic Personality Inventory), который HR-специалисты обычно вспоминают первым. Дают представление об индивидуально- психологических особенностях личности, типичных способах поведения человека. В бизнес-практике применяются, несмотря на то, что их, часто называют «клиникой». К ним также обычно относят проективные методики – самые популярные в среде российского HR. Что может быть проще, чем заставить кандидата нарисовать что-либо («Рисунок неизвестного животного» или «Дом, дерево, человек»). Нарисована лошадь. По крайней мере, это существо было больше всего похоже именно на нее. Однако шея у нее была слишком длинная, а хвост висел мочалкой, вместо того, чтобы торчать кверху или хотя бы развеваться параллельно земле. «Это означает, что у вас заниженная самооценка, а эмоции часто выходят из под контроля»,– проинтерпретировала Анна Мостяева, ведущий психолог компании АКМР. Понятно, что на позиции, где нужна уравновешенность и напористость (например, директор по продажам), уже точно не попасть. РНЖ («рисунок неизвестного животного» – та самая лошадь) из-за своей простоты, малых временных затрат и легкости интерпретации пользуется огромным спросом у

большинства специалистов по управлению персоналом. Естественно, применять его можно только тогда, когда есть желание дополнить впечатление о кандидате – ни о какой абсолютной валидности здесь и речи быть не может. А вот правильное применение тестов и опросников в российской корпоративной практике встречается редко. Хорошо, если тесты внедряют под заказ специализированные компании. Однако чаще руководство просто доверяется предпочтениям своих HR-ов. Нетрудно догадаться, что по частотности применения в практике российского HR-менеджмента впереди всех проективные методики. Освоить их несложно. Правда, и информации с их помощью много не получишь. Тем не менее, базовые представления о личности все же дают или рассказать об ассоциациях, возникающих при взгляде на некие абстрактные картины. Тест Майерс Бриггс (Myers Briggs Type Indicator). Этот тест - одна из самых интересных методик, не теряющая своей популярности уже несколько лет. Основана на идеях Юнга. Включает четыре шкалы, которые являются индикаторами базисных предпочтений человека (экстраверсия – интроверсия; сенсорность – интуиция; мышление – чувствование; решение – восприятие). Комбинация личностных предпочтений составляет индивидуальный профиль человека. С его помощью можно определить, какая модель поведения человеку ближе: «коммуникатор»,
«стабилизатор», «стратег» или «пожарник». В конце прошлого века проводился личностный тест опыты Бакстера (из серии «Приборные методики»). Ученый Клив Бакстер - ведущий американский специалист по
«лай-детектору» в 1966 году попробовал присоединить датчик к листу растения. Серия экспериментов дала любопытные результаты - даже мысленная угроза поджечь цветок или сломать его стебель, вызвала всплеск кривых самописца. Было выдвинуто предположение, что растение способно распознавать мысли - реагировать на агрессию. Весьма популярны тематический апперцептивный тест ТАТ, тест СМИЛ.
Тесты способностей. Пользуются стабильной популярностью, так как позволяют определить уровень развития качеств, необходимых кандидату для занятия определенной должности, например, внимания и памяти. Иногда к этой группе относят и весьма популярный в России КОТ (краткий ориентировочный тест). Эта методика выбирается за простоту и за то, что его автор нам неизвестен – о лицензии можно не беспокоиться. Тест находится
«на пограничье» интеллектуальных методик и тестов способностей. Позволяет оценить скорость и логику мышления, внимательность, получить представление о базовом уровне развития интеллекта. Главный недостаток – примитивность: применять КОТ можно только при наборе персонала самого низкого звена. Применяются таблицы Шульте, которые позволяют определять, насколько у кандидата развита память, внимание, способность к анализу. Просты и потому популярны. MMPI слишком громоздок (более 500 вопросов) и «клиничен». Выявляет черты и типы характера, стиль поведения и общения, способность к адаптации и скрытые психические отклонения, в некоторой степени помогает оценить профессиональную пригодность кандидата или сотрудника. В России есть адаптированный вариант этого теста

– СМИЛ (редакция Л. Собчик), который не менее объемен (полный вариант содержит 566 вопросов, а сокращенный – 366). В результате обработки данных этого опросника получается так называемый профиль – числовое выражение оценочных шкал, используемых при расшифровке теста. Именно профиль характеризует особенности личности и психическое состояние испытуемого. Особняком стоят продукты SHL. Тесты способностей и опросники этой компании пользуются спросом у потребителей, предпочитающих покупать лицензионные продукты. Среди опросников наиболее известны OPQ (профессиональный личностный опросник) и MQ (мотивационный опросник). Самые популярные батареи тестов – AMT (тесты для руководителей высшего звена), CRTB (анализ информации), MGIB (тесты для менеджеров). Популярен здесь и тест Равена.

3 Персонал фирмы и его роль в утечке информации

Имеющийся зарубежный и отечественный опыт защиты служебных, производственных и коммерческих секретов свидетельствует, что без активного вовлечения в этот процесс всех сотрудников, имеющих доступ к конфиденциальной информации, результат не может быть полным. Специалисты по защите информации приводят данные, утверждающие, что определяющей фигурой, в обеспечении сохранности ценных сведений предприятия является его сотрудник. Уже сегодня 75% служащих США и 80% в Японии - занимаются обработкой информации.

Анализ угроз информации, проведенной специальной командой по обеспечению безопасности информации проведенной в 2008 г. в министерстве обороны США, позволил выделить следующие виды угроз информационным ресурсам - по возрастанию степени их опасности:

- некомпетентные служащие;
- хакеры и крекеры (специалисты по взлому коммерческих программ);
- неудовлетворенные своим статусом служащие;
- нечестные служащие;
- инициативный шпионаж;
- организованная преступность;
- политические диссиденты;
- террористические группы.

Угроза, исходящая от некомпетентности служащих, по мнению экспертов, основывается на алгоритмической уязвимости информационных систем, которая не исключает возможности некомпетентных действий и может привести к сбоям системы. Эта угроза исходит в основном от слабо

подготовленных администраторов, которые незаслуженно достигли привилегированного положения и способны на нечестные поступки для достижения еще больших привилегий.

Хакеры и крекеры являются гораздо более технически грамотными личностями. В зависимости от мотивов, целей и методов действий всех хакеров можно разбить на несколько групп, начиная с дилетантов и кончая профессионалами. Их можно представить четырьмя группами:

- начинающий хакер;
- освоивший основы работы на ПЭВМ и в составе сети;
- классный специалист;
- специалист высокого класса.

В таблице 1 представлены группы хакеров и их возможности по реализации злонамеренных действий:

Хакеры весьма многообразны и многочисленны, среди них встречаются просто «шутники» и настоящие вандалы. Неудовлетворенные служащие предоставляют внутреннюю угрозу. Они опасны тем, что имеют легальный доступ. То же можно сказать и про нечестных служащих. В данном случае трудно определить, какая из этих категорий служащих может нанести больший урон. Обычно действия таких служащих выливаются в закладку

«логической бомбы». Так в августе 1983 г. на ВАЗе следственной бригадой прокуратуры РСФСР был изобличен программист, который из мести к руководству предприятия умышленно внес изменения в программу ЭВМ, обеспечивающей заданное технологическое функционирование автоматической системы подачи механических узлов на главный сборочный конвейер завода. В результате произошел сбой в работе и был причинен материальный ущерб: 200 машин не сошло с конвейера (ущерб в 1 млн. рублей в ценах 1983 г.). Программист был привлечен к уголовной ответственности. В ходе судебного разбирательства судья и заседатели испытали немалые трудности, т.к. преступление не попадало ни под одну статью действующего уголовного законодательства. Однако приговор был все-таки вынесен: три года лишения свободы условно; взыскание суммы, выплаченной рабочим за время вынужденного простоя главного конвейера; перевод на должность сборщика.

Таблица 8 - Классификация групп хакеров

Возможности	Запуск задачи из фиксированного набора, реализующих заранее предусмотренные функции	Создание и запуск собственных программ с новыми функциями по обработке информации	Возможность управления функционированием ИС, т.е. воздействие на базовое ПО, на состав и конфигурац	Полное и всестороннее воздействие на средства ИС вплоть до включения в состав ИС своих средств и ПО

	по		ию ее	

	обработке		оборудования	
Начинающий хакер	+			
Освоивший основы работы на ПЭВМ и в составе сети	+	+		
Классный специалист	+	+	+	
Специалист высшего класса	+	+	+	+

Инициативный шпионаж непосредственно примыкает к двум вышеприведенным угрозам, исходящим от служащих, и может принести массу неприятностей компании.

Угроза, исходящая от организованных преступных группировок, основывается на том, что информация является основой мировой экономики, а, следовательно, криминальные элементы будут пытаться получить доступ к информационным ресурсам компаний, чтобы получить незаконные доходы.

Включение информационных систем фирм в международную сеть привлекают политических диссидентов. Их интересы состоят в распространении призывов к различным акциям, гражданскому неповиновению.

Участники террористических групп с помощью овладения информационными ресурсами и системами стараются придать своим акциям больше значения, запугать население, посеять панику.

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

Как свидетельствуют многочисленные опросы и приведенные свидетельства, в настоящее время многие руководители ведущих московских коммерческих

структур, все более глубоко осознают роль и место своих сотрудников в создании и поддержке общей системы безопасности. Такое понимание этой проблемы ведет к настойчивому внедрению процедур тщательного отбора и расстановки кадров. Так, постепенно приобретают все

более большую значимость рекомендательные письма, научные методы проверки на профпригодность и различного рода тестирования.

4 Основные принципы организации профессионального отбора персонала в учреждения и предприятия

Особенности психологических подходов к профотбору

Обычно процедура отбора кадров проводится по традиционно- формальным признакам: образование; разряд; стаж работы по специальности. На современных предприятиях при весьма ограниченной численности сотрудников, все более частом совмещении рядовыми исполнителями различных участков и стремительно увеличивающихся потоков информации и управленческих команд, каждый сотрудник во все возрастающей степени становится носителем конфиденциальных сведений, которые могут представлять интерес, как для конкурентов, так и для криминальных сообществ.

В таких условиях весьма существенно повышаются и изменяются требования к личным и деловым качествам сотрудников и, следовательно, к кандидатам на работу. Данное обстоятельство побуждает руководителей все чаще обращаться к методам и процедурам научной психологии, с помощью которых можно достаточно быстро, надежно и всесторонне оценивать возможного кандидата и составлять его психологический портрет. Психологический профотбор преследует следующие основные цели:

- выявление ранее имевших место судимостей, преступных связей, криминальных наклонностей;
- выявление предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков в случае формирования в его окружении определенных обстоятельств;
- установление фактов, свидетельствующих о морально- психологической надежности.

Функции организационных схем управления и профессиограмм

В настоящее время ведущие государственные и коммерческие структуры имеют строго разработанные и утвержденные руководством организационные структуры и функции управления для каждого подразделения. Наибольшей популярностью пользуются методики составления организационных схем или организационных чертежей, на которых графически изображается каждое рабочее место, прописываются должностные обязанности и определяются информационные потоки для отдельного исполнителя.

Кроме того, для большей конкретизации этих процедур на каждое рабочее место рекомендуется составлять профессиограмму, т.е. перечень личностных качеств, которыми в идеале должен обладать потенциальный сотрудник. Обязательными атрибутами подобных документов являются разделы, отражающие профессионально значимые качества (психические характеристики, свойства личности, без которых невозможно выполнение

основных функциональных обязанностей), а также противопоказания (личностные качества, которые делают невозможным зачисление кандидата на конкретную должность).

Проблемы дееспособности и работоспособности сотрудников

Проблема состоит в том, что отделу кадров трудно быстро оценить психическое состояние лиц, пришедших на собеседование. Этому способствует повышенное волнение, бесконтрольное самолечение психосоматических расстройств. В этом случае необходимо направлять кандидата в поликлиники. Такой подход позволяет достаточно быстро составить представление о состоянии здоровья будущего сотрудника и планировать его работу.

5 Основные рекомендации при организации проверки и отбора кандидатов на работу в организации и предприятия

Задачи службы безопасности

Сегодня представляется целесообразным вновь напомнить о том, что с точки зрения обеспечения стратегических интересов организации являются обязательными следующие функции службы безопасности:

- определение степени вероятности формирования у кандидата преступных наклонностей в случаях возникновения в его окружении определенных благоприятных обстоятельств (персональное распоряжение кредитно-финансовыми ресурсами, возможность контроля за движением наличных средств и ценных бумаг, доступ к материально-техническим ценностям, работа с конфиденциальной информацией и пр.);
- выявление имевших место ранее преступных наклонностей, судимостей, связей с криминальной средой (преступное прошлое, наличие конкретных судимостей, случаи афер, махинаций, мошенничества, хищений на предыдущем месте работы кандидата и установление, либо обоснованное суждение о его возможной причастности к этим преступным деяниям).

Комплексный подход к организации профотбора кадров

Для добывания подобной информации используются возможности различных подразделений организации, в первую очередь службы безопасности, отдела кадров, юридического отдела, подразделений медицинского обеспечения, а также некоторых сторонних организаций, например, детективных агентств, бюро по занятости населения, диспансеров и пр.

Для сбора сведений такого характера применяются в рамках Закона «О частной детективной и охранной деятельности в РФ» следующие методы: опрос, анкетирование, целевые беседы с лицами по месту жительства кандидатов и на предыдущих местах их учебы или работы, наведение справок через медицинские учреждения и пр.

Очевидно, также, что представители организации должны быть абсолютно уверены в том, что проводят тесты, собеседования и встречи именно с теми лицами, которые выступают в качестве кандидатов на работу. Это подразумевает тщательную проверку паспортных данных, иных

документов, а также получения фотографий кандидатов без очков, контактных линз, парика, макияжа. Необходимо требовать предоставления комплекта фотографий нескольких размеров (6х12, 4х6 и др).

Рекомендуется настаивать на получении набора цветных фотографий кандидата, которые могут быть использованы в случае необходимости для предъявления жильцам по месту его проживания или коллегам по работе. Использование в кадровой работе цветных фотографий, соответствующих паспортным данным, предпочтительнее также в связи с тем, что они четко и без искажений передают цвет волос, кожи, возраст и характерные приметы.

В практике уже известны случаи, когда для дополнительного анализа анкеты кандидата и его фотографий руководители организации приглашали высоко профессиональных юристов, графологов, известных психоаналитиков и даже экстрасенсов с целью обеспечения максимальной полноты формулировок окончательного заключения и выявления возможных скрытых противоречий в характере проверяемого лица.

В последние годы в ведущих московских коммерческих банках широко практикуется почерковедческая экспертиза, которая позволяет определить многие черты характера кандидата: темперамент, выдержку, волевые качества, собранность, аккуратность, грамотность, общеобразовательный уровень и пр., а также предрасположенность к совершению неблаговидных и нечестных поступков.

В том случае, если результаты работы проверок, тестов и психологического изучения не противоречат друг другу и не содержат данных, которые бы препятствовали приему на работу данного кандидата, с ним заключается трудовое соглашение, в большинстве случаев предусматривающие определенный испытательный срок (1-3 месяца).

Особенности проверки руководящих кадров

Лица, принимаемые на ответственные вакантные должности в организации (члены правлений, главные бухгалтеры, консультанты, начальники служб безопасности и охраны, руководители компьютерных центров и цехов, помощники и секретари первых лиц) сегодня подвергаются, как правило, следующей стандартной проверке, включающей:

- достаточно продолжительные процедуры сбора и верификации (проверка истинности теоретических положений, установление достоверности опытным путем) установочно-биографических сведений с их последующей аналитической обработкой;
- предоставление рекомендательных писем от известных государственных и предпринимательских структур с их последующей проверкой;
- проверки по учетам правоохранительных органов;
- установки по месту жительства и по предыдущим местам работы;
- серии собеседований и тестов с последующей психоаналитической обработкой результатов.

По мнению экспертов, даже каждый, взятый в отдельности из

упомянутых методов проверки достаточно эффективен. В совокупности же достигается весьма высокая степень достоверности информации о профессиональной пригодности и надежности кандидата, его способностях к творческой работе на конкретном участке в соответствующем коммерческом предприятии.

Методическая работа с персоналом

Несмотря на любую квалификацию пользователя, поскольку развитие информационного пространства предприятия не стоит на месте, необходимо регулярное обучение сотрудников как работе в новых информационных системах, так и мерам безопасности в этих системах. Кроме того, развитие злоумышленной части мирового информационного пространства может по- требовать от пользователей дополнительных более или менее квалифициро- ванных знаний по ряду атак (например, как в случае с известным вирусом IKourmkova — отличать расширения jpg от jpg.vbs). Это означает, что следует продумать систему оперативного оповещения сотрудников о необходимых мероприятиях, а также возможное проведение регулярных семинаров для всех или наиболее подготовленной части сотрудников. Для больших, распределенных корпораций желательно применять способ подготовки под- робных методических материалов, их рассылки и обязательного ознакомления сотрудников с ними.

Как бы старательно и качественно не работали сотрудники, периодически приходится проверять их деятельность. Проверки могут быть выборочными или регулярными, их диапазон может простираться от анализа регистрационных журналов данной конкретной информационной системы до полного сканирования содержимого жесткого диска и внешних носителей пользователя. При таких проверках, по всей видимости, будут периодически обнаруживаться какие-то нарушения в работе пользователей, в том числе и по их вине. Степень зависимости вины пользователя в том или ином нарушении и размер наказания должны определить уполномоченные лица конкретной организации.

Хотелось бы дать один совет: не всегда суровое наказание даже за маленький проступок — это хорошее решение проблемы. По опыту известно, что даже при информированности пользователей о том, что их деятельность - это предмет наблюдения соответствующих служб, значительная часть из них все равно будет пытаться искать мелкие выгоды для себя в процессе своей рабочей деятельности. Возможно, это будет посещение развлекательных сайтов в Интернете или установка компьютерных игр. В таких случаях на- поминание в виде электронного письма с примерным содержанием: «Вчера вы посетили сайт www.xxx.com и провели на нем 42 минуты рабочего времени. Рекомендуем вам во избежание неприятностей не посещать сайты, не связан- ные с вашей рабочей деятельностью. Служба безопасности» — будет хорошей профилактикой развития злоупотребления корпоративными ресурсами. Однако даже если данный незначительный инцидент формально "прощен", тем не менее, он должен быть зафиксирован в некоем "черном списке", куда вносятся все нарушения информационной безопасности пользователем с

первого дня работы. Такой документ полезен, во-первых, поскольку пользо- ватели склонны забывать о своих нарушениях (в этом случае данный документ будет полезен при некоем переполнении списка мелких нарушений, условно прощенных для этого пользователя). Во-вторых, с помощью данного документа можно отслеживать тенденции в развитии работы пользователя с точки зрения информационной безопасности.

Мелкой, но, тем не менее, важной деталью является вопрос идентификации работника при межличностном общении. В организации, насчитывающей несколько десятков человек, специалист по безопасности может знать каждого сотрудника лично, но в большой организации, где персонал составляет 1000 и более человек, вопросы распознавания личности, особенно для новых работников, станут уязвимостью, которая может быть использована, например, средствами социальной инженерии.

Ближайшим примером является обращение пользователя по телефону с просьбой замены пароля по той или иной причине. Каким образом проверить соответствие реального пользователя названному username? Если поль- зователь находится неподалеку, наиболее простой способ — пригласить его прибыть к администратору с документами, подтверждающими личность. Кстати, для этих целей хорошим корпоративным стандартом считается но- шение на груди опознавательного пропуска с необходимой информацией (желательно продумать вопросы воспрепятствования их подделке). Но что, если пользователь географически удален от администратора, а вопросы биз- неса требуют обеспечения немедленного начала работы в информационной системе? В этом случае вступает в действие система временных паролей для однократного входа (с немедленной заменой), для которой в Интернете на- работаны два основных варианта решения проблемы.

Контрольный вопрос. При регистрации в учетную запись пользователя, доступ к которому есть только у администратора, заносится вопрос и соответствующий ответ, которые известны только данному пользователю. Таким образом, перед сменой пароля администратор аутентифицирует пользователя по ответу на контрольный вопрос. Если система позволяет, следует сохранять несколько вопросов для одного пользователя, также следует заменять вопросы, после их использования.

Альтернативная обратная связь. После обращения пользователя админи- стратор фиксирует номер телефона и, проверив корректность номера, перезванивает пользователю сам. Кроме того, временный пароль высылается пользователю по электронной почте, возможно, даже не самому пользователю, а его непосредственному руководителю.

Следует только учесть важность того, чтобы временный пароль был достаточно уникальным, с тем, чтобы в каждый конкретный момент не было известно о том, какой временный пароль использован для данного работника.

6 Процесс увольнения кадров из организации

Серьезное влияние на вопросы безопасности государственных и коммерческих предприятий оказывают процедуры увольнения сотрудников. К сожалению, отдельных руководителей порой мало интересуют чувства и переживания персонала, который по тем или иным причинам попадает под сокращение или самостоятельно изъявляет желание покинуть банк или акционерное общество. Как показывает опыт, такой подход приводит, как правило, к серьезным негативным последствиям.

Психологические подходы к проблеме увольнения персонала

Другой важный момент — взаимоотношения с сотрудником, который собирается покинуть организацию. Естественно, должны быть проведены некоторые технические мероприятия по блокированию или удалению учетных записей данного сотрудника как пользователя информационных систем. Но для этого служба безопасности как минимум должна быть оповещена о предстоящем увольнении сотрудника. Также в этой ситуации необходим контакт с подразделением по работе с персоналом.

Для ряда увольняющихся сотрудников, а возможно и для всех, целесообразно проводить собеседования, в ходе которых напомнить о продолжении действия обязательств, взятых на себя сотрудником по отношению к организации (если заключенные контракты и договоренности не теряют своей силы при увольнении сотрудника).

Современные психологические подходы к процессу увольнения позволяют выработать следующую принципиальную рекомендацию: каковы бы ни были причины увольнения сотрудника, он должен покидать коммерческую организацию без чувства обиды, раздражения и мести.

Только в этом случае можно надеяться на то, что увольняемый сотрудник не предпримет необдуманных действий и не проинформирует правоохранительные органы, налоговую инспекцию, конкурентов, криминальные структуры об известных ему подлинных, а чаще всего мнимых недостатках, промахах, ошибках в деятельности его прежних руководителей.

Таким образом, представители кадровых подразделений и служб безопасности должны быть четко ориентированы на выяснение истинных мотивов увольнения всех категорий сотрудников. Зачастую причины, на которые ссылается сотрудник при увольнении, и подлинные мотивы, побудившие его к такому шагу, существенно отличаются друг от друга. Обычно ложный защитный мотив используется потому, что сотрудник в силу прежних привычек и традиций опасается неправильной интерпретации своих действий со стороны руководителей и коллег по работе.

Наряду с этим весьма часто имеют место случаи, когда сотрудник внутренне сам уверен в том, что увольняется по откровенно называемой им

причине, хотя его решение сформировано и принято под влиянием совершенно иных, порой скрытых от него обстоятельств. Так, в практике уже известны случаи тонких и тайных комбинаций оказания влияния на высококвалифицированных специалистов с целью их переманивания на другое место работы.

В этой связи принципиальная задача состоит в том, чтобы определить истинную причину увольнения сотрудника, попытаться правильно ее оценить и решить, целесообразно ли в данной ситуации предпринимать попытки к искусственному удержанию данного лица в коллективе либо отработать и реализовать процедуру его спокойного и бесконфликтного увольнения. Решение рекомендуется принимать на основе строго объективных данных в отношении каждого конкретного сотрудника.

Подготовка к беседе с увольняемыми сотрудниками

При поступлении устного или письменного заявления об увольнении рекомендуется во всех без исключения случаях провести с сотрудником беседу с участием представителей кадрового подразделения и кого-либо из руководителей организации. Однако до беседы целесообразно предпринять меры по сбору следующей информации об увольняемом сотруднике:

- характер его взаимоотношений с коллегами в коллективе;
- отношение к работе;
- уровень профессиональной подготовки;
- наличие конфликтов личного или служебного характера;
- ранее имевшие место высказывания или пожелания перейти на другое место работы;
- доступ к информации, в том числе составляющей коммерческую тайну;
- вероятный период устаревания сведений, составляющих коммерческую или служебную тайну для данного предприятия;
- предполагаемое в будущем местоработы увольняющегося (увольняемого) сотрудника.

Особенности проведения беседы

Беседа при увольнении проводится лишь только после того, когда собраны все необходимые сведения. Конечно, предварительно руководитель организации отрабатывает принципиальный подход к вопросу о том, целесообразно ли предпринимать попытки склонить сотрудника изменить его первоначальное решение либо санкционировать оформление его увольнения. В любом случае рекомендуется дать собеседнику высказаться и в развернутой форме объяснить мотивы своего решения. При выборе места проведения беседы предпочтение отдается, как правило, служебным помещениям.

В зависимости от предполагаемого результата беседа может проводиться в официальном тоне либо иметь форму доверительной беседы, задушевного разговора, обмене мнениями. Однако каковы бы ни были планы в отношении данного сотрудника, разговор с ним должен быть построен таким образом, чтобы последний ни в коей мере не испытывал чувства униженности, обиды, оскорбленного достоинства. Для этого следует сохранять тон беседы

предельно корректным, тактичным и доброжелательным, даже, несмотря на любые критические и несправедливые замечания, которые могут быть высказаны сотрудником в адрес коммерческой структуры и ее конкретных руководителей.

Проблемы защиты служебной и коммерческой тайны при увольнении персонала

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

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

Что касается лиц с темпераментом холерика, то с этой категорией сотрудников рекомендуется завершить беседу на официальной ноте. В ряде случаев объявление им принятого решения об увольнении вызывает бурную негативную реакцию, связанную с попытками спекулировать на своих истинных, а порой и мнимых профессиональных достоинствах. Поэтому с сотрудниками такого темперамента и склада характера целесообразно тщательно оговаривать и обуславливать в документах возможности наступления для них юридических последствий раскрытия коммерческой тайны.

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

Кроме того, таких лиц традиционно стремятся сохранить в структуре банка или фирмы (их дочерних предприятий, филиалов) до тех пор, пока не будут приняты меры к снижению возможного ущерба от разглашения ими сведений, составляющих коммерческую тайну, либо найдены адекватные средства защиты конфиденциальных данных (технические, административные, патентные, юридические, финансовые и пр.).

Только лишь после реализации этих мер рекомендуется приглашать на собеседование подлежащего увольнению сотрудника и объявлять конкретные причины, по которым коммерческая организация отказывается от его услуг. Желательно при этом, чтобы эти причины содержали элементы объективности, достоверности и проверяемости (перепрофилирование

производства, сокращение персонала, ухудшение финансового положения, отсутствие заказчиков и пр.). При мотивации увольнения целесообразно, как правило, воздержаться от ссылок на негативные деловые и личные качества данного сотрудника.

СОХРАНЕНИЕ ПСИХОЛОГИЧЕСКОГО КОНТАКТА С УВОЛЬНЯЕМЫМИ СОТРУДНИКАМИ

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

Если подходить не предвзято и объективно к подобной критике, то эти соображения могут быть использованы в дальнейшем весьма эффективно в интересах фирмы или банка. В ряде случаев увольняемому сотруднику вполне серьезно предлагают даже изложить письменно свои рекомендации, конечно, за соответствующее вознаграждение.

Кроме того, такая беседа позволяет выработать решение о целесообразности предоставления увольняемому лицу каких-либо рекомендательных документов для последующего трудоустройства на новом месте работы. Следует категорически избегать каких-либо намеков о сведении личных счетов с увольняемым кандидатом за его прежние недостатки в работе и поведении.

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

В любом случае после увольнения сотрудников, осведомленных о сведениях, составляющих коммерческую тайну, целесообразно через возможности службы безопасности банка или фирмы (частного детективного агентства) проводить оперативную установку по их новому месту работы и моделировать возможности утечки конфиденциальных данных.

Кроме того, в наиболее острых и конфликтных ситуациях увольнения персонала проводятся оперативные и профилактические мероприятия по новому месту работы, жительства, также в окружении носителей коммерческих секретов.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

1 *Лукичева Л. И.* Управление персоналом. — М.: Омега-Л, 2007.

2 *Маслоу А. Г.* Мотивация и личность / пер. с англ. А.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM-

совместимых персональных ЭВМ с использованием программного комплекса «Гарант».

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив методики, применяющиеся в корпоративной практике тестирования персонала, сформулировать и письменно ответить на Задания для контроля владения компетенциями данной Практического занятия.

Техника безопасности

Для выполнения Практического занятия студент должен:

1 Ознакомиться с методикой и порядком выполнения работы.

2 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.

3 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

- работать без соответствующего освещения и вентиляции рабочего места;
- работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;
- передвигаться по аудитории без разрешения преподавателя;
- работать в специализированных аудиториях без сменной обуви;
- работать на одном рабочем месте более двух человек.

4 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.

5 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы

Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов

Не требуется

Порядок оформления отчета по практическому занятию и его защиты

Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на Задания для контроля владения компетенциями работы.

Рекомендации для преподавателей по проведению занятия

К защите требуется отчет с подробными ответами на вопросы к ПЗ.

Задания для контроля владения компетенциями:

1 Что такое метапрограммы?
2 Залог успешности руководителя.
3 Почему в нашей стране граждан рефлективного типа гораздо больше, чем активного?
4 Где (указать должности) достигнут лучших результатов активные и рефлективные граждане?
5 Характеристика внутренниреферентных, внешнереферентных и ориентированных на контекст людей.
6 Какая система оплаты лучше работает для людей с мотивацией избегания и с мотивацией достижения?
7 Приведите примеры должностей, на которых работник должен быть клиентоориентированным и ориентированным на себя.
8 Охарактеризовать отечественную и зарубежную школы тестирования.
9 Опишите функциональные и психологические тесты. 10 Четыре группы психологических тестов.
11 Представить конспект беседы (интервью) начальника службы безопасности (руководителя предприятия) с принимаемым на работу сотрудником (не менее 15 вопросов).
12 Виды угроз.
13 На чем основана угроза, исходящая от организованных преступных группировок?
14 Что привлекает политических диссидентов?
15 Действия участников террористических групп?
16 Что является наиболее целесообразным в целях обеспечения информационной безопасности коммерческих структур?
17 Почему в настоящее время на современных предприятиях каждый сотрудник во все возрастающей степени становится носителем конфиденциальных сведений?
18 Какие цели преследует психологический профотбор?
19 Что такое организационные структуры и функции управления для каждого подразделения?
20 Что такое профессиограмма? 21 Функции службы безопасности.
22 Возможности каких подразделений организации используются для добывания информации о профпригодности сотрудника?

23 Какие методы при этом используются?
24 К чему прибегают руководители организации для дополнительного анализа анкеты кандидата и его фотографий?
25 Какой проверке подвергаются лица, принимаемые на ответственные вакантные должности в организации?
26 Какие меры по сбору информации об увольняемом сотруднике следует предпринять до беседы?
27 Нужна ли беседа руководителя с увольняемым?
28 В какой атмосфере должна протекать беседа и в каких помещениях? 29 Как максимально защитить коммерческую тайну при увольнении
человека, принявшего решение самостоятельно, и человека, от услуг которого решила избавиться фирма?
30 Чего следует избегать руководству при увольнении сотрудника?

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 25.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 25
Исследование юридической ответственности

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 7,5 часов
Вступительная часть 2 мин
Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Учебная и воспитательная цели:

Изучить основы теории юридической ответственности. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

1 Общие положения.
2 Правовосстановительная ответственность.
3 Дисциплинарная и административная ответственность.
4 Уголовная ответственность.

Краткие теоретические или справочно-информационные материалы

1 Общие положения

Юридической ответственностью называется применение к лицу, совершившему правонарушение, мер государственного принуждения, предусмотренных санкцией нарушенной нормы, в установленном для этого процессуальном порядке.
Общей целью применения юридической ответственности является

охрана правопорядка. Эта цель в зависимости от характера правонарушений и их последствий достигается либо принудительным восстановлением нарушенных прав и пресечением противоправных состояний, либо наказанием правонарушителя, либо сочетанием того и другого.

Основанием ответственности является правонарушение (дей- ствительное или предполагаемое), которое характеризуется четырьмя элементами, образующими состав правонарушения:

- объект — нарушенное материальное или нематериальное благо, защищаемое правом;
- субъект — дееспособное лицо, совершившее правонарушение;
- объективная сторона — само противоправное деяние, насту- пивший вредоносный результат и причинная связь между деянием и результатом;
- субъективная сторона — вина, т.е. отношение правонарушителя к деянию и его результату в форме умысла или неосторожности.

Юридическая ответственность может быть возложена на лицо лишь при установлении всех элементов состава правонарушения. Это требование является обязательным при возложении дисциплинарной, административной и уголовной ответственности. По гражданским правонарушениям правонарушитель при определенных обстоятельствах может нести ответственность и без вины.

При применении к лицу мер государственного принуждения карательного характера (в административном и уголовном праве) действует принцип презумпции невиновности, т.е. предположение, в соответствии с которым даже при наличии фактов, свидетельствующих в доказанности объективной стороны, лицо считается невиновным, пока в предусмотренном законом порядке не будет доказана и установлена судом его вина. При этом бремя доказывания лежит на компетентных государственных органах — органах следствия, прокуратуре, осуществляющих обвинение.

Ответственность всегда конкретна: это ответственность определенного лица за доказуемое нарушение точно обозначенной нормы права при обстоятельствах, заранее предусмотренных законом или другими нормативными актами.

Правонарушение не причиняет урона и ущерба нормам закона, которые продолжают действовать и считаются обязательными; оно вредно или опасно для общества, стабильности общественных отношений, конкретных прав и охраняемых законом интересов.

Правонарушение представляет собой конкретный факт, юридическое определение (квалификация) которого содержится в законе. То же и правовое принуждение: оно может применяться лишь к конкретным лицам (субъектам права) за точно определенные Нарушения в той сфере, где люди общаются между собой, вступают в отношения.

Применение юридической ответственности осуществляется на основе нормативных конструкций, представляющих единство норм материального и процессуального права.

Признаки правонарушения и санкции за его совершение предусмотрены нормами материального права; порядок доказывания, определения того, было или не было правонарушение и кто его (совершил, а также назначение конкретной меры государственного принуждения в пределах санкции нарушенной нормы строго регламентированы нормами процессуального права.

Основные виды юридической ответственности предопределяются содержанием санкций, которые применяются за правонарушения.

Санкции делятся на два основных вида в соответствии со способом, каким они служат охране правопорядка:

- правовосстановительные санкции, которые направлены:
  a) на устранение непосредственного вреда, причиненного правопорядку;
  b) восстановление нарушенных прав;
  c) принудительное выполнение обязанностей;
  d) устранение противоправных состояний;
- штрафные, карательные санкции, которые имеют целью воздействие на правонарушителя в целях общей и частной превентивности правонарушений (дисциплинарные, административные и уголовно-правовые санкции).

Поскольку выраженный в санкции способ охраны правопорядка предопределяет порядок ее применения и реализации, соответственно и основным делением видов ответственности является деление на правовосстановительную и штрафную. Для правовосстановительной ответственности существенно точное определение уже существующих обязанностей правонарушителя и в случае необходимости их принудительное осуществление. Для штрафной, карательной ответственности — правильная квалификация правонарушения, индивидуализация наказания или взыскания, реализация примененных к правонарушителю мер принуждения, освобождение его от ответственности, когда ее цели достигнуты. К штрафной, карательной ответственности, сообразно видам правонарушений и санкций за их совершение, относятся уголовная, административная и дисциплинарная ответственность.

В процессе применения юридической ответственности могут применяться предусмотренные законодательством принудительные меры, обеспечивающие производство по делу о правонарушении — меры обеспечения доказательств (обыски, выемки и др.) или исполнения решения (опись имущества, его изъятие и др.), а также меры пресечения (отстранение от работы, задержание, содержание под стражей и др.). Эти принудительные меры носят вспомогательный характер: их применение зависит от тяжести правонарушения, но не содержит его итоговой правовой оценки (их применением не исчерпывается и не решается вопрос об ответственности за правонарушение); при применении санкции они поглощаются назначенным наказанием, взысканием, принудительным исполнением.

При юридической ответственности нарушитель претерпевает меры

государственного принуждения за свою вину и несет известные лишения, урон.

2 Правовосстановительная ответственность

Правовосстановительная ответственность, как правило, применяется при нарушении правовых норм, регулирующих гражданские отношения, и заключается в восстановлении незаконно нарушенных прав, в принудительном исполнении невыполненной обязанности. Основным источником права в этой области является Гражданский кодекс Российской Федерации.

Особенность этого вида ответственности состоит в том, что в ряде случаев правонарушитель может без вмешательства государственных органов выполнить свои обязанности, восстановить нарушенные права, прекратить противоправное состояние. На этом основаны дополнительные санкции, применяемые к правонарушителю в процессе реализации данных отношений ответственности (пени, штрафы, другие меры понуждения).

Так, в соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, которая составляет коммерческую тайну, обязаны возместить причиненные убытки Такая же обязанность возлагается на работников, разгласивших коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие другие нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. Гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший эти сведения не докажет, что они соответствуют действительности. Кроме того, он вправе наряду с опровержением требовать возмещения убытков и морального вреда, причиненного распространением таких сведений.

Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, распространены в средствах массовой информации, то они должны быть опровергнуты в тех же средствах массовой информации.

Правовосстановительная ответственность возникает с момента правонарушения и завершается восстановлением (в установленных законом пределах) нарушенного правопорядка. Процессуальные нормы регулируют осуществление этого вида ответственности в случае спора (в суде, в арбитраже) или отказа правонарушителя восстановить нарушенный правопорядок (исполнительное производство).

3 Дисциплинарная и административная ответственность

Дисциплинарная ответственность применяется за нарушение трудовой, учебной, служебной, воинской дисциплины. Рабочие и служащие,

нарушившие трудовую дисциплину, привлекаются к дисциплинарной ответственности администрацией предприятия, учреждения, организации. До наложения взыскания должны быть потребованы объяснения от нарушителя трудовой дисциплины. Законодательством определен порядок обжалования дисциплинарного взыскания, сроки его применения и действия, порядок досрочного снятия. Определенную специфику имеет дисциплинарная ответственность работников гражданской авиации, железнодорожного транспорта, военнослужащих по уставам о дисциплине, а также дисциплинарная ответственность судей и некоторых других категорий должностных лиц, дела о проступках которых рассматриваются и решаются специальными дисциплинарными коллегиями.

Административная ответственность осуществляется на основе законодательства об административных правонарушениях. Это законодательство состоит из Кодекса Российской Федерации об административных правонарушениях.

Основными задачами законодательства об административных правонарушениях являются защита личности, охрана прав и свобод человека и гражданина, охрана здоровья граждан, санитарно- эпидемиологического благополучия населения, защита общественной нравственности, охрана окружающей среды, установленного порядка осуществления государственной власти, общественного порядка и общественной безопасности, собственности, защита законных интересов физических и юридических лиц, общества и государства от административных правонарушений, а также их предупреждение.

Административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое Кодексом Российской Федерации об административных правонарушениях установлена административная ответственность.

Административная ответственность проявляется в форме ад- министративного наказания. Установлены следующие виды адми- нистративных наказаний: предупреждение; административный штраф; возмездное изъятие орудия совершения или предмета административного правонарушения; конфискация орудия совершения или предмета административного правонарушения; лишение специального права, предоставленного физическому лицу: административный арест; административное выдворение за пределы Российской Федерации иностранного гражданина или лица без гражданства; дисквалификация.

Законодательство об административных правонарушениях закрепляет значительное количество правонарушений в области информационной безопасности, за совершение которых к виновным лицам должна применяться административная ответственность.

Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от трех до пяти

минимальных размеров оплаты труда; на должностных лиц — от пяти до десяти минимальных размеров оплаты труда; на юридических лиц — от пятидесяти до ста минимальных размеров оплаты труда.

Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, влечет наложение административного штрафа на должностных лиц в размере от тридцати до сорока минимальных размеров оплаты труда с конфискацией несертифицированных средств, предназначенных для зашиты информации, составляющей государственную тайну, или без таковой.

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц — от сорока до пятидесяти минимальных размеров оплаты труда.

Производство по делу начинается с составления протокола об административном правонарушении. В предусмотренных законом случаях к лицу, привлеченному к административной ответственности, могут применяться меры обеспечения производства по делу: административное задержание лица, личный досмотр, досмотр вещей и изъятие вещей и документов. Дела об административных нарушениях рассматриваются народными судами, народными судьями, органами внутренних дел, органами государственных инспекций и другими государственными органами и должностными лицами, уполномоченными на то законодательными актами. Дело рассматривается открыто, в присутствии лица, привлекаемого к административной ответственности. Привлеченный к ответственности вправе знакомиться с материалами дела, давать объяснения, представлять доказательства, заявлять ходатайства, пользоваться юридической помощью адвоката, обжаловать постановление по делу; он также имеет ряд других прав. Законодательством определены сроки привлечения к административной ответственности и исполнения наложенных взысканий.

4 Уголовная ответственность

Уголовная ответственность применяется за преступления и включает самые строгие меры государственного принуждения. Порядок ее осуществления регламентирован наиболее детально и определяется уголовным, уголовно-процессуальным и уголовно- исполнительным законодательством. Ряд принципов уголовной ответственности закреплен в международных пактах и в конституционном законодательстве.

Уголовное законодательство составляет Уголовный кодекс Российской Федерации. Задачами уголовного законодательства являются охрана прав и свобод

человека и гражданина, собственности, общественного порядка и общественной безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечение мира и безопасности человечества, а также предупреждение преступлений.

Преступлением признается виновно совершенное общественно опасное деяние, запрещенное Уголовным кодексом Российской федерации под угрозой наказания.

Не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного кодексом, но в силу малозначительности не представляющее общественной опасности.

В зависимости от характера и степени общественной опасности деяния, предусмотренные Уголовным кодексом, подразделяются за преступления небольшой тяжести, средней тяжести, тяжкие и особо тяжкие.

Физическое лицо подлежит уголовной ответственности только за те общественно опасные действия (бездействие) и наступившие общественно опасные последствия, в отношении которых установлена его вина.

Наказание и иные меры уголовно-правового характера, применимые к лицу, совершившему преступление, должны быть справедливыми, т.е. соответствовать характеру и степени общественной опасности преступления, обстоятельствам его совершения, личности виновного.

Виновным в преступлении признается лицо, совершившее деяние умышленно или по неосторожности. Деяние, совершенное по неосторожности, признается преступлением лишь в том случае, когда это специально предусмотрено соответствующей статьей Уголовного кодекса.

Уголовная ответственность проявляется в форме наказания. Наказание есть мера государственного принуждения, назначаемого по приговору суда. Наказание применяется к лицу, признанному виновным в совершении преступления, и заключается в предусмотренных Уголовным кодексом лишении или ограничении прав и свобод этого лица. Оно применяется в целях восстания социальной справедливости, а также в целях исправления осужденного и предупреждения совершения новых преступлений.

Методами наказаний являются:

- штраф;
- лишение права занимать определенные должности или заниматься определенной деятельностью;
- лишение специального, воинского или почетного звания, классного чина и государственных наград;
- обязательные исправительные работы;
- ограничение по военной службе;
- лишение свободы;
- арест; содержание в дисциплинарной воинской части;
- лишение свободы на определенный срок;
- пожизненное лишение свободы;
- смертная казнь.

В уголовном законодательстве содержится значительное количество общественно опасных деяний в информационной сфере. Часть этих деяний связана со сферой компьютерной информации, которая в рамках данного раздела представляет наибольший интерес.

К числу этих деяний относятся следующие.

Неправомерный доступ к охраняемой законом компьютерной ин- формации, т.е. информации на машинном носителе, в электронно- вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом в размере до 200 тыс. р. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, наказывается штрафом в размере от 100 тыс. до 300 тыс. р. или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказываются лишением свободы на срок до трех лет со штрафом в размере до 200 тыс. р. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от 180 до 240 ч, либо ограничением свободы на срок до двух лет.

То же деяние, повлекшее по неосторожности тяжкие последствия, наказывается лишением свободы на срок до четырех лет.

Привлечению определенного лица к уголовной ответственности в качестве обвиняемого обычно предшествует возбуждение уголовного дела по факту преступления, сбор и исследование относящихся к этому делу

доказательств. С момента привлечения к уголовной ответственности обвиняемый имеет право на защиту. Уголовно-процессуальным законодательством определены права и обязанности обвиняемого, подозреваемого и других участников процесса, а также правомочия должностных лиц и государственных органов, ведающих производством по делу, порядок сбора и исследования доказательств, применения в случае необходимости принудительных мер (мер пресечения, обысков, выемок, при- водов и др.). Решающей стадией уголовной ответственности является рассмотрение дела в судебном заседании. Никто не может быть признан виновным в совершении преступления, а также подвергнут уголовному наказанию иначе как по приговору суда и в соответствии с законом. Каждый осужденный за уголовное преступление имеет право на пересмотр приговора вышестоящей судебной инстанцией в порядке, установленном законом, а также право просить о помиловании или смягчении наказания.

Отношения уголовной ответственности завершаются отбытием наказания, назначенного осужденному.

Отчетность за занятие

1 Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.
2 Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

1 ***Безлепкин Б. Т.*** Судебная система, правоохранительные органы и адвокатура России. — М.: Юристъ, 2001.
2 *Дмитриев Ю.А.* Правоохранительные органы / Ю.А.Дмитриев, М. А. Шап- кин. — М.: Мастерство, 2002.
3 Федеральныйконституционный закон «О судебной системе Российской Федерации» от 31 декабря 1996 г.
4 Федеральныйконституционный закон «О военных судах Российской Федерации» от 23 июня 1999 г.
5 Федеральный конституционный закон «Об арбитражных судах в Российской Федерации» от 28 апреля 1995 г.
6 Федеральный закон «О мировых судьях в Российской Федерации» от 17 декабря 1998 г.
7 Федеральныйзакон «О третейских судах в Российской Федерации» от 24 июля 2002 г.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности

Для выполнения практического занятия студент должен:

1 Ознакомиться с методикой и порядком выполнения работы.

2 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.

3 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

- работать без соответствующего освещения и вентиляции рабочего места;
- работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;
- передвигаться по аудитории без разрешения преподавателя;
- работать в специализированных аудиториях без сменной обуви;
- работать на одном рабочем месте более двух человек.

4 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.

5 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы

Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов

Не требуется

Порядок оформления отчета по практическому занятию и его защиты

Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на вопросы для контроля владения

компетенциями работы.

Рекомендации для преподавателей по проведению занятия

К защите требуется отчет с подробными ответами на вопросы.

Задания для контроля владения компетенциями:

1 В чем заключается применение юридической ответственности? Раскройте ее сущность и признаки.
2 В чем заключается правоприменительная ответственность?
3 В чем заключается дисциплинарная и административная ответственность?
4 В чем заключается уголовная ответственность?

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 26.
ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 26
Организация защиты прав

1. Цель занятия

1. Изучить на практике виды матричных операций.

2. Подготовка к занятию

1. Изучить (повторить) теоретический материал.
2. Ознакомиться с заданием на практическое занятие.

3. Распределение времени занятия:

Всего: 7,5 часов
Вступительная часть 2 мин
Проверка готовности студентов к занятию 5 мин

Программа практического занятия

1. Повторение теоретического материала 35 мин
2. Выполнение практического задания 35 мин Проверка выполнения практического занятия 10 мин Заключительная часть 3 мин

Учебная и воспитательная цели:

Изучить теорию организации защиты прав. Прививать студентам навыки исследовательского подхода к изучению дисциплины. Воспитывать у студентов сознательное отношение к процессу обучения

Вопросы, подлежащие исследованию:

1 Суды общей юрисдикции, арбитражные суды и третейские суды.
2 Процедура обращения в суд за судебной защитой.

Краткие теоретические или справочно-информационные материалы

1 Суды общей юрисдикции, арбитражные суды и третейские суды

Одним из наиболее важных способов защиты прав и законных интересов субъектов информационной сферы является судебное разбирательство, осуществляемое в рамках деятельности судебной власти.

Судебная власть представляет собой самостоятельную и независимую составляющую государственной власти, действующую наряду с

законодательной и исполнительной властями.

Судебная система Российской Федерации образуется совокупностью федеральных судов, конституционных (уставных) судов и мировых судей субъектов Российской Федерации

К федеральным судам относятся:

- Конституционный Суд Российской Федерации;
- суды общей юрисдикции — Верховный Суд Российской Фе- дерации, верховные суды республик, краевые и областные суды, суды городов федерального значения, суды автономной области и автономных округов, районные суды, военные и специализированные суды, составляющие систему федеральных судов обшей юрисдикции;
- арбитражные суды — Высший Арбитражный Суд Российской Федерации, федеральные арбитражные суды округов (арбитражные кассационные суды), арбитражные апелляционные суды, арбитражные суды субъектов Российской Федерации, составляющие систему федеральных арбитражных судов.

К судам субъектов Российской Федерации относятся:

- конституционные (уставные) суды субъектов Российской Фе- дерации,
- мировые судьи, являющиеся судьями общей юрисдикции субъектов Российской Федерации.

Конституционный Суд Российской Федерации является судебным органом конституционного контроля, самостоятельно и независимо осуществляющим судебную власть посредством конституционного судопроизводства.

Верховный Суд Российской Федерации является высшим судебным органом по гражданским, уголовным, административным и иным делам, подсудным судам общей юрисдикции. Он осуществляет в предусмотренных федеральным законом процессуальных формах судебный надзор за деятельностью судов общей юрисдикции, включая военные и специализированные федеральные суды. В пределах своей компетенции Верховный Суд Российской Федерации рассматривает дела в качестве суда второй инстанции, в порядке надзора и по вновь открывшимся обстоятельствам, а в случаях, предусмотренных федеральным законом, также и в качестве суда первой инстанции.

Верховный Суд Российской Федерации является непосредственно вышестоящей судебной инстанцией по отношению к верховным судам республик, краевым (областным) судам, судам городов федерального значения, судам автономной области и автономных округов, военным судам военных округов, флотов, видов и групп войск. Он уполномочен давать разъяснения по вопросам судебной практики.

Верховный суд республики, краевой (областной) суд, суд города фе- дерального значения, суд автономной области, суд автономного округа в пределах своей компетенции рассматривают дела в качестве суда первой и

второй инстанции, в порядке надзора и по вновь открывшимся обстоятельствам. Эти суды являются непосредственно вышестоящими судебными инстанциями по отношению к районным судам, действующим на территории соответствующего субъекта Российской Федерации.

Районный суд в пределах своей компетенции рассматривает дела в качестве суда первой и второй инстанции и осуществляет другие полномочия, предусмотренные федеральным конституционным законом. Районный суд является непосредственно вышестоящей судебной инстанцией по отношению к мировым судьям, действующим на территории соответствующего судебного района.

Военные суды создаются по территориальному принципу по месту дислокации войск и флотов и осуществляют судебную власть в войсках, органах и формированиях, где федеральным законом предусмотрена военная служба. В пределах своей компетенции военные суды рассматривают дела в качестве суда первой и второй инстанции, в порядке надзора и по вновь открывшимся обстоятельствам.

Высший Арбитражный Суд Российской Федерации является высшим судебным органом по разрешению экономических споров и 'иных дел, рассматриваемых арбитражными судами. Он является вышестоящей судебной инстанцией по отношению к федеральным арбитражным судам округов, арбитражным апелляционным "судам и арбитражным судам субъектов Российской Федерации.

Высший Арбитражный Суд Российской Федерации осуществляет в предусмотренных федеральным законом процессуальных формах судебный надзор за деятельностью арбитражных судов, рассматривает в соответствии с федеральным законом дела в качестве суда первой инстанции, в порядке надзора и по вновь открывшимся обстоятельствам.

Высший Арбитражный Суд Российской Федерации уполномочен давать разъяснения по вопросам судебной практики.

Федеральный арбитражный суд округа в пределах своей компетенции рассматривает дела в качестве суда кассационной инстанции, а также по вновь открывшимся обстоятельствам. Он является вышестоящей судебной инстанцией по отношению к действующим на территории соответствующего судебного округа арбитражным апелляционным судам и арбитражным судам субъектов Российской Федерации.

Арбитражный апелляционный суд в пределах своей компетенции рассматривает дела в качестве суда апелляционной инстанции, а также по вновь открывшимся обстоятельствам.

Арбитражный суд субъекта Российской Федерации в пределах своей компетенции рассматривает дела в качестве суда первой инстанции, а также по вновь открывшимся обстоятельствам.

Специализированные федеральные суды по рассмотрению гражданских и административных дел учреждаются путем внесения изменений и дополнений в настоящий Федеральный конституционный закон.

Конституционный (уставный) суд субъекта Российской Федерации

может создаваться субъектом Российской Федерации для рассмотрения вопросов соответствия законов субъекта Российской Федерации, нормативных правовых актов органов государственной власти субъекта Российской Федерации, органов местного самоуправления субъекта Российской Федерации конституции (уставу) субъекта Российской Федерации, а также для толкования конституции (устава) субъекта Российской Федерации. Конституционный (уставный) суд субъекта Российской Федерации рассматривает отнесенные к его компетенции вопросы в порядке, установленном законом субъекта Российской Федерации. Решение, принятое им в пределах установленных полномочий, не может быть пересмотрено иным судом.

Мировой судья в пределах своей компетенции рассматривает гражданские, административные и уголовные дела в качестве суда первой инстанции.

Суд представляет собой государственный орган, осуществляющий правосудие в форме рассмотрения и разрешения уголовных, гражданских, административных и некоторых иных категорий дел в установленном законодательством процессуальном порядке.

Суды осуществляют судебную власть самостоятельно, независимо от чьей бы то ни было воли, подчиняясь только Конституции Российской Федерации и закону.

Судьи, присяжные, народные и арбитражные заседатели, участвующие в осуществлении правосудия, независимы и подчиняются только Конституции Российской Федерации и закону. Гарантии их независимости устанавливаются Конституцией Российской Федерации и федеральным законом.

Защиту прав и законных интересов граждан и организаций можно осуществлять в третейских судах, если существует соглашение сторон о передаче дела в третейский суд. Соглашение заключается в письменной форме. Стороны, передавая спор на рассмотрение третейского суда, принимают обязательство подчиниться решению последнего. Третейские суды не входят в судебную систему. Деятельность третейских судов регулируется законом «О третейских судах в Российской Федерации» от 21 июня 2002 г., а также отдельными положениями гражданского и арбитражного процессуального законодательства.

Действующие в качестве негосударственного механизма разрешения споров, третейские суды, по сравнению с судами арбитражными, предоставляют участникам спора ряд преимуществ, таких, как специализация в вопросах, касающихся фактических взаимоотношений сторон, быстрота и экономичность, отсутствие публичности в деятельности, удобство для сторон в отношении времени и места разрешения споров и т.д.

В Российской Федерации могут образовываться постоянно дей- ствующие третейские суды и третейские суды для разрешения конкретного спора (разовые).

По процессуальной компетенции суды подразделяются на суды первой инстанции, суды второй (кассационной) инстанции и суды надзорной

инстанции.
Судебной инстанцией считается суд (или его структурное под- разделение), выполняющий ту или иную судебную функцию, связанную с разрешением судебных дел (принятие решения по существу дела, проверка законности и обоснованности этих решений).
Суд первой инстанции — это разбирательство дела по существу с целью осуждения или оправдания подсудимого — по уголовному делу; с целью удовлетворения иска или отказа в иске — по гражданскому делу. Дела по первой инстанции могут рассматривать все суды в пределах своей компетенции, но основное количество уголовных и гражданских дел по первой инстанции рассматривают районные суды. Наиболее сложные или особого общественного значения судебные дела рассматривают по существу вышестоящие суды вплоть до Верховного Суда Российской Федерации.
Решения и приговоры большинства судов в течение установленного законом срока (7 дней для приговора, 10 дней для решения) не вступают в законную силу и могут быть обжалованы в кассационном порядке подсудимым, потерпевшим, истцом или ответчиком либо опротестованы прокурором в суд второй инстанции.
Суд второй инстанции — это суды апелляционной и кассационной инстанций. Для мировых судей и районных судов — областной и соответствующие ему суды, а для областного суда — Верховный Суд Российской Федерации. Прокуратура на основании жалоб заинтересованных лиц или кассационного протеста прокурора проверяет законность и обоснованность решений суда первой инстанции, не вступивших в законную силу.
По итогам кассационного разбирательства дела суд второй инстанции выносит определение, которое вступает в законную силу немедленно и не подлежит ни обжалованию, ни опротестованию в кассационном порядке. Оно может быть опротестовано лишь в порядке судебного надзора.
Суд надзорной инстанции по протестам лиц, указанных в законе, проверяет законность и обоснованность вступивших в законную силу решений суда первой инстанции, а также решений суда кассационной инстанции либо нижестоящей надзорной инстанции.
Судебные акты надзорных инстанций (постановления президиумов или определения коллегий) вступают в законную силу немедленно.
Подсудность дел — это распределение между судами дел, подлежащих слушанию по первой инстанции, т.е. установление конкретного суда, который должен разрешить данное дело. В судебном процессе различают два основных вида подсудности: родовую (предметную) и территориальную (местную). Родовая подсудность относит дело к ведению того или иного звена судебной системы — в зависимости от вида преступления и характера гражданского дела. Территориальная подсудность разграничивает компетенцию между судами одного и того же звена.
Верховные суды республик, краевые, областные, городские суды городов федерального значения Москвы и Санкт-Петербурга, автономной

области, автономного округа в настоящее время, в частности, рассматривают и разрешают по первой инстанции дела, связанные с нарушением законодательства о государственной тайне.

Все гражданские дела, с точки зрения их родовой подсудности, делятся на дела подсудные по первой инстанции: мировым судьям; районным судам; верховным судам республики, областным, краевым судам, городским судам городов Москвы и Санкт-Пе- тербурга, суду автономной области, судам автономных округов; Верховному Суду Российской Федерации.

Общее правило территориальной подсудности гражданских дел (общая территориальная подсудность) заключается в том, что иск предъявляется в суд по месту жительства ответчика. Иск к организации предъявляется по месту нахождения организации (ее имущества, а также филиала или представительства).

Альтернативная подсудность по выбору истца (заявителя) означает, что дело подсудно не только суду по месту нахождения ответчика, но и другому суду, указанному в законе. Согласно закону, когда дело подсудно нескольким судам одного уровня, выбор суда для рассмотрения и разрешения дела принадлежит истцу (заявителю) (ст. 29 ГПК РФ).

Договорная подсудность означает, что стороны по соглашению между собой могут изменять общую и альтернативную территориальную подсудность для данного дела.

Исключительная подсудность устанавливает правила, которые исключают применение других видов территориальной подсудности, в частности, общей территориальной, альтернативной, договорной и по связи требований (дел).

В арбитражном процессе общее положение родовой (предметной) подсудности выражено в формуле: все дела, подведомственные арбитражным судам, подсудны судам субъектов Российской Федерации, за исключением дел, подсудных исключительно Высшему Арбитражному Суду РФ.

В территориальной подсудности прежде всего различают общую территориальную подсудность, согласно которой иски предъявляются в арбитражный суд по месту нахождения или месту жительства ответчика.

Подсудность уголовных дел характеризуют следующие признаки:

- предметный (родовой) признак подсудности определяется родом (видом) преступления, составляющего предмет производства по уголовному делу, т.е. в конечном счете квалификацией преступления по статье Уголовного кодекса РФ (с помощью родового признака подсудности устанавливается, суд какого звена судебной системы компетентен рассматривать данное дело);
- территориальный (местный) признак определяет подсудность уголовных дел в зависимости от места совершения преступления.

2 Процедура обращения в суд за судебной защитой

Для обращения в суд, прежде всего, необходимо определить, в какой суд обращаться, в порядке какого судопроизводства.

Основная задача гражданского судопроизводства — защита на- рушенных или оспариваемых прав, свобод и охраняемых законом интересов граждан, организаций и их объединений, а также охрана государственных и общественных интересов.

В Гражданском процессуальном кодексе выделены четыре вида Гражданского судопроизводства:

- исковое производство;
- приказное производство;
- производство по делам, вытекающим из публичных правоотношений;
- особое производство.

Исковое производство существует при обращении в суд за защитой нарушенных прав или интересов. По общему правилу исковое производство возникает при наличии спора.

Приказное производство предусматривает упрощенную процедуру по выдаче судебного приказа.

В производстве по делам, возникающим из публичных правоотношений, рассматриваются дела по жалобам на действия административных и государственных органов, общественных организаций, должностных лиц, нарушающих права и свободы граждан.

Особое производство не связано с разрешением спора о праве, здесь нет спорящих сторон. К особому производству отнесены дела установления фактов, имеющих юридическое значение.

Возбуждение дел искового производства происходит путем подачи искового заявления. Что касается неисковых производств, то эти дела возбуждаются в суде путем подачи заявления или жалобы.

Соблюдение надлежащей формы искового заявления — важное условие соблюдения процедуры обращения в суд.

Исковое заявление подается обязательно в письменной форме и должно содержать следующие сведения:

- наименование суда, в который подается заявление;
- наименование истца, его место жительства или, если истцом является организация, ее место нахождения, а также наименование представителя и его адрес, если заявление подается представителем;
- наименование ответчика, его место жительства или, если от- ветчиком является организация, ее место нахождения; в чем заключается нарушение либо угроза нарушения прав, свобод или законных интересов истца и его требования;
- обстоятельства, на которых истец основывает свои требования, и доказательства, подтверждающие эти обстоятельства;
- цена иска, если он подлежит оценке, а также расчет взыскиваемых или оспариваемых денежных сумм;
- сведения о соблюдении досудебного порядка обращения к ответчику, если это установлено федеральным законом или предусмотрено

договором сторон;

перечень прилагаемых к заявлению документов.

В заявлении могут быть указаны и иные сведения, в том числе номера телефонов, факсов, адреса электронной почты, если они необходимы для правильного и своевременного рассмотрения дела.

Наряду с тем, что в исковом заявлении должны содержаться сведения, общие для всех категорий дел, имеется определенная специфика в его содержании, обусловленная целым рядом обстоятельств. Содержание искового заявления по отдельным категориям гражданских дел определяется, исходя из характера спорного материального правоотношения, субъектного состава и ряда других обстоятельств, имеющих существенное значение для правильного разрешения дела.

Важное значение имеет указание в исковом заявлении того материально- правового требования истца к ответчику, которое составляет предмет иска. В заявлении необходимо указать, в чем заключаются нарушение или угроза нарушения прав, свобод или охраняемых законом интересов истца и его требования. Характер искового требования определяется характером спорного материального правоотношения, из которого вытекает требование истца. Просьба истца, реализованная в виде этого требования, и составляет просительный пункт искового заявления.

Цена иска, указываемая в исковом заявлении, должна быть определена в соответствии с законодательством. В исковом заявлении должна быть указана цена иска, если он подлежит оценке, а также расчет взыскиваемых денежных сумм. Кроме того, в исковом заявлении должны содержаться сведения о соблюдении досудебного порядка обращения к ответчику, когда это установлено законом или предусмотрено договором сторон.

Исковое заявление должно содержать указание на прилагаемые письменные доказательства (документы) и быть подписано истцом или его представителем при наличии у него полномочий на подписание заявления и предъявление его в суд.

К исковому заявлению должны быть обязательно приложены до- кументы, перечень которых утвержден гражданско-процессуальным законодательством. Особо следует обратить внимание на то, что среди них должны содержаться документы, подтверждающие обстоятельства, на которых истец основывает свое требование, копии этих документов для ответчиков и третьих лиц, а также доказательство, подтверждающее выполнение обязательного досудебного порядка разрешения спора, если такой порядок предусмотрен законом или договором. Также необходимо приложить документ, подтверждающий расчет взыскиваемой или оспариваемой суммы, который должен быть подписан истцом или его представителем с приложением копий по числу ответчиков и третьих лиц.

В соответствии с законом исковое заявление представляется в суд вместе с копиями по числу ответчиков. Документы, прилагаемые к исковому заявлению, их перечень определяются, как правило, характером дела, подлежащего рассмотрению в суде, и зависят от того материально-правового

требования, которое истец предъявляет к ответчику.

Судья принимает исковое заявление к производству суда только в том случае, если имеются для этого основания, предусмотренные законом. Принятие искового заявления может последовать только при наличии как предпосылок права на предъявление иска, так и условий, образующих порядок предъявления иска.

Отказ судьи в принятии искового заявления может последовать только по основаниям, указанным в законе, перечень которых является исчерпывающим и не подлежит расширительному толкованию.

При обращении в арбитражный суд основным процессуальным документом, без которого не может быть возбуждено дело, является исковое заявление, а по делам, возникающим из административных и иных публичных отношений, и по делам, рассматриваемым в порядке особого производства, — заявление.

Документ, исходящий от истца (заявителя), должен отвечать определенным требованиям. Требования, прежде всего, касаются формы и содержания заявления.

Исковое заявление подается в арбитражный суд в письменном виде и должно быть подписано истцом или его представителем.

Содержание искового заявления включает сведения, которые позволяют установить:

- какому арбитражному суду адресуется заявление;
- от кого оно исходит и к кому предъявляется иск (с подробными данными о сторонах и месте их нахождения);
- в чем заключаются исковые требования;
- какова законодательная база, на которой строятся заявленные требования;
- что входит в круг фактических обстоятельств, лежащих в основе предъявленного иска;
- какими доказательствами подтверждается существование этих обстоятельств.

В заявлении также приводится расчет взыскиваемой или оспариваемой денежной суммы, если это входит в предмет иска, указывается цена иска, если иск подлежит оценке. В случае, если федеральным законом или договором предусмотрен претензионный или иной досудебный порядок разрешения данного спора, приводятся сведения о соблюдении этого порядка.

Неотъемлемым атрибутом искового заявления является определенный состав документов, которые прилагаются к исковому заявлению. В перечень этих документов входят:

- уведомление о вручении или иные документы, подтверждающие направление другим лицам, участвующим в деле;
- копии искового заявления и приложенных к нему документов, которые у других лиц, участвующих в деле, отсутствуют;
- документы, подтверждающие уплату государственной пошлины в

установленном порядке и размере или право на получение льгот по уплате государственной пошлины, либо ходатайство о предоставлении отсрочки, рассрочки, об уменьшении размера государственной пошлины;

- документы, подтверждающие обстоятельства, на которых истец основывает свои требования;
- копии свидетельства о государственной регистрации в качестве юридического лица или индивидуального предпринимателя;
- доверенность или иные документы, подтверждающие полномочия на подписание искового заявления;
- копии определения арбитражного суда об обеспечении иму- щественных интересов до предъявления иска;
- документы, подтверждающие соблюдение истцом претензионного или иного досудебного порядка, если он предусмотрен федеральным законом или договором;
- проект договора, если заявлено требование о понуждении заключить договор.

Закон предоставляет лицам, участвующим в деле, возможность направить в арбитражный суд отзыв на исковое заявление, в котором, в случае возражения против иска, указываются мотивы полного или частичного несогласия с требованиями истца, законодательство, а также доказательства, обосновывающие возражения. Отзыв может содержать и иные сведения, а также имеющиеся ходатайства.

Исковое заявление, подаваемое в третейский суд заинтересованным лицом, составляется в письменной форме. Оно должно содержать дату, наименование и реквизиты сторон, обоснование компетенции третейского суда, требование и обстоятельства, на которых истец основывает свое требование, подтверждающие их доказательства, цену иска (если иск подлежит оценке), перечень прилагаемых к заявлению документов и иных материалов.

Копии заявления и других приобщенных к нему документов передаются ответчику, который в срок, определенный правилами третейского разбирательства, либо до первого заседания третейского суда (если этот срок правила не содержат), вправе представить истцу и в суд отзыв на исковое заявление, изложив в нем свою позицию.

В уголовном процессе первой стадией является возбуждение уголовного дела. В уголовном законодательстве предусмотрены следующие поводы к возбуждению Уголовного дела:

- заявление о преступлении;
- явка с повинной;
- сообщение о совершенном или готовящемся преступлении, полученное из иных источников;
- наличие достаточных данных, указывающих на признаки пре- ступления.

По результатам рассмотрения сообщения о преступлении орган

дознания, дознаватель, следователь или прокурор принимает одно из следующих решений: о возбуждении уголовного дела; об отказе в возбуждении уголовного дела; о передаче сообщения по подследственности, а по уголовным делам частного обвинения — в суд.

О принятом решении сообщается заявителю. При этом ему разъясняется право и порядок обжалования данного решения.

Необходимо отметить, что расследование преступлений в сфере обеспечения информационной безопасности более сложное, нежели других видов преступлений и требует от соответствующих должностных лиц специальной технической и юридической подготовки.

Отчетность за занятие

1 Каждый студент должен оформить в отдельной тетради и защитить работу у преподавателя.
2 Ответить на вопросы для самоконтроля.

Рекомендации студентам по подготовке к практическому занятию с указанием литературы

1 Конституция Российской Федерации от 12 декабря 1993 года.
2 *Стрельцов А.А.* Правовое обеспечение информационной безопасности России. Теоретические и методологические основы. — Минск: Белл1тфонд, 2004.
3 *Туманова Л. В.*. Обеспечение и защита права на информацию / Л. В.Туманова, А.А.Снытников. — М.: Городец, 2001.
4 *Фатьянов А.А.* Правовое обеспечение безопасности информации в Российской Федерации. — М.: Юрист, 2001.
5 *Фисун А.П.* Право и информационная безопасность / А. П.Фисун [и др.]. — М.: Приор, 2005.

Описание экспериментальных установок (лабораторного оборудования)

Практическое занятие проводится в компьютерном классе на IBM- совместимых персональных ЭВМ.

Краткое содержание работы, выполняемой студентами в ходе занятия. Порядок проведения эксперимента, постановки опыта, снятия замеров и обработки данных эксперимента

Изучив теорию и методические указания к проведению ПЗ, сформулировать и письменно ответить на вопросы для контроля владения компетенциями данного практического занятия.

Техника безопасности

Для выполнения практического занятия студент должен:

1 Ознакомиться с методикой и порядком выполнения работы.

2 Перед включением ЭВМ подготовить рабочее место, убрать ненужные для работы предметы; обо всех замеченных технических неисправностях сообщить преподавателю. Запрещается включать устройства при неисправных заземлении или кабелях питания; пользоваться поврежденными розетками, рубильниками и другими электроустановочными приборами.

3 После получения разрешения преподавателя включить ЭВМ и приступить к работе. Во время работы запрещается производить любые действия, связанные с включением или выключением ЭВМ, а также подключением или отключением различных периферийных устройств. Запрещается:

- работать без соответствующего освещения и вентиляции рабочего места;
- работать, если при прикосновении к корпусам оборудования ощущается действие электрического тока;
- передвигаться по аудитории без разрешения преподавателя;
- работать в специализированных аудиториях без сменной обуви;
- работать на одном рабочем месте более двух человек.

4 После выполнения задания и получения разрешения преподавателя закрыть активные приложения, корректно завершить работу ЭВМ и отключить питание.

5 Привести в порядок рабочее место, и после получения разрешения преподавателя покинуть помещение.

Исходные данные для работы

Методические рекомендации для проведения практического занятия.

Методика анализа полученных результатов

Не требуется

Порядок оформления отчета по практическому занятию и его защиты

Отчет по результатам выполнения практического занятия оформляется в тетради и должен содержать ответы на вопросы для контроля владения компетенциями работы.

Рекомендации для преподавателей по проведению занятия

К защите требуется отчет с подробными ответами на вопросы.

Задания для контроля владения компетенциями:

1 Перечислите основные разновидности судебных органов.

2 В чем заключается компетенция судов?

3 Раскройте содержание понятия «подсудность дел».

4 Раскройте основное содержание процедуры обращения в суд.

Содержание отчета о практическом задании

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Основной литературы:

1 Корнеев, И.К. Защита информации в офисе: учебник/ И. К. Корнеев, Е. А. Степанов- М.: ТК Велби, 2018.

2. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие/ В. Ф. Шаньгин- М.: ИНФРА-М, 2019.

Дополнительная литература:

1. Садердинов, А.А. Информационная безопасность предприятия [Текст]: учеб.пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. - 4-е изд. - М.: ИТК "Дашков и К", 2012.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие/ В. Ф. Шаньгин- М.: ФОРУМ, 2012.

Методическая литература:

1. Методические указания по выполнению практических работ по дисциплине «Организационное и правовое обеспечение информационной безопасности ».
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Организационное и правовое обеспечение информационной безопасности ».

Интернет-ресурсы:

1. www.intuit.ru – национальный открытый университет «ИНТУИТ»;
2. www.window.edu.ru –единое окно доступа к образовательным ресурсам;
3. www.citforum.ru – сервер информационных технологий.
4. http://biblioclub.ru
5. http://elibrary.ru/

Программное обеспечение:

1	Альт Рабочая станция 10
2	Альт Рабочая станция К
3	Альт «Сервер»
4	Пакет офисных программ - Р7-Офис

Материально-техническое обеспечение

1. Лабораторные и практические занятия проводятся в компьютерных классах, в которых установлено вышеперечисленное программное обеспечение.

2. Лекционный курс проводится в аудиториях, оснащенных проектором.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы
по дисциплине **«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2025

СОДЕРЖАНИЕ

1. Общие положения 234

2.Цель и задачи самостоятельной работы 235

3.Технологическая карта самостоятельной работы студента 235

4.Порядок выполнения самостоятельной работы студентом 235

4.1. Методические рекомендации по работе с учебной литературой 236

4.2. Методические рекомендации по подготовке к практическим занятиям 237

4.3. Методические рекомендации по самопроверке знаний 238

4.4. Методические рекомендации по написанию научных текстов (докладов, рефератов, эссе, научных статей и т.д.) 238

4.5. Методические рекомендации по подготовке к зачетам 263

Список литературы для выполнения СРС 264

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- написание докладов;
- подготовка к семинарам, практическим и лабораторным работам, их оформление;
- составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
- выполнение учебно-исследовательских работ, проектная деятельность;
- подготовка практических разработок и рекомендаций по решению проблемной ситуации;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;
- компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;
- выполнение курсовых работ (проектов) в рамках дисциплин;
- выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

2.Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование универсальных компетенций.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3.Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
6 семестр					
ОПК-5(ИД-1 ИД-2 ИД-3) ОПК-6, (ИД-1 ИД-2 ИД-3) ОПК-1.1, (ИД-1 ИД-2 ИД-3)	Самостоятельное изучение литературы	Собеседование	24,84	2,76	27,6
ОПК-5(ИД-1 ИД-2 ИД-3) ОПК-6, (ИД-1 ИД-2 ИД-3) ОПК-1.1, (ИД-1 ИД-2 ИД-3)	Подготовка к практическим занятиям	Собеседование	5,76	0,64	6,4
ОПК-5(ИД-1 ИД-2 ИД-3) ОПК-6, (ИД-1 ИД-2 ИД-3) ОПК-1.1, (ИД-1 ИД-2 ИД-3)	Подготовка доклада	Доклад	9	1	10
		Итого за 6 семестр	39,6	4,4	44

7 семестр					
ОПК-5(ИД-1 ИД-2 ИД-3) ОПК-6, (ИД-1 ИД-2 ИД-3) ОПК-1.1, (ИД-1 ИД-2 ИД-3)	Самостоятельное изучение литературы	Собеседование	0,72	0,08	0,8
ОПК-5(ИД-1 ИД-2 ИД-3) ОПК-6, (ИД-1 ИД-2 ИД-3) ОПК-1.1, (ИД-1 ИД-2 ИД-3)	Подготовка к практическим занятиям	Собеседование	6,48	0,72	7,2
ОПК-5(ИД-1 ИД-2 ИД-3) ОПК-6, (ИД-1 ИД-2 ИД-3) ОПК-1.1, (ИД-1 ИД-2 ИД-3)	Подготовка доклада	Доклад	9	1	10
Итого за 7 семестр			16,2	1,8	18
Итого			55,8	6,2	62

4.Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист

помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.
2. Выделите главное, составьте план.
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим занятиям

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных

занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение отвечать на вопросы для собеседования.

Вопросы для собеседования

Базовый уровень:

Вопросы для проверки уровня обученности

Знать:

1. Основные термины и определения в области правовой защитыинформации.
2. Информация как объект правовых отношений. Обладатель информации.
3. Система права и место в ней информационного права.
4. Структура и состав информационного законодательства.
5. Структура правоотношений и виды юридической ответственности.
6. Общедоступная информация и информация с ограниченным доступом.
7. Классификация информации по ее доступности.
8. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
9. Защита права на доступ к информации.
10. Ограничение права на доступ к информации.
11. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
12. Система нормативно-правовых документов в области защите государственной тайны.
13. Закон Российской Федерации «О государственной тайне» (преамбула дополнена с 9 октября 1997 года Федеральным законом от 6 октября 1997 года N 131-ФЗ).
14. Полномочия органов государственной власти и должностных лиц в области

отнесения сведений к государственной тайне.

15. Основные понятия в области защиты государственной тайны.
16. Система перечней сведений, составляющих государственную тайну.
17. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
18. Принципы отнесения сведений к государственной тайне.
19. Грифы секретности носителей информации, составляющей государственную тайну.
20. Порядок засекречивания сведений, составляющих государственную тайну и их носителей.
21. Реквизиты носителей сведений, составляющих государственнуютайну.
22. Порядок рассекречивания сведений, составляющих государственную тайну и их носителей.
23. Права собственника информации, составляющей государственнуютайну.
24. Допуск должностных лиц и граждан к государственной тайне.
25. Основания для отказа в допуске к государственной тайне.
26. Ограничение прав должностных лиц и граждан, допущенных кгосударственной тайне.
27. Особый порядок допуска должностных лиц и граждан к государственной тайне.
28. Условия прекращения допуска к государственной тайне.
29. Организация доступа должностных лиц или граждан к государственной тайне.
30. Понятие и виды ответственности за нарушение законодательства в области защиты государственной тайны.
31. Понятие административной ответственности за нарушение законодательства в области защиты государственной тайны.
32. Понятие уголовной ответственности за нарушение законодательства в области защиты государственной тайны.
33. Дисциплинарная ответственность за нарушение в области защиты государственной тайны.
34. Органы защиты государственной тайны.
35. Лицензирование деятельности юридических лиц в области защиты государственной тайны.
36. Порядок сертификации средств защиты информации.
37. Государственная политика в сфере информатизации.
38. Структура органов информационного законодательства РФ.
39. Понятие служебной тайны в российском законодательстве. Объектыи субъекты права на служебную тайну.
40. Нормативно-правовая база в области защиты служебной тайны.
41. Сведения, относящиеся и не относящиеся к служебной тайне.
42. Федеральный закон Российской Федерации от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне».
43. Законодательные и иные нормативно-правовые акты, регулирующие защиту коммерческой тайны. Объекты и субъекты права на коммерческую тайну.
44. Постановление Правительства РФ от 5.12.1991 г. №35 «О перечне сведений, которые не могут составлять коммерческую тайну».
45. Рекомендации по отнесению сведений к коммерческой тайне. Режим коммерческой тайны.
46. Основные права и обязанности собственника коммерческой тайны.
47. Юридический статус информации «ноу-хау», в режиме коммерческой тайны
48. Система защиты коммерческой тайны.
49. Защита коммерческой тайны в трудовых и гражданско-правовыхотношениях.

50. Понятие профессиональной тайны в российском законодательстве. бъекты и субъекты права на профессиональную тайну.

51. Ответственность за разглашение или незаконное использование профессиональной тайны.

52. Источники, объекты и субъекты права на профессиональную тайну.

53. Особенности врачебной (медицинской) тайны и ее правовая защита. Основы законодательства РФ об охране здоровья граждан от 22.07.1993 г.

54. Закон Российской Федерации «О психиатрической помощи и гарантиях прав граждан при ее оказании» от 02.07.1992 г.

55. Закон Российской Федерации «О трансплантации органов и (или) тканей человека» от 22.12.1992 г.

56. Особенности нотариальной тайны и ее правовая защита.

57. «Основы законодательства РФ о нотариате» от 10.02.1993 г.

58. Закон Российской Федерации «О банках и банковской деятельности»от 3.02 1996 г.

59. Банковская тайна и ее правовая защита.

60. Законодательные и иные нормативно-правовые акты, регулирующие защиту информации персонального характера.

61. Федеральный закон Российской Федерации от 27 июля 2006 № 152- ФЗ «О персональных данных», структура и содержание.

62. Права субъектов и обязанности операторов в процессе обработки, передачи, хранения и использования персональных данных.

63. Обработка персональных данных работников и их защита в организации и на предприятии.

64. Ответственность, предусмотренная российским законодательством в области защиты информации персонального характера.

65. Международное законодательство в области защиты информации персонального характера.

66. Интеллектуальная собственность как объект правовой защиты.

67. Особенности защиты информации и интеллектуальной собственности в сети Интернет.

68. Понятие и структура интеллектуальной собственности.

69. ГК РФ, ч. 4, раздел 6 «Права на результаты интеллектуальной деятельности и средства индивидуализации».

70. ГК РФ, ч. 4, раздел 6, глава 70 «Авторское право».

71. ГК РФ, ч. 4, раздел 6, глава 72 «Патентное право».

72. ГК РФ, ч. 4, раздел 6, глава 74 «Право на топологии интегральныхмикросхем».

73. ГК РФ, ч. 4, раздел 6, глава 75 «Право на секрет производства (ноу-хау)».

74. ГК РФ, ч. 4, раздел 6, глава 76 «Права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий».

75. ГК РФ, ч. 4, раздел 6, глава 77 «Право использования результатов интеллектуальной деятельности в составе единой технологии».

76. Бернская конвенция по охране литературных и художественных произведений (Берн, 9 сентября 1886 года).

77. Всемирная конференция об авторском праве (Женева, 6 сентября1952 г.)

78. Лиссабонское соглашение о защите указаний места происхожденияизделий и их международной регистрации от 31 октября 1958 г.

79. Ниццское Соглашение о Международной классификации товаров и услуг для регистрации знаков (Ницца, 15 июня 1957).

80. Договор о законах по товарным знакам (Женева, 27 октября 1994).

Повышенный уровень:

Знать:

1. Страсбургское соглашение о Международной патентной классификации от 24 марта 1971 г.
2. Лиссабонское соглашение о защите указаний места происхожденияизделий и их международной регистрации от 31 октября 1958 г.
3. Закон Российской Федерации «О предприятиях и предпринимательской деятельности» от 12.06.1990 г.
4. Источники, объекты и субъекты права защиты против недобросовестной конкуренции.
5. Правовая охрана права на защиту против недобросовестной конкуренции.

6. Виды «вредной» информации деструктивно воздействующей на человека.
7. Понятие информационно-психологической безопасности иособенности ее обеспечения.
8. Государственная система обеспечения информационно-психологической безопасности.
9. Особенности правовой охраны прав на информационные системы.
10. Понятие информационной безопасности РФ. Нормативно-правовые акты в области информационной безопасности.
11. Источники права о сохранении единого информационногопространства.
12. Понятие и признаки информационного общества.
13. Понятие, признаки, структура и потенциальные угрозы дляРоссийской Федерации.
14. Нормативно-правовые акты в области информационнойбезопасности.
15. Понятие «организационные методы защиты информации».
16. Перечень и содержание организационных мер, направленных на защиту ГТ.
17. Документальное оформление допуска граждан РФ к государственной тайне.
18. Физические мероприятия по обеспечения защиты информации.
19. Технические мероприятия по защите информации.
20. Служба безопасности предприятия: назначение, структура.

1.1 Комплект тестовых заданий

Базовый уровень

Вопрос 1

Организованная совокупность специальных органов, средств, методов, обеспечивающих защиту информации от внутренних и внешних угроз – это:
-: модель защиты информации
+: система защиты информации
-: организация
-: подразделение защиты

Вопрос 2

Свойствами защиты информации являются:
-: непрерывность
-: целенаправленность
-: универсальность
+: все вышеперечисленное

Вопрос 3

Что не входит в виды собственного обеспечения системы защиты информации?
-: организационное обеспечение
-: информационное обеспечение
+: физическое обеспечение
-: правовое обеспечение

Вопрос 4

Компонентами концептуальной модели безопасности информации являются:
-: объекты угроз

-: цели угроз со стороны злоумышленников
-: способы защиты информации
+: все вышеперечисленное

Вопрос 5

Потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями – это:

+: угрозы конфиденциальной информации
-: мировые угрозы
-: компьютерные преступления
-: личные угрозы

Вопрос 6

Что представляет из себя система?

-: совокупность элементов, формирующих определенную функцию системы по реализации поставленных целей
+: совокупность взаимосвязанных элементов, объединенных единством цели и функциональной целостностью
-: совокупность взаимосвязанных структурных элементов с устойчивыми межэлементными связями
-: верного ответа нет

Вопрос 7

Основной признак понятия системы:

+: целостность
-: интегрированность
-: относительная обособленность системы от окружающей среды
-: непрерывность

Вопрос 8

Чем характеризуются сложные системы?

+: размерностью системы
-: наличием неисправного состояния
+: свойством устойчивости
-: все вышеперечисленное

Вопрос 9

Основные типы связей элементов сложных систем:

+: структурные
+: функциональные
-: линейные
+: пространственно-временные

Вопрос 10

Источниками внешних угроз не являются:

-: отдельные лица и организации административно-управленческого аппарата
+: разведка иностранцев
-: преступные группировки и формирования
-: недобросовестные конкуренты

Вопрос 11

Формами защиты информации являются:

-: товарные знаки
-: авторское право
-: патентование
+: всё вышеперечисленное

Вопрос 12

Не являющиеся государственными секретами сведения, связанные с производством, технологией, управлением, финансами, разглашение, утечка и несанкционированный доступ к которым может нанести ущерб их

владельцам – это:

+: коммерческая тайна

-: конфиденциальные сведения

-: служебная тайна

-: тайна следствия

Вопрос 13

К коммерческой тайне относятся:

-: охраняемые государством сведения

+: сведения о производстве

-: общедоступные сведения, патенты, товарные знаки

-: сведения о негативной стороне деятельности

Вопрос 14

Какие этапы включает жизненный цикл управления организационно-экономической системы?

+: планирование

+: координация

-: регистрация

+: контроль

Вопрос 15

Какие этапы включает жизненный цикл информационной системы?

-: планирование

+: регистрация

-: координация

+: передача и обработка

Вопрос 16

Совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации – это:

-: правовая защита

-: организационная защита

+: инженерно-техническая защита

-: программная защита

Вопрос 17

Важнейшими принципами обеспечения безопасности информационных систем на предприятиях являются:

-: законность мероприятий по выявлению и предотвращению правонарушений в информационной сфере

-: непрерывность совершенствования средств защиты информационной системы

-: экономическая целесообразность, то есть сопоставимость возможного ущерба и затрат на обеспечение безопасности информации

+: все вышеперечисленное

Вопрос 18

Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Назовите тип этого злонамеренного кода:

-: макровирус

-: троянский конь

+: червь

-: файловый вирус

Вопрос 19

Предметом правового регулирования в информационной среде являются:

+: создание и распространение информации

+: формирование информационных ресурсов

-: установление запрета на использование открытых каналов связи для передачи конфиденциальной информации

+: реализация прав граждан на поиск, получения, передачу и потребление информации

Вопрос 20

Нормативными актами, регулирующими отношения в информационной сфере, являются:

-: Конституция Российской Федерации

-: Закон “Об информации информатизации и защиты информации”

-: Постановление правительства Российской Федерации

+: все вышеперечисленное

Вопрос 21

В каком федеральном законе определены основные направления государственной политики в сфере информатизации?

-: "О федеральной службе безопасности"

+: "Об информации, информатизации и защите информации"

-: "О коммерческой тайне"

-: "О лицензировании отдельных видов деятельности"

Вопрос 22

В реализации государственной политики в сфере информатизации участвуют следующие структуры власти:

-: Президент Российской Федерации

-: Советы безопасности Российской Федерации

-: Органы местного самоуправления

+: Все вышеперечисленное

Вопрос 23

Структуру аппарата системы безопасности Российской Федерации составляют:

+: Межведомственная комиссия Совета безопасности Российской Федерации по информационной безопасности

-: Комитет по информационной политике и связи

+: Управление информационной безопасности и стратегического прогнозирования

-: Комитет по безопасности, составной частью которого является комитет по информационной безопасности

Вопрос 24

В состав информационного законодательства Российской Федерации не входит:

-: Концепция развития рынка телекоммуникационного оборудования РФ

-: Закон Российской Федерации “О коммерческой тайне”

-: Доктрина информационной безопасности Российской Федерации

+: Закон Российской Федерации "Об авторском праве и смежных правах"

Вопрос 25

Организационно-распорядительные документы по защите государственной тайны разделяются на:

-: результаты научно-исследовательских работ, касающиеся защиты государственной тайны

+: положения по защите государственной тайны

+: концепции по защите государственной тайны

-: все вышеперечисленное

Вопрос 26

Межведомственная комиссия при осуществлении своей деятельности не должна:

-: координировать работы по организации сертификации средств защиты информации

-: подготавливать предложения и экспертные заключения в вопросах, касающихся государственной тайны

-: формировать перечень сведений, отнесенных к государственной тайне

+: разрабатывать целевые программ обеспечения информационной безопасности Российской Федерации

Вопрос 27

Предметом правового регулирования в информационной среде являются:

+: создание и распространение информации

+: формирование информационных ресурсов

-: установление запрета на использование открытых каналов связи для передачи конфиденциальной информации

+: реализация прав граждан на поиск, получения, передачу и потребление информации

Вопрос 28

Метод «Троянский конь» состоит в:

-: несанкционированном проникновении, как в пространственные, так и в электронные закрытые зоны

-: использовании ошибки или неудачи в логике построения программы

+: в тайном введении в чужую программу команд, которые позволяют осуществлять не планировавшиеся программные функции, сохраняя прежнюю работоспособность

-: использовании злоумышленником необходимых средств для проникновения в компьютерную систему, выдавая себя за законногопользователя

Вопрос 29

Организационные методы защиты информации предусматривают

формирование и обеспечение функционирования следующих механизмов защиты:

+: стандартизации методов и средств защиты информации

-: организация специального делопроизводства для конфиденциальной информации

-: установление запрета на использование открытых каналов связи для передачи конфиденциальной информации

+: страхования информационных рисков, связанных с функционированием компьютерных систем и сетей

Вопрос 30

Доктрина Информационной Безопасности РФ служит основой для:

-: принятия уголовно-правовых норм, устанавливающих уголовную ответственность за совершение компьютерных преступлений

+: развития Концепции национальной безопасности Российской Федерации применительно к информационной сфере

+: формирования государственной политики в области обеспечения информационной безопасности Российской Федерации

-: страхования информационных рисков, связанных с функционированием компьютерных систем и сетей

Вопрос 31

Государственными органами, ответственными за организацию и проведение специальных экспертиз предприятий, являются:

-: Федеральное агентство правительственной связи и информации при президенте РФ

+: Федеральная служба безопасности РФ

-: Государственная техническая комиссия при президенте РФ

+: Федеральная служба по техническому и экспортному контролю России

Вопрос 32

Участниками сертификации средств защиты информации не являются:

-: Федеральный орган по сертификации

-: Центральный орган системы сертификации

-: Испытательные лаборатории

+: Все вышеперечисленные являются

Вопрос 33

Что подразумевается под уголовно-правовыми мерами борьбы с компьютерными преступлениями?

-: разработка и создание новых, более совершенных законов в сфере уголовной ответственности за совершение компьютерных преступлений

-: тотальный контроль над использованием компьютерной техники

+: принятие уголовно-правовых норм, устанавливающих уголовную ответственность за совершение компьютерных преступлений

-: усиление мер безопасности против возможных злоупотреблений ЭВМ

Вопрос 34

Что входит в направления борьбы с компьютерными правонарушениями?

+: усиление мер безопасности против возможных злоупотреблений ЭВМ

-: создание специального отдела сотрудников

-: введение новых должностей

-: всё вышеперечисленное

Вопрос 35

Какой путь решения проблемы правового регулирования является традиционным для отечественного законодательства?

+: принятие отдельных институтов норм права, объединенных объектом преступного посягательства

-: принятие общих институтов норм права, объединенных объектом преступного посягательства

-: оба являются традиционными для отечественного законодательства

-: верного ответа нет

Вопрос 36

В какой печати впервые появился термин «компьютерная преступность» (60е годы)?

-: в греческой

-: в российской

+: в американской

-: в европейской

Вопрос 37

Какие общественно опасные деяния относятся к компьютерным преступлениям?

-: с использованием средств массовой информации

-: с использованием всех знаний, полученных человечеством

-: с использованием взрывчатых средств

+: с использованием средств компьютерной техники в отношении информации, обрабатываемой в компьютерной системе

Вопрос 38

Что относится к видам противоправных деяний, входящих в состав компьютерных преступлений?

-: шантаж, информационная блокада и другие методы компьютерного давления

-: подделка и фальсификация компьютерной информации

-: хищение системного и прикладного программного обеспечения

+: всё вышеперечисленное

Вопрос 39

Какие методы перехвата информации включают в себя компьютерные преступления?

-: конфиденциальный

-: неофициальный

+: видеоперехват

-: официальный

Вопрос 40

Что такое логическая бомба?

-: пластиковый контейнер, начиненный взрывчатым веществом

+: тайно встраиваемый в программу набор команд, срабатываемый лишь однажды при неких условиях

-: бомба, принцип действия которой направлен на физическое уничтожение компьютерной техники

-: бомба, принцип действия которой направлен на физическое уничтожение программиста

Вопрос 41

На какие группы делятся преступления, связанные с использованием информационных технологий?

-: преступления против информационной безопасности

-: преступления, где электронная информация является орудием или средством совершения другого преступления

-: преступления, совершаемые с использованием компьютерной или другой электронной техники

+: все вышеперечисленные

Вопрос 42

Что понимается под уничтожением информации?

+: утрата с невозможностью дальнейшего использования

-: передача другому лицу

-: присвоение информации статуса общедоступности

-: отправка документов в архив

Вопрос 43

Что понимается под модификацией информации?

-: изменение носителя информации

-: уничтожение информации

-: присвоение информации грифа конфиденциальности

+: изменение содержания информации по сравнению с первоначальным

Вопрос 44

Какие лица могут быть субъектами преступлений?

+: физические вменяемые лица, достигшие 16 лет

-: физические невменяемые лица, достигшие 16 лет

-: физические вменяемые лица, достигшие 13 лет

-: физические невменяемые лица, достигшие 13 лет

Вопрос 45

Что не является методом несанкционированного доступа и перехвата?

-: «неспешный выбор»

-: «маскарад»

+: «копейка плюс»

-: «поиск бреши»

Вопрос 46

Что не включает в себя понятие «компьютерный саботаж»?

-: выведение из стоя и разрушение аппаратной части

-: стирание и фальсификация данных

+: забастовка программистов

-: запугивание и шантаж обслуживающего персонала с целью прекращения ими работы

Вопрос 47

Что не входит в общую классификацию компьютерных преступлений?

+: физические компьютерные преступления

-: экономические компьютерные преступления

-: компьютерные преступления, связанные с нарушением личных прав

-: компьютерные преступления против частных интересов

Вопрос 48

Что в трасологии понимается под отображением морфологических особенностей внешнего строения объекта, имеющего устойчивые

пространственные границы, образующиеся в результате взаимодействия, сопряженного с событием преступления?

-: вид

+: след

-: раса

-: вес

Вопрос 49

Остаточные явления, представляющие собой материально фиксированные отображения на одном объекте относительно внешнего строения другого однотипного объекта – это:

-: следы-находки

-: следы-вещества

-: следы-предметы

+: следы-отображения

Вопрос 50

Что является носителем следовой информации при компьютерном преступлении?

-: бумага

+: файл данных или прикладного ПО

-: пакет

-: контейнер

Вопрос 51

Что выступает в качестве следообразующего объекта у следов-отображений?

+: виртуальный объект – система команд ЭВМ

-: визуальный объект – система команд ПК

-: осязаемый объект

-: следы-вещества

Вопрос 52

Что входит в классификацию следов-отображений?

-: виртуальный объект

-: файл

-: система команд

+: всё вышеперечисленное

Вопрос 53

По какому признаку не классифицируются следы-отображения?

-: по характеру изменений

-: по размещению

+: по замещению

-: по степеням завершенности обработки команд

Вопрос 54

Что понимается под структурными файловыми следами?

-: стабильные во времени файловые следы

+: изменение содержимого файла, делающего файл отличным от оригинального

-: временные файловые следы

-: преобразование носитель информации

Вопрос 55

Что относится к внешним файловым следам?

+: изменение атрибутов файла, его размера, типа, имени и модификации

-: изменение носителя информации

-: изменение местонахождения файла

-: верного ответа нет

Вопрос 56

Какое время могут существовать на носителях информации стабильные во времени файловые следы-отображения?

+: сколько определено работой прикладного ПО

-: неограниченное количество

-: два часа

-: два года

Вопрос 57

В каком случае возникают временные файловые следы?

-: при несанкционированном доступе в систему

-: при отказе в доступе

+: при аварийном завершении работы прикладной программы или процесса

-: при задержании преступника с поличным

Вопрос 58

Какие следы образуются на рабочих местах пользователей в результате работы клиентской части сетевой ос и (или) прикладного ПО?

-: сетевые файловые следы

-: прикладные файловые следы

-: временные файловые следы

+: локальные файловые следы

Вопрос 59

Какие следы могут быть обнаружены в виде расходных материалов (тонеров, красок), различных смазок, используемых в КС?

+: следы-вещества

-: следы-отображения

-: следы-предметы

-: временные следы

Вопрос 60

В классификацию следов-предметов входят:
-: сменные диски и ленты
-: аппаратные закладные устройства
-: устройства дистанционного съёма информации
+: всё вышеперечисленное

Вопрос 61

Что не входит в классификацию следов-предметов?
-: сменные диски и ленты
-: аппаратные закладные устройства
+: внешние файловые следы
-: устройства дистанционного съёма информации

Вопрос 62

Что является важнейшими следами-предметами при расследовании дел о компьютерных преступлениях?
+: документы на бумажных и электронных носителях
-: аппаратные закладные устройства
-: устройства дистанционного съёма информации
-: всё вышеперечисленное

Вопрос 63

Что, как правило, не осуществляется в сетевых операционных системах?
-: фиксация и контроль регистрации пользователя в системе и выхода из неё
+: фиксация подключения к сети Интернет в соседнем помещении
-: фиксация операций чтения, записи, создания и удаления файлов
-: фиксация изменений полномочий доступа

Вопрос 64

Какая политика определяет права, присваиваемые группам и отдельным пользователям?
-: политика учетных записей
-: политика аудита
+: политика прав пользователей
-: политика интерфейса

Вопрос 65

Предоставление пользователю возможности выполнить определённое действие в системе – это:
+: привилегия
-: приоритет
-: право доступа
-: интерфейс

Вопрос 66

Какой набор пригодных для идентификации сведений содержит учетная запись пользователя?
-: имя
-: пароль для входа в систему
-: права и разрешения
+: всё вышеперечисленное

Вопрос 67

Пользователь с каким именем в системе управляет всеми сторонами работы компьютера?
-: Guest
-: Programmist
+: Administrator

-: User

Вопрос 68

Какая учетная запись создана для того, чтобы пользователь, работающий на компьютере редко или единожды, мог войти в систему и получить

ограниченный доступ к ресурсам?

+: Guest

-: Programmist

-: Administrator

-: User

Вопрос 69

Организационная защита обеспечивает:

+: организацию охраны, работу с кадрами

+: использование технических средств безопасности

+: организацию работы с документами

-: формирование информационных ресурсов

Вопрос 70

Организационные средства защиты ПЭВМ и информационных сетей применяются:

-: при подборе и подготовке персонала

-: при хранении и использовании документов и др. носителей

-: при проектировании и строительстве объектов сети

+: все вышеперечисленное

Вопрос 71

По видам угрозы чаще всего подразделяют на 2 основных класса:

+: Естественные

-: Косвенные

-: Непреднамеренные

+: Субъективные

Вопрос 72

Обработка персональных данных должна осуществляться на основе принципов:

+: недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных

-: соответствия объема и характера обрабатываемых персональных данных

-: осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами

+: соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных

Вопрос 73

Организационно-правовыми формами защиты являются:

-: перечень сведений с коммерческой тайной

-: обязательства при совместной деятельности

-: договоры о совместной деятельности

+: все вышеперечисленное

Вопрос 74

Недостаточная квалификация или нарушение должностных инструкций могут породить такие проявления непреднамеренных угроз:

-: съем информации путем установки специальных технических средств

+: повреждение оборудования

+: нерациональное изменение технологий

-: хищение материальных носителей

Вопрос 75

Преднамеренные угрозы классифицируются как:

+: бесконтактные

-: информационные

+: контактные

-: внешние

Вопрос 76

Умышленными информационные угрозами по цели воздействия на автоматические системы обработки информации (АСОИ) являются:

+: неадекватность политики безопасности реалиям АСОИ

+: нарушение целостности информации

-: нерациональное изменение технологий

-: все вышеперечисленное

Вопрос 77

Умышленные информационные угрозы по способу воздействия на автоматические системы обработки информации (АСОИ) классифицируются:

-: непосредственное воздействие на объект

-: с использованием скрытых каналов

+: в интерактивном режиме

+: в пакетном режиме

Вопрос 78

Угрозами по способу воздействия объект (при активном воздействии) являются:

-: через других пользователей

-: присвоение прав другого пользователя

-: использование «вслепую»

+: все вышеперечисленное

Вопрос 79

Злоумышленными действиями персонала предприятия не являются:

-: прерывание

-: кража

+: утеря

-: модификация

Вопрос 80

Угрозы безопасности информации по субъектам классифицируются:

+: стихийные

+: техногенные

-: правовые

+: антропогенные

Повышенный уровень

Вопрос 81

Все физические средства защиты объектов можно разделить на категории:

+: средства предупреждения

-: контактные средства

+: средства обнаружения

-: информационные средства

Вопрос 82

По тактическому назначению охранные системы подразделяются на системы охраны:

+: вспомогательные технические средства

-: бесконтактные средства
-: информационные средства
+: периметров объектов

Вопрос 83

К средствам физической защиты относятся:
-: средства обнаружения
+: зоны безопасности
+: особые конструкции периметров
-: системы контроля доступа

Вопрос 84

Различают 2 вида обязательной составной части систем защиты объекта – охранного освещения:
-: постоянное
-: сигнальное
+: дежурное
+: тревожное

Вопрос 85

К персональным методам опознавания относят:
+: атрибутивные способы
-: статистические способы
-: динамические способы
+: все вышеперечисленное

Вопрос 86

На службу безопасности предприятия возлагаются следующие функции:
+: осуществление контроля выполнения требований «Инструкции по защите конфиденциальной безопасности»
+: организация обучения сотрудников службы и персонала
-: определение участков сосредоточения конфиденциальных сведений
+: осуществление контроля выполнения требований «Инструкции по защите конфиденциальной безопасности»

Вопрос 87

Служба безопасности является самостоятельной организационной единицей предприятия, подчиняясь непосредственно:
-: начальнику службы
-: заместителю руководителя предприятия по безопасности
+: руководителю предприятия
-: экспертной комиссии по безопасности

Вопрос 88

Организационно служба безопасности состоит из следующих структурных единиц:
-: подразделения режима и охраны
-: информационно-аналитические подразделения
-: инженерно-технические подразделения
+: все вышеперечисленное

Вопрос 89

Аппаратные средства защиты информации применяются для решения следующих задач:
+: локализация каналов утечки информации
+: поиск и обнаружение средств промышленного шпионажа
-: оперативная корректировка информационной базы данных с доступом по паролю
-: определение участков сосредоточения конфиденциальных сведений

Вопрос 90

Подразделение службы безопасности «Детективная группа» выполняет следующие функции:

+: проверка кандидатов для приема на работу на объект

-: контроль работоспособности элементов системы защиты

+: разработка специальных мероприятий в отношении фирм-конкурентов

-: разработка соответствующих инструкций о порядке работы с конфиденциальной информацией

Вопрос 91

Подразделение службы безопасности «Группа охраны и сопровождения» выполняет следующие функции:

-: контроль работоспособности элементов системы защиты

+: допуск персонала к работе с конфиденциальной информацией

-: ответственность за личную охрану руководства

+: обеспечение безопасности транспортировки грузов и документов

Вопрос 92

Подразделение службы безопасности «Группа режима» выполняет следующие функции:

+: организация закрытого делопроизводства

+: проверка выполнения сотрудниками объекта регламента работы с конфиденциальной информацией

-: контроль работоспособности элементов системы защиты

-: поддержка контакта с правоохранительными органами по вопросам обеспечения безопасности объекта

Вопрос 93

К методам перехвата информации относятся:

+: непосредственный

-: косвенный

+: уборка мусора

-: нет верного ответа

Вопрос 94

Смарт-карты включают в себя:

+: программируемое ПЗУ

-: кэш память

-: флеш память

+: энергозависимую перепрограммируемую память

Вопрос 95

Какой кодекс является частью законодательства РФ о коммерческой тайне:

-: Кодекс РФ об Административных нарушениях

+: Гражданский кодекс

-: Трудовой кодекс

-: Гражданский процессуальный кодекс

Вопрос 96

Метод «Поиск Бреши» - это метод:

-: при котором злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя

+: при котором используются ошибки или неудачи в логике построения программы

-: который используется при случайном подключении «чужой» системы

-: который используется как для анализа процессов, так и для планирования методов совершения преступления

Вопрос 97

Действие ФЗ «О Персональных данных» не распространяется на отношения, возникающие при:

-: обработке персональных данных (ПД), относящихся к сведениям, составляющим государственную тайну

+: обработке ПД физическими лицами исключительно для личных и семейных

-: обработке персональных данных (ПД), относящихся к сведениям, составляющим коммерческую тайну

-: все вышеперечисленное

Вопрос 98

Результатами интеллектуальной деятельности, которым предоставляется правовая охрана, не являются:

-: промышленные образцы

-: товарные знаки

-: топологии интегральных микросхем

+: все вышеперечисленное является

Вопрос 99

Автор(ы) результата интеллектуальной деятельности – это:

+: гражданин, творческим трудом которого создан такой результат

-: граждане, не внесшие личного творческого вклада в создание такого результата

-: граждане, оказавшие его автору только техническое, консультационное, организационное или материальное содействие

-: граждане, осуществлявшие контроль за выполнением соответствующих

-: все вышеперечисленное

Вопрос 100

Исключительные права на результаты интеллектуальной деятельности и на средства индивидуализации, установлены:

+: международными договорами Российской Федерации

-: Гражданским процессуальным кодексом

+: Конвенцией по охране промышленной собственности

-: верного ответа нет

Вопрос 101

В какой части Гражданского кодекса рассмотрены права на результаты интеллектуальной деятельности и средства индивидуализации:

-: 1 ч.

-: 2 ч.

-: 3 ч.

+: 4 ч.

Вопрос 102

Обладатель исключительного права на результат интеллектуальной деятельности или на средство индивидуализации – это:

-: лицензиат

+: лицензиар

-: правообладатель

-: юридическое лицо

Вопрос 103

Лицензионный договор должен предусматривать:

+: предмет договора путем указания на результат интеллектуальной деятельности или на средство индивидуализации

-: лицензиату в праве использовать результаты интеллектуальной

деятельности с сохранением за лицензиаром права выдачи лицензий другим лицам

+: способы использования результата интеллектуальной деятельности или средства индивидуализации

+: определение поведения системы в реальном времени

Вопрос 104

Автору произведения не принадлежат следующие права:

-: исключительное право на произведение

-: право автора на имя

-: право авторства

+: принадлежат все вышеперечисленные права

Вопрос 105

Авторские права распространяются на:

-: языки программирования

-: способы, решения технических, организационных или иных задач

+: аудиовизуальные произведения

+: составные произведения

Вопрос 106

Заявка на регистрацию программ для ЭВМ и баз данных должна содержать:

-: заявление о государственной регистрации программы для ЭВМ или базы данных с указанием правообладателя

-: документ, подтверждающий уплату государственной пошлины в установленном размере

-: депонируемые материалы, идентифицирующие программу для ЭВМ или базу данных

+: все вышеперечисленное

Вопрос 107

При положительном результате проверки федеральный орган

исполнительной власти по интеллектуальной собственности вносит программу для ЭВМ или базу данных в:

+: реестр программ для ЭВМ

+: реестр баз данных

-: официальный бюллетень этого органа

-: верного ответа нет

Вопрос 108

Действия, необходимые для достижения способности к взаимодействию разработанной программы с другими, правомерны при соблюдении:

-: информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников

-: действия осуществляются в отношении частей декомпилируемой

программы для ЭВМ, которые необходимы для достижения способности к взаимодействию

-: информация, полученная в результате декомпилирования, не может передаваться иным лицам

+: все вышеперечисленное

Вопрос 109

Объектами смежных прав являются:

+: базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов

+: фонограммы

-: информация, полученная в результате декомпилирования программы

+: сообщения передач организаций эфирного или кабельного вещания

Вопрос 110

Изготовителю базы данных (БД) принадлежат следующие права:

-: исключительное право изготовителя БД

-: право на указание на экземплярах базы данных и (или) их упаковках своего имени или наименования

-: право изготовителя БД признается независимо от наличия и действия авторских прав изготовителя на составляющие БД материалы

+: все вышеперечисленное

Вопрос 111

Объектами патентных прав являются:

+: результаты интеллектуальной деятельности в научно-технической сфере

-: способы клонирования человека

+: результаты интеллектуальной деятельности в сфере художественного конструирования

-: иные решения, противоречащие общественным интересам, принципам гуманности и морали

Вопрос 112

Действие ФЗ "О персональных данных" не распространяется на отношения, возникающие при обработке:

+: персональных данных физическими лицами исключительно для личных и семейных нужд без нарушения прав субъектов

+: подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах

+: персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну

-: обработке персональных данных, осуществляемых государственными органами РФ

Вопрос 113

Законодательство Российской Федерации в области персональных данных основывается на:

+: Конституции Российской Федерации

+: Законе «О персональных данных»

-: Законе «О коммерческой тайне»

-: Уголовном кодексе РФ

Вопрос 114

Обеспечение конфиденциальности персональных данных не требуется

+: в случае обезличивания персональных данных:

-: в случае соответствия объема и характера обрабатываемых персональных данных

-: в случае достоверности персональных данных

+: в отношении общедоступных персональных данных

Вопрос 115

Регламентация производственной деятельности и взаимоотношения на нормативно-правовой основе исключающее или существенно затрудняющей проявление внутренних и внешних угроз – это:

+: организационная защита

-: правовая защита

-: организационно-правовая

-: информационная защита

Вопрос 116

Сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию – это:

-: правообладатель
-: оператор
+: контрагент
-: лицензиар

Вопрос 117

Государственный орган, муниципальный орган, юридическое или физическое лицо, осуществляющие обработку персональных данных – это:
-: контрагент
+: оператор
-: лицензиат
-: лицензиар

Вопрос 118

Основные компоненты критериев качества баз данных:
-: организация защиты баз данных от несанкционированных действий
+: программные средства системы управления баз данных
+: информация баз данных конкретной проблемно-ориентированной сферы применения
-: все вышеперечисленное

Вопрос 119

Мозговая атака – это:
-: логическая последовательность событий или возможных вариантов решения проблемы, упорядоченных во времени
+: метод тренировки мышления, нацеленный на открытие новых идей и достижение согласия группы людей на основе интуитивного мышления
-: применение математических методов лицами, обладающими достаточным опытом в рассматриваемой предметной области
- метод, при котором используются ошибки или неудачи в логикепостроения программы

Вопрос 120

Задачи, решаемые инструментальными средствами структурного анализа:
+: определение задач, которые система должна выполнять
+: определение отношений между данными
-: применение графических и текстовых средств моделированияработ

1.2 Вопросы для собеседования по темам лекций 1-27

Базовый уровень

1. Порядок засекречивания сведений, составляющих государственнуютайну и их носителей.
2. Реквизиты носителей сведений, составляющих государственную тайну.
3. Порядок рассекречивания сведений, составляющихгосударственную тайну и их носителей.
4. Права собственника информации, составляющей государственную тайну.
5. Допуск должностных лиц и граждан к государственной тайне.
6. Основания для отказа в допуске к государственной тайне.
7. Ограничение прав должностных лиц и граждан, допущенных к государственной тайне.
8. Особый порядок допуска должностных лиц и граждан кгосударственной тайне.
9. Условия прекращения допуска к государственной тайне.

10. Организация доступа должностных лиц или граждан кгосударственной тайне.

11. Понятие и виды ответственности за нарушение законодательства вобласти защиты государственной тайны.

12. Понятие административной ответственности за нарушение законодательства в области защиты государственной тайны.

13. Понятие уголовной ответственности за нарушение законодательства в области защиты государственной тайны.

14. Дисциплинарная ответственность за нарушение в области защиты государственной тайны.

15. Органы защиты государственной тайны.

16. Лицензирование деятельности юридических лиц в области защиты государственной тайны.

17. Порядок сертификации средств защиты информации.

18. Государственная политика в сфере информатизации.

19. Структура органов информационного законодательства РФ.

20. Понятие служебной тайны в российском законодательстве. Объекты и субъекты права на служебную тайну.

Повышенный уровень

1. Нормативно-правовая база в области защиты служебной тайны.

2. Сведения, относящиеся и не относящиеся к служебной тайне.

3. Федеральный закон Российской Федерации от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне».

4. Законодательные и иные нормативно-правовые акты, регулирующие защиту коммерческой тайны. Объекты и субъекты права на коммерческую тайну.

5. Постановление Правительства РФ от 5.12.1991 г. №35 «О перечне сведений, которые не могут составлять коммерческую тайну».

6. Рекомендации по отнесению сведений к коммерческой тайне. Режим коммерческой тайны.

7. Основные права и обязанности собственника коммерческой тайны.

8. Юридический статус информации «ноу-хау», в режиме коммерческой тайны

9. Система защиты коммерческой тайны.

10. Защита коммерческой тайны в трудовых и гражданско-правовых отношениях.

11. Понятие профессиональной тайны в российском законодательстве. бъекты и субъекты права на профессиональную тайну.

5. Список рекомендуемой литературы

5.1.1. Основная литература

1. Романов О.А. Организационное обеспечение информационной безопасности: учебник для студ. высш. учеб. заведений / О.А.Романов, С.А.Бабин, С.Г.Жданов. – М.: Издательский центр «Академия», 2013. – 192 с.

2. Шумский А.А. Системный анализ в защите информации: учебное пособие для студентов ВУЗов, обучающихся по специальностям в области информ. безопасности / А.А.Шумский, А.А.Шелупанов. – М.: Гелиос АРВ, 2013. – 224 с.

3. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студ. Высших учеб. заведений / В.П.Мельников,

С.А.Клейменов, А.М.Петраков. – М.: Издательский центр «Академия», 2013. – 336 с.

4. Корнеев И.К. Защита информации в офисе: учеб. – М.: ТК Велби, Изд-во Проспект, 2013. – 336 с.

5. Аверченков В.И. Защита персональных данных в организации. Монография / В.И.Аверченков, М.Ю.Рытов, Т.Г.Гайнулин. – Брянск. БГТУ, 2014. – 124 с.

4.4. Методические рекомендации по написанию научных текстов (докладов, рефератов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление.

Структура доклада:

- Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.
- Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.
- Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса
- Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.
- Приложение (при необходимости).

Требования к оформлению:

- текст с одной стороны листа;
- шрифт Times New Roman;
- кегль шрифта 14;

- межстрочное расстояние 1,5;
- поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
- реферат должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Доклад оценивается по следующим критериям: соблюдение требований к его оформлению; необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации; умение студента свободно излагать основные идеи, отраженные в докладе; способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

4.5. Методические рекомендации по подготовке к зачетам

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет (Sзач) при различных рейтинговых баллах по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре (*Rсем*)	**Количество баллов за зачет (*S*зач)**
50 ≤ *Rсем* ≤ 60	**40**
39 ≤ *Rсем*< 50	**35**
33 ≤ *Rсем* < 39	**27**
***Rсем*< 33**	**0**

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка выполнения доклада и его презентации.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основной литературы:

1 Корнеев, И.К. Защита информации в офисе: учебник/ И. К. Корнеев, Е. А. Степанов- М.: ТК Велби, 2018.

2. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие/ В. Ф. Шаньгин- М.: ИНФРА-М, 2019.

Дополнительная литература:

1. Садердинов, А.А. Информационная безопасность предприятия [Текст]: учеб.пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. - 4-е изд. - М.: ИТК "Дашков и К", 2012.
2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие/ В. Ф. Шаньгин- М.: ФОРУМ, 2012.

Методическая литература:

1. Методические указания по выполнению практических работ по дисциплине «Организационное и правовое обеспечение информационной безопасности».
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Организационное и правовое обеспечение информационной безопасности».

Интернет-ресурсы:

1. www.intuit.ru – национальный открытый университет «ИНТУИТ»;
2. www.window.edu.ru –единое окно доступа к образовательным ресурсам;

3. www.citforum.ru – сервер информационных технологий.
4. http://biblioclub.ru
5. http://elibrary.ru/

Программное обеспечение:

1	Альт Рабочая станция 10
2	Альт Рабочая станция K
3	Альт «Сервер»
4	Пакет офисных программ - Р7-Офис

Материально-техническое обеспечение

1. Лабораторные и практические занятия проводятся в компьютерных классах, в которых установлено вышеперечисленное программное обеспечение.
2. Лекционный курс проводится в аудиториях, оснащенных проектором.