Уп2013

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«29» 12 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ГОСУДАРСТВЕННАЯ И КОММЕРЧЕСКАЯ ТАЙНА

(наименование дисциплины)

Направление подготовки 10.03.01 Информационная безопасность

Профиль / программа подготовки Комплексная защита объектов информатизации

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
7	3/108	18	18		72	Зачет
Итого	3/108	18	18		72	Зачет

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины Целями освоения дисциплины «Государственная и коммерческая тайна» являются: знакомство обучающихся с актуальной, действующей на текущий момент нормативной базой в области информационной безопасности; рассмотрение основных направлений развития законодательства; обсуждение проблем правоприменения действующих норм в отношении защиты государственной и коммерческой тайны.

В курсе рассматривается вопросы формирования и правоприменения Федеральных законов в области защиты государственной и коммерческой тайны, вновь утвержденные документы ФСТЭК, базы документов, регламентирующих деятельность в области защиты коммерческих интересов организаций, сертификации и лицензирования в сфере деятельности с секретными и конфиденциальными сведениями.

Задачей изучения дисциплины «Государственная и коммерческая тайна» является изучение: - законодательства РФ в области защиты конфиденциальной информации и информации, составляющей государственную тайну; -текущее состояние законодательства в области защиты критических инфраструктур; - законодательство в области защиты национальной платежной системы; -законодательство в области защиты государственных информационных систем; -законодательное регулирование отдельных видов конфиденциальной информации; защита результатов интеллектуальной деятельности.

Курс предусматривает овладение навыками практической деятельности в области правоприменения существующего законодательства в области защиты информации, коммерческой и государственной тайны.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО БАКАЛАВРИАТА

Данная дисциплина относится к дисциплинам по выбору вариативной части Блока Б1 (код Б1.В.ДВ.1). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

Дисциплина изучается на четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсу «Актуальные вопросы информационного права» по направлению подготовки 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курса «Правоведение».

Курс тесно взаимосвязан и с другими дисциплинами данного цикла, например, с такими как «Организационное и правовое обеспечение информационной безопасности», «Правоохранительные органы», «Служба информационной безопасности на предприятии» и другими.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими общекультурными компетенциями:

ОК-5- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

общепрофессиональными компетенциями:

ОПК-7- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

профессиональными компетенциями:

ПК-4- способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) Знать: основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России. Знать понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности (ОК-5, ОПК-7, ПК-4);

2) Уметь: - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности сведений, составляющих государственную и коммерческую тайну; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач (ОК-5, ОПК-7, ПК-4);

3) Владеть:- навыками анализа информационной инфраструктуры информационной системы и ее безопасности; -пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; -применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну (ОК-5, ОПК-7, ПК-4).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей:

- способность разрабатывать основополагающие организационно-распорядительные документы для обеспечения безопасности сведений, составляющих государственную и коммерческую тайну.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
1.	Понятие информации в теории права и законодательстве. Роль информации в жизни общества.	6	2	1	1			4		1/50%	
2.	Понятие и значение коммерческой тайны. Определение информации, подлежащей защите	6	2	1	1			4		1/50%	
3.	Институт коммерческой тайны в системе информационной безопасности компании.	6	4	2	2			8		2/ 50%	
4.	Режим коммерческой тайны. Установление сроков защиты информации, составляющей коммерческую тайну.	6	6	1	1			4		1/50%	Рейтинг-контроль №1
5.	Правовое регулирование отношений в сфере формирования и использования коммерческой тайны.	6	6	1	1			4		1/50%	
6.	Правовое регулирование отношений в сфере организации защиты коммерческой тайны	6	8	2	2			8		2/50%	
7.	Правовое регулирование отношений в области охраны коммерческой тайны	6	10	2	2			8		2/50%	
8.	Юридическая ответственность за разглашение коммерческой тайны	6	12	2	2			8		2/50%	Рейтинг-контроль №2
9.	Правовое регулирование делопроизводства в сфере защиты коммерческой тайны	6	14	2	2			8		2/50%	
10	Правовой режим защиты государственной тайны..	6	16	1	1			4		1/50%	
11	Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.	6	16	1	1			4		1/50%	

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
12	Порядок доступа должностных лиц и граждан РФ к сведениям, составляющим государственную тайну	6	17	1	1			4		1/50%	
13	Перечень и содержание организационных мер, направленных на защиту государственной тайны.	6	17	1	1			4		1/50%	Рейтинг-контроль №3
Всего		6		18	18			72		18/ 50%	Зачет

Содержание дисциплины «Государственная и коммерческая тайна»

Раздел 1. Понятие информации в теории права и законодательстве. Роль информации в жизни общества. Информационное общество. Хартия Глобального информационного общества. Понятие социальной информации. Юридические свойства информации

Раздел 2. Понятие и значение коммерческой тайны. Определение информации, подлежащей защите, исходя из законодательства Российской Федерации, а также информации, которая может быть защищена созданием в компании режима коммерческой тайны; оптимизация защищаемых информационных потоков

Раздел 3. Институт коммерческой тайны в системе информационной безопасности компании. Законодательство Российской Федерации в сфере информации, информационных технологий и защиты информации. Информация, доступ к которой не может быть ограничен.

Раздел 4. Режим коммерческой тайны. Установление сроков защиты информации, составляющей коммерческую тайну. Определение времени и процедур оценки конфиденциальности конкретных документов компании. Установление порядка вывода документов из режима коммерческой тайны

Раздел 5. Правовое регулирование отношений в сфере формирования и использования коммерческой тайны. Понятие правового режима информации и его виды. Льготный правовой режим информации. Режим общественного достояния. Режим исключительных прав.

Раздел 6. Правовое регулирование отношений в сфере организации защиты коммерческой тайны. Защита коммерческой тайны. Комплексный и системный подход к защите информации. Организационные, кадровые, технические, режимные и иные мероприятия по защите коммерческой тайны

Раздел 7. Правовое регулирование отношений в области охраны коммерческой тайны Определение перечня должностей, при назначении на которые сотрудники будут допущены к коммерческой тайне компании.

Раздел 8. Юридическая ответственность за разглашение коммерческой тайны Виды юридической ответственности (уголовная, гражданско-правовая, дисциплинарная и иная) за разглашение коммерческой тайны, а также за незаконное получение этой информации.

Раздел 9. Правовое регулирование делопроизводства в сфере защиты коммерческой тайны Создание конфиденциального делопроизводства

Раздел 10. Правовой режим защиты государственной тайны. Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой

информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну.

Раздел 11. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне.

Раздел 12. Порядок доступа должностных лиц и граждан РФ к сведениям, составляющим государственную тайну

Раздел 13. Перечень и содержание организационных мер, направленных на защиту государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления бакалавра по направлению «Информационная безопасность».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

разбор конкретных ситуаций;

учебную дискуссию;

электронные средства обучения (слайд-лекции).

Лекционные занятия проводятся в аудитории, оборудованной проектором, что позволяет сочетать активные и интерактивные формы проведения занятий.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысления бакалаврами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП бакалавриата по направлению 10.03.01, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования не могут составлять более 45 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность бакалавра в различных видах учебной деятельности, степень сформированности у бакалавра общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1

1. Понятие «коммерческая тайна». Классификация коммерческих секретов
2. Законодательная и нормативная база Российской Федерации, регламентирующая и защищающая коммерческую тайну.
3. Зарубежный опыт правовой защиты коммерческой тайны.
4. Порядок отнесения информации к коммерческой тайне в организациях.
5. Каналы противоправного овладения коммерческой тайной.
6. Технические средства промышленного шпионажа.
7. Система защиты коммерческой тайны.
8. Персонал как фактор внутренней угрозы информационной безопасности.
9. Организация защищенного документооборота конфиденциальных документов.

10. Защита коммерческой информации при переговорах.
1. Режимы защиты информации.
2. Правовой режим государственной тайны.
3. Правовая охрана коммерческой и банковской тайны.
4. Порядок создания информационных технологий.
5. Применение информационных технологий.
6. Ограничения в применении информационных технологий.
7. Нарушение порядка применения информационных технологий.
8. История развития Интернет.
9. Подходы к определению Интернета и его составляющих.
10. Понятие информационной системы.
11. Средства обеспечения автоматизированных информационных систем и их технологий.
12. Понятие и общая характеристика юридической ответственности в Интернете.
13. Субъекты юридической ответственности интернет-отношений.
14. Виды юридической ответственности.
15. Законодательство Российской Федерации в области персональных данных. Принципы и условия обработки персональных данных.
16. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных.

Вопросы рейтинг-контроля №2

1. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных.
2. Право субъекта персональных данных.
3. Ответственность за нарушение требований законодательства о персональных данных.
4. Определение документа, электронного документа и других форм представления информации.
5. Структура электронного документа.
6. Электронный документооборот. Правовой статус электронной цифровой подписи.
7. Понятие средства массовой информации.
8. Формы распространения информации.
9. Электронные средства массовой информации.
10. Законодательство о средствах массовой информации
11. Государственный контроль и лицензирование средств массовой информации.
12. Понятие информационной безопасности.
13. Основные направления защиты информационной сферы.
14. Обеспечение защиты в информационной сфере.
15. Понятие ответственности в информационном праве.
16. Особенности информационных правонарушений и их выявления.
17. Виды и формы правонарушений в информационной сфере.
18. Как осуществляется допуск предприятий, учреждений и организаций к проведению работ, вязанных с использованием сведений, составляюший государственную тайну?
19. Что включает в себя правовой режим информации по закону «Об информации, информационных технологиях и о защите информации»?
20. Какие существуют основания для прекращения допуска гражданам и должностным лицам в доступе к государственной тайне?
21. На что имеет право обладатель информации, если иное не предусмотрено федеральными законами, согласно закону «Об информации, информационных технологиях и о защите информации»?

Вопросы рейтинг-контроля №3

1. Какие существуют основания для прекращения допуска гражданам и должностным лицам в доступе к государственной тайне?

2. На что имеет право обладатель информации, если иное не предусмотрено федеральными законами, согласно закону «Об информации, информационных технологиях и о защите информации»?
3. Какие существуют основания для отказа гражданам и должностным лицам в доступе к государственной тайне?
4. Какие существуют виды информационных систем согласно закону «Об информации, информационных технологиях и о защите информации»?
5. Какие государственные структуры относятся к органам защиты государственной тайны?
6. На что направлены меры по защите информации согласно закону «Об информации, информационных технологиях и о защите информации»?
7. В каких случаях сведения, содержащие государственную тайну подлежат рассекречиванию?
8. Что обязан обеспечить обладатель информации и оператор информационной системы (в случаях, установленных законодательством Российской Федерации) согласно закону «Об информации, информационных технологиях и о защите информации»?
9. Какую информацию должны содержать реквизиты носители сведений, содержащих государственную тайну?
10. Какие существуют грифы секретности и формы допуска к государственной тайне?
11. Дайте краткий перечень сведений, которые могут составлять государственную тайну.
12. Что обычно является основными лицензионными требованиями и условиями?
13. Каким образом приостанавливается и аннулируется лицензия?
14. Назовите основные виды деятельности по обеспечению информационной безопасности, подлежащие лицензированию.

Перечень вопросов к зачету (промежуточной аттестации по итогам освоения дисциплины):

1. Понятие «коммерческая тайна». Классификация коммерческих секретов
2. Законодательная и нормативная база Российской Федерации, регламентирующая и защищающая коммерческую тайну.
3. Зарубежный опыт правовой защиты коммерческой тайны.
4. Порядок отнесения информации к коммерческой тайне в организациях.
5. Каналы противоправного овладения коммерческой тайной.
6. Технические средства промышленного шпионажа.
7. Система защиты коммерческой тайны.
8. Персонал как фактор внутренней угрозы информационной безопасности.
9. Организация защищенного документооборота конфиденциальных документов.
10. Защита коммерческой информации при переговорах.
11. Режимы защиты информации.
12. Правовой режим государственной тайны.
13. Правовая охрана коммерческой и банковской тайны.
14. Порядок создания информационных технологий.
15. Применение информационных технологий.
16. Ограничения в применении информационных технологий.
17. Нарушение порядка применения информационных технологий.
18. История развития Интернет.
19. Подходы к определению Интернета и его составляющих.
20. Понятие информационной системы.
21. Средства обеспечения автоматизированных информационных систем и их технологий.
22. Понятие и общая характеристика юридической ответственности в Интернете.
23. Субъекты юридической ответственности интернет-отношений.
24. Виды юридической ответственности.
25. Законодательство Российской Федерации в области персональных данных. Принципы и условия обработки персональных данных.

26. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных.
27. Право субъекта персональных данных.
28. Ответственность за нарушение требований законодательства о персональных данных.
29. Определение документа, электронного документа и других форм представления информации.
30. Структура электронного документа.
31. Электронный документооборот. Правовой статус электронной цифровой подписи.
32. Понятие средства массовой информации.
33. Формы распространения информации.
34. Электронные средства массовой информации.
35. Законодательство о средствах массовой информации
36. Государственный контроль и лицензирование средств массовой информации.
37. Понятие информационной безопасности.
38. Основные направления защиты информационной сферы.
39. Обеспечение защиты в информационной сфере.
40. Понятие ответственности в информационном праве.
41. Особенности информационных правонарушений и их выявления.
42. Виды и формы правонарушений в информационной сфере.
43. Как осуществляется допуск предприятий, учреждений и организаций к проведению работ, вязанных с использованием сведений, составляющий государственную тайну?
44. Что включает в себя правовой режим информации по закону «Об информации, информационных технологиях и о защите информации»?
45. Какие существуют основания для прекращения допуска гражданам и должностным лицам в доступе к государственной тайне?
46. На что имеет право обладатель информации, если иное не предусмотрено федеральными законами, согласно закону «Об информации, информационных технологиях и о защите информации»?
47. Какие существуют основания для отказа гражданам и должностным лицам в доступе к государственной тайне?
48. Какие существуют виды информационных систем согласно закону «Об информации, информационных технологиях и о защите информации»?
49. Какие государственные структуры относятся к органам защиты государственной тайны?
50. На что направлены меры по защите информации согласно закону «Об информации, информационных технологиях и о защите информации»?
51. В каких случаях сведения, содержащие государственную тайну подлежат рассекречиванию?
52. Что обязан обеспечить обладатель информации и оператор информационной системы (в случаях, установленных законодательством Российской Федерации) согласно закону «Об информации, информационных технологиях и о защите информации»?
53. Какую информацию должны содержать реквизиты носители сведений, содержащих государственную тайну?
54. Какие существуют грифы секретности и формы допуска к государственной тайне?
55. Дайте краткий перечень сведений, которые могут составлять государственную тайну.
56. Что обычно является основными лицензионными требованиями и условиями?
57. Каким образом приостанавливается и аннулируется лицензия?
58. Назовите основные виды деятельности по обеспечению информационной безопасности, подлежащие лицензированию.

Темы для рефератов:

- Государственное регулирование в области информации, информатизации и защиты информации.
- Информационные технологии, информационные системы и информационные сети.
- Основные требования по защите информации.

- Государственные секреты.
- Служебная тайна как объект гражданских прав.
- Основы управления интеллектуальной собственностью
- Понятие и объекты авторского права
- Правовая охрана изобретений
- Системы патентования и выдачи патентов
- Вопросы зарубежного патентования изобретения
- Понятие недобросовестной конкуренции.
- Оценка стоимости объектов интеллектуальной собственности
- Информационное общество и право, информационно-правовое знание. Окинавская Хартия. Роль информационного права в обеспечении национальной безопасности. Основные задачи государственной информационной политики РФ.
- Общие (содержательность и защищённость) и специальные (легитимность) свойства информации, принципиальные для правового регулирования информационных отношений.
- Правовой режим информационных систем, информационных технологий и средств их обеспечения. Государственная политика в области их создания.
- Проблемы и способы международно-правового обеспечения глобального информационного обмена.
- Концепция гражданского оборота результатов интеллектуальной деятельности военного, специального и двойного назначения.
- Институт тайны как универсальный способ правовой защиты информации ограниченного доступа.
- Модели правового регулирования информационных отношений в области коммерческой тайны.
- Модели правового регулирования применения электронно-цифровой подписи в России. Правовые свойства (аутентичность, легальность, верифицируемость) информации.
- Особенности и модели правового регулирования применения электронной подписи за рубежом.
- Особенности правового регулирования информационных отношений в области государственной тайны.
- Информационные аспекты интеллектуальной собственности. Особенности правового регулирования информационных отношений институтом патентного права.

Темы практических занятия:

- Отнесение сведений к различным видам конфиденциальной информации
- Закрепление права предприятия на защиту информации в нормативных документах
- Организация допуска и доступа персонала к конфиденциальной информации
- Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации
- Основы работы с персоналом предприятия. Обеспечение защиты информации при работе с кадрами
- Организация аналитической работы в области защиты информации на предприятии. Основные этапы аналитической работы
- Корпоративные политики информационной безопасности
- Планирование системы информационной безопасности предприятия и разработка политик информационной безопасности
- Разработка опросных листов и анализ соответствия стандартам информационной безопасности.
- Методы оценки информационной безопасности
- Расследование инцидентов информационной безопасности

Список вопросов для проработки в рамках самостоятельной работы студентов:

- Правовая защита коммерческой тайны
- Информация, составляющая коммерческую тайну
- Разделение коммерческой тайны на группы
- Сроки защиты информации, составляющей коммерческую тайну
- Информационное законодательство
- Правовые режимы информации
- Определение времени и процедур оценки конфиденциальности конкретных документов компании. Установление порядка вывода документов из режима коммерческой тайны;
- Обязательства сотрудников по сохранению коммерческой тайны компании. Где прописать – в трудовом договоре или в отдельном документе. Обязан ли сотрудник хранить коммерческие секреты компании после увольнения;
- Особенности включения в режим коммерческой тайны информации, представленной в электронном виде;
- Защита коммерческой тайны. Комплексный и системный подход к защите информации. - - Организационные, кадровые, технические, режимные и иные мероприятия по защите коммерческой тайны;
- Правое регулирование отношений в сфере обеспечения информационной безопасности

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: ISBN 978-5-369-01378-6, Режим доступа: http://znanium.com/catalog.php?bookinfo=474838
2. Правовое обеспечение государственного и муниципального управления: Учебное пособие / С.Н. Кленов и др. - М.: НИЦ ИНФРА-М, 2015. - 268 с. ISBN 978-5-16-010110-1. Режим доступа: http://znanium.com/catalog.php?bookinfo=471455
3. Коммерческое (предпринимательское) право: Учебник / В.Ф. Попондопуло. - 3-е изд., перераб. и доп. - М.: НОРМА, 2013. - 800 с.: ISBN 978-5-468-00262-9 Режим доступа: http://znanium.com/catalog.php?bookinfo=414912
4. Баиллы, П. Н. Информационная безопасность и защита информации : Учебник / П. Н. Баиллы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: http://znanium.com/catalog.php?bookinfo=405000

б) Дополнительная литература:

1. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере / Н. Н. Куняев. - М.: Логос, 2010. - 348 с. - ISBN 978-5-98704-513-8. Режим доступа: http://znanium.com/catalog.php?bookinfo=469026
2. Братановский, С. Н. Специальные правовые режимы информации / С. Н. Братановский. - Саратов: «Научная книга», 2010. - 172 с. - Режим доступа: http://znanium.com/catalog.php?bookinfo=416111
3. Файман, Ольга Игоревна. Правовое обеспечение информационной безопасности : учебное пособие / О. И. Файман, В. А. Граник, М. Ю. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир (ВлГУ), 2010 .— 86 с. ISBN 978-5-9984-0020-9

в) Периодические издания

1. ООО "Издательский Дом "ИНТЕЛЛЕКТУАЛЬНАЯ ПРЕССА" журнал «Интеллектуальная собственность. Авторское право и смежные права». Режим доступа: http://superpressa.ru/index.php?option=com_content&view=article&id=357&Itemid=111;
2. Журнал «Право интеллектуальной собственности» Издательская группа «Юрист», г. Москва. Режим доступа: http://pravois.ru/

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
3. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокрост 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Тельный А.В.
(ФИО, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»

к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 7 от 28.12.16 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Протокол № 4 от 28.12.16 года

Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017/18 учебный год

Протокол заседания кафедры № 1 от 28.08.17 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Приложение

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт _____

Кафедра _____

Актуализированная
рабочая программа
рассмотрена и одобрена
на заседании кафедры
протокол № ____ от ____ 20__г.

Заведующий кафедрой

_____
(подпись, ФИО)

Актуализация рабочей программы дисциплины

_____
(наименование дисциплины)

Направление подготовки

Профиль/программа подготовки

Уровень высшего образования

Форма обучения

Владимир 20__

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: _____
(подпись, должность, ФИО)

а) основная литература: _____

б) дополнительная литература: _____

в) периодические издания: _____

в) интернет-ресурсы: _____