Министерство образования и науки Российской федерации

федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»

Кафедра радиоэлектроники и защиты информации (РЗИ)

Организационно-правовое обеспечение информационной безопасности

Методические указания по практическим занятиям и самостоятельной работе
для специальности 090106 «Информационная безопасность телекоммуникационных систем»

Разработчик:
доцент каф. РЗИ, к.т.н.
_____Э.В. Семенов

2012

Учебно-методическое пособие предназначено для подготовки и проведения практических занятий по дисциплине «Организационно-правовое обеспечение информационной безопасности» для специальности 090106 «Информационная безопасность телекоммуникационных систем». Пособие содержит перечни вопросов для контрольных работ и тем для индивидуальных заданий.

Содержание

1. Цели и задачи дисциплины, ее место в учебном процессе

Цели преподавания дисциплины

Цель преподавания дисциплины – ознакомить студентов с основами существующей системы организационных мер и правовых норм, имеющих отношение к информационной безопасности.

Задачи изучения дисциплины

Для достижения целей преподавания решаются следующие задачи:

- изучение общих понятий и норм, регулирующих обеспечение информационной безопасности в целом (правовое обеспечение информационной безопасности);
- изучение вопросов организационного обеспечения информационной безопасности.

В результате изучения дисциплины студент должен знать:

- информационные аспекты конституционного права, право на доступ к информации;
- законодательство о государственной тайне;
- правовые нормы в области защиты конфиденциальной информации;
- правовые нормы в области защиты интеллектуальной собственности;
- нормы ответственности за нарушения в области секретной, конфиденциальной информации и интеллектуальной собственности;
- средства и методы физической защиты объектов;
- вопросы организации пропускного, внутриобъектового режима и режима секретности.

Студент должен уметь:

- анализировать и оценивать угрозы и ущерб информационной безопасности объекта;
- практически использовать рассмотренные правовые нормы при обеспечении информационной безопасности;
- решать вопросы организации информационной безопасности объекта.

Место дисциплины

Дисциплина относится к циклу общепрофессиональных дисциплин (ОПД.Ф.6).

Перечень дисциплин и разделов (тем), необходимых студентам для изучения данной дисциплины:

- политология (политическая жизнь и властные отношения, политическая система, политические технологии, мировая политика и международные отношения, национально-государственные интересы России в новой геополитической ситуации);
- правоведение (государство и право; источники российского права; система российского права; отрасли права; конституция – основной закон государства; система органов государственной власти в РФ; трудовая дисциплина и

ответственность за ее нарушение; административные правонарушения и административная ответственность; уголовная ответственность за совершение преступлений);

- основы информационной безопасности (анализ угроз ИБ; виды информации; методы и средства обеспечения ИБ; методы нарушения конфиденциальности, целостности и доступности информации; основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем).

2. Контрольные работы

Контрольная 1. Защита государственной и служебной тайн

Вариант 1

1. Для кого обязательны положения закона о государственной тайне?
2. Порядок отнесения сведений к государственной тайне.
3. Являются ли секретными развернутые перечни сведений, подлежащих засекречиванию?
4. Обязано ли государство компенсировать собственнику ущерб в связи с засекречиванием информации?
5. Какие права граждан могут быть ограничены в связи с допуском к государственной тайне?
6. В каких случаях проводятся проверочные мероприятия, связанные с допуском к государственной тайне, и в каких нет?
7. Как определяются должности, при приеме на которые работники подлежат оформлению на допуск?
8. Каким образом пересылаются документы, составляющие служебную тайну?

Вариант 2

1. Перечислите классы сведений, составляющих государственную тайну.
2. Кто формирует печень сведений, отнесенных к государственной тайне?
3. Приведите примеры должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.
4. Для кого предусматривается допуск к государственной тайне без проведения проверочных мероприятий?
5. Какой документ определяет порядок обращения с информацией, составляющей служебную тайну?
6. Какие существуют ограничения по допуску к ГТ лиц, не достигших 18 лет?
7. Является ли карточка формы 3 секретным документом, где она хранится, что с ней происходит при увольнении работника?
8. Как размножают документы, составляющие служебную тайну?

Вариант 3

1. Принципы отнесения сведений к государственной тайне.
2. Является ли секретным перечень сведений отнесенных к государственной тайне?
3. Может ли быть засекречена информация, находящаяся в собственности граждан и негосударственных организаций?
4. Перечислите основания для отказа в допуске к государственной тайне.
5. В каком порядке ведется переписка по вопросам допуска?
6. Как и в каких случаях производится переоформление допуска?
7. Какая пометка присваивается документам, содержащим информацию, составляющую служебную тайну?
8. Как передаются работникам документы, составляющие служебную тайну?

Вариант 4

1. Приведите примеры сведений, не подлежащих засекречиванию.

2. Чем отличается перечень сведений, отнесенных к государственной тайне от печечня сведений, составляющих государственную тайну?
3. Может ли быть засекречена информация, находящаяся в собственности иностранных граждан и организаций?
4. Перечислите основания для прекращения допуска к государственной тайне.
5. Какими подразделениями ведется подготовка документов по вопросам допуска?
6. Какой набор документов необходим командируемому в другую организацию по секретным вопросам? Что с ними делают по месту командировки и возвращают ли назад?
7. Допускается ли учет документов, составляющих служебную тайну, совместно с другими несекретными документами?
8. Как выполняется уничтожение документов, составляющих служебную тайну?

Контрольная 2. Защита коммерческой тайны и персональных данных

Вариант 1

1. Какие сведения могут составлять коммерческую тайну (КТ)?
2. Кто имеет право относить информацию к КТ?
3. С какого момента они возникают права обладателя КТ?
4. В каком случае обладатель КТ не имеет права прекратить по своему желанию охрану КТ?
5. Что такое персональные данные (ПД)
6. Что такое специальные категории персональных данных?
7. В чем состоит право на доступ субъекта к своим ПД и когда оно ограничивается?

Вариант 2

1. Кто такой "обладатель информации, составляющей КТ?"
2. Законные и незаконные способы получения КТ.
3. Кто является обладателем КТ, полученной в рамках трудовых отношений?
4. Какая ответственность предусмотрена за использование КТ, полученной по ошибке?
5. Возможно ли, чтобы персональные данные были общедоступными?
6. Когда допускается обработка специальных категорий персональных данных? Варианты ответа.
    - Всегда.
    - Никогда.
    - Не допускается при следующих исключениях...
7. Требуется ли согласие субъекта ПД на обработку его ПД для продвижения товаров и услуг путем прямых контактов с потребителем? Варианты ответа.
    - Требуется предварительное согласие.
    - Достаточно "молчаливого" согласия.
    - Оператор вправе действовать без согласия субъекта ПД.

Вариант 3

1. В чем отличие между доступом, передачей и предоставлением КТ?
2. Перечислите сведения, которые не могут составлять КТ.
3. Сохраняются ли обязанности работника по неразглашению КТ после увольнения?
4. На что и на кого распространяется действие закона о ПД и на какие случаи не распространяется.

5. Требуется ли согласие субъекта ПД на обработку его ПД? Варианты ответа.
    - Не требуется никогда.
    - Требуется всегда.
    - Требуется, за исключением случаев...
6. Что такое биометрические персональные данные?
7. Какие органы обеспечивают надзор за исполнением закона о ПД?

Вариант 4

1. Может ли бездействие квалифицироваться как разглашение КТ?
2. Имеют ли право государственные органы истребовать КТ? Варианты ответов:
    - мотивированно;
    - немотивированно.
3. В каких случаях закон освобождает разгласившего КТ от возмещения ущерба?
4. Принципы обработки персональных данных.
5. В какой форме должен давать субъект ПД свое согласие на обработку ПД. Должен ли оператор доказывать, что согласие суъекта ПД на обработку его ПД было получено или это согласие считается наличествующим по умолчанию?
6. Требуется ли согласие субъекта ПД на обработку биометрических ПД? Варианты ответа.
    - Не требуется никогда.
    - Требуется всегда.
    - Требуется, за исключением случаев...
7. Что должно включать в себя согласие субъекта на обработку персональных данных?

Контрольная 3. Правовые основы деятельности специальных служб

Вариант 1

1. В каком случае граждане и организации имеют право получать разъяснения от органов ФСБ?
2. В каком случае сотрудники органов ФСБ имеют право входить в помещения, принадлежащие гражданам?
3. Необходимо ли согласие руководителя для прикомандировывания сотрудника ФСБ к предприятию?
4. Перечислите задачи ФСБ, связанные с работой радиопередающих средств.
5. Могут ли органы внешней разведки осуществлять разведывательную деятельность в отношении граждан РФ?
6. Спецсвязь и фельдъегерская связь. История возникновения, сходства и различия.
7. Задачи федеральной фельдъегерской связи.
8. Сферы, направления деятельности ФСТЭК.
9. Какое направление в структуре ФСО занимается связью?

Вариант 2

1. Перечислите направления деятельности органов ФСБ.
2. В каком случае сотрудники органов ФСБ имеют право проверять у граждан документы?
3. Имеют ли право лица, содействующие органам ФСБ, зашифровывать свою личность?

4. Обязанности различных организаций, связанные с изготовлением органами ФСБ документов оперативного прикрытия.
5. Задачи службы специальной связи.
6. Права федеральной фельдъегерской связи.
7. Действия фельдъегерей перед применением оружия, специальных средств и физической силы.
8. Подведомственность и руководство ФСТЭК.
9. Какого рода связь обеспечивает ФСО и кого она обеспечивает этой связью?

Вариант 3

1. Допустимо ли осуществление разведовательной деятельности органами ФСБ?
2. Для предприятий какой формы собственности обязательны представления ФСБ об устранении условий, способствующих реализации угроз безопасности РФ?
3. Кого не имеют права органы ФСБ привлекать к сотрудничеству?
4. Какая задача помимо добывания и обработки информации возлагается на внешнюю разведку РФ?
5. Могут ли сотрудники органов внешней разведки состоять в политических партиях?
6. Структура специальной связи.
7. Порядок задержания и досмотра корреспонденции, доставляемой фельдъегерской связью.
8. Для каких организаций обязательны нормативные документы ФСТЭК?
9. Задачи ФСО.

Вариант 4

1. В каких случаях органы ФСБ имеют право использовать не принадлежащие им средства связи и транспорт?
2. Какие организации обязаны включать дополнительное оборудование в состав средств связи по требованию органов ФСБ?
3. В чьем подчинении находятся силы, обеспечивающие охрану государственной границы?
4. Какие органы осуществляют деятельность в сфере внешней разведки?
5. Какой деятельностью по совместительству могут заниматься сотрудники органов внешней разведки?
6. Кто может быть получателем корреспонденции, доставляемой спецсвязью:
    - физические лица;
    - юридические лица;
    - государственные структуры?
7. Действия фельдъегеря при отсутствии возможности обеспечить сохранность корреспонденции.
8. Какие основные документы регламентируют деятельность ФСО?
9. Структура ФСО.

Контрольная 4. Система правовой ответственности за разглашение защищаемой инфомации и невыполнение правил ее защиты

Вариант 1

1. В какой форме возможна защита права на информацию с ограниченным доступом?
2. Каково наказание за гос. измену?

3. В чем заключается постановление конституционного суда в отношении понятия "выдача гос. тайны"?
4. Формальный или материальный состав преступления предусмотрен статьей 284 УК?
5. Перечислите статьи УК, предусматривающие ответственность за разглашение сведений, составляющих СТ или ПТ.
6. Являются ли преступлением незаконные:
    - производство;
    - сбыт;
    - приобретение

    специальных технических средств, предназначенных для негласного получения информации?

7. Какой состав преступления в ст. 272 УК (Неправомерный доступ к компьютерной информации) формальный или материальный? Каково максимальное наказание?
8. На какую территорию и каких лиц (гражданство) распространяется уголовный закон?
9. Что такое необходимая оборона?

Вариант 2

1. В каком порядке возможна защита права на информацию с ограниченным доступом?
2. Какие альтернативные формы гос. измены предусмотрены в УК?
3. Кто является субъектом преступления по 276 статье УК?
4. При каком условии разглашение ГТ становится оконченным преступлением?
5. Кто является субъектом преступления по ч.2 статьи, предусматривающей ответственность за разглашение КТ и БТ?
6. Какие обстоятельства приводят к квалификации преступления по более строгой (второй) части статьи 138 (Нарушение тайны переписки...)?
7. Является ли уголовным преступлением создание программ-вирусов само по себе или лишь после нанесения ими ущерба? Каково максимальное наказание?
8. При каких условиях российские граждане, совершившие преступление на территории иностранного государства, выдаются этому государству?
9. Формы вины.

Вариант 3

1. Перечислите статьи уголовного кодекса, предусматривающие ответственность за нарушения, связанные с ГТ.
2. Какие сведения могут быть предметом шпионажа как уголовно наказуемого деяния?
3. Кто является субъектом преступления по 283 статье УК?
4. Какая форма вины предусматривается статьей 284 УК?
5. Какая статья УК предусматривает ответственность за разглашение по неосторожности сведений, составляющих КТ и БТ?
6. Каково максимальное наказание по статье 138 (Нарушение тайны переписки...) и за какие деяния оно предусмотрено?
7. При каком условии нарушение правил эксплуатации ЭВМ является уголовным преступлением? Каково максимальное наказание?
8. Что называется преступлением?

9. В каком случае лицо, совершившее деяние, описанное одной из статей особенной части УК, не считается виновным?

Вариант 4

1. При каких условиях лицо, совершившее гос. измену, освобождается от ответственности?
2. Может ли рассматриваться как шпионаж хранение сведений?
3. Формальный или материальный состав преступления предусмотрен статьей 283 ч.2 УК?
4. За разглашение всякой ли СТ предусмотрена уголовная ответственность?
5. Какой состав преступления (формальный или материальный) предусматривают ч.1 и ч.2 статьи о разглашении сведений, составляющих КТ и БТ?
6. В каком случае уголовным законом охраняются личные тайны? Каково максимальное наказание?
7. Имеет ли уголовный закон обратную силу?
8. Классификация преступлений по тяжести.
9. В каком случае наступает ответственность за приготовление к преступлению?

Контрольная 5. Защита интеллектуальной собственности

Вопрос 1

1. Перечислите основные институты, на которые подразделяется законодательство об интеллектуальной собственности.
2. Кому принадлежат неимущественные и имущественные права на служебное произведение?
3. В каких случаях допускается осуществлять декомпиляцию программ для ЭВМ?
4. Что такое коллективное управление имущественными правами?
5. Какие объекты ИС нельзя защищать секретными патентами?
6. Обеспечиваются ли имущественные права автора, не являющегося патентообладателем?
7. Перечислите основные разновидности лицензий и их особенности.
8. Какова судьба "открытой" заявки, если будет установлено, что в ней содержатся сведения, составляющие государственную тайну?
9. Что такое недобросовестная конкуренция вообще в определении парижской конвенции?
10. Как определяется, на какие государства будет распространяться правовая охрана в случае "удовлетворения" международной заявки?

Вопрос 2

1. Какие конкретно права объединяет термин "личные неимущественные права"?
2. Перечислите отличительные особенности (принципы) авторского права. Произведения в каких сферах регулируются законом об авторском праве и смежных правах? Что не является объектом авторского права?
3. Как осуществляется выплата вознаграждения автору при воспроизведении его произведения в личных целях?
4. Какие выплаты и в каком размере можно потребовать от нарушителя авторских прав?
5. Условия патентоспособности изобретения, полезной модели?

6. Если несколько лиц обладают одним патентом и между ними отсутствует консенсус, то как регулируются их права?
7. Каким органом рассматриваются заявки на секретные изобретения?
8. При каком общем условии нарушения авторского и патентного прав являются преступлениями?
9. Каких этапов патентования касается договор о патентной кооперации? В соответствии с договором о патентной кооперации на изобретение выдается один патент или несколько?
10. Каков срок действия охранного документа в соответствии с Евразийской патентной конвенцией?

Вопрос 3

1. При каком условии библиотека может предоставить произведение в цифровой форме?
2. Каков срок действия авторского права? Смежных прав?
3. Назовите наиболее существенный момент, который отличает охрану программ для ЭВМ в рамках закона "Об авторском праве и смежных правах" и в рамках закона "О правовой охране программ для ЭВМ и баз данных".
4. Могут ли быть заявителю противопоставлены по новизне собствнные публикации?
5. Может ли быть предоставлена лицензия против воли патентообладаетеля?
6. Как устанавливается дата приоритета объектов патентного права?
7. Какие сведения включаются в уровень техники при установлении новизны секретного изобретения?
8. Какие конкретно действия парижская конвенция рассматривает как недобросовестную конкуренцию?
9. Какой охранный документ можно получить в соответствии с Евразийской патентной конвенцией, какие права он удостоверяет?
10. Чем принципиально отличаются объекты защиты в патентном праве, что делает невозможной их защиту в рамках авторского права?

Вопрос 4

1. Как регулирует закон взаимоотношения соавторов?
2. Нужно ли согласие автора при использовании его произведения таким образом, что оно одновременно сообщается большому количеству людей?
3. При каких условиях допускается репродуцирование произведения без согласия автора и выплаты ему авторского вознаграждения?
4. Срок действия патентных прав.
5. Срок действия права авторства в рамках патентного права.
6. Какие действия не признаются нарушением прав патентообладателя?
7. Какие экспертизы и в какой последовательности проводятся в отношении заявок?
8. Особенности подачи заявок на выдачу патента в иностранных государствах связанные с соблюдением законодательства о государственной тайне.
9. Что такое конвенционный приоритет?
10. На какую территорию распространяется действие охранного документа, полученного в соответствии с Евразийской патентной конвенцией?

3. Индивидуальные задания

Студент может выбрать одну из нижеперечисленных тем индивидуальных заданий либо предложить по согласованию с преподавателем собственную тему.

1. Право на доступ к информации.
2. Право на защиту от вредной информации.
3. Информационное противодействие.
4. Правовой анализ законодательства о распространении вредной информации в разных странах.
5. Законодательство о защите государственной тайны в разных странах.
6. Степени секретности и грифы конфиденциальности различных стран.
7. Правоприменительная практика в области государственной тайны.
8. Правовая и организационная защита служебной тайны в разных странах.
9. Правовая и организационная защита коммерческой тайны в разных странах.
10. Правоприменительная практика в области коммерческой тайны.
11. Правовые проблемы защиты персональных данных.
12. Правовые основы контрразведывательной деятельности в разных странах.
13. Правовые основы разведывательной деятельности в разных странах.
14. Оперативно-розыскные, разведывательные и контрразведывательные мероприятия, затрагивающие тайну связи: правовые основы и правоприменительная практика.
15. Правовое обеспечение технического и экспортного контроля.
16. Нормативные документы ФСТЭК.
17. Защита информации при международном обмене.
18. Уголовное право разных стран в сфере информационной безопасности.
19. Развитие российского законодательства об интеллектуальной собственности.
20. Правовая защита интеллектуальной собственности в Китае.
21. Особенности авторского права в разных странах.
22. Правоприменительная практика в области защиты авторских прав в сети Интернет.
23. Авторское право и библиотеки (в том числе электронные).
24. Российские организации, управляющие правами авторов на коллективной основе.
25. Проблемы защиты авторских прав в сети Интернет.