Уп2015

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

Организационно-правовые механизмы обеспечения информационной безопасности

Направление подготовки 10.04.01 Информационная безопасность

Программа подготовки _____

Уровень высшего образования магистратура

Форма обучения очная

Семестр	Трудоем-кость зач. ед./час.	Лек-ций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
3	2/72	18	18		36	Зачет
Итого	2/72	18	18		36	Зачет

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 2Информационная безопасность». Целью освоения дисциплины является углубленное изучение магистрантами сведений по организационному и правовому обеспечению информационной безопасности. При изучении курса происходит формирование и уяснение магистрантами значения норм права, регулирующих поиск, получение, производство и распространение информации по действующему законодательству Российской Федерации. В курсе изучаются правовые средства и организационные механизмы, используемые наряду с техническими для обеспечения защиты информационных прав и свобод.

Задачами изучения дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности» является предоставление знаний по следующим тематикам:

- угрозы информационной безопасности объекта; - организация и ведение секретного и конфиденциального делопроизводства; - организация службы безопасности объекта; - подбор и работа с кадрами в сфере информационной безопасности; - организация охраны объектов; - ознакомление с важнейшими источниками информационного права Российской Федерации; - усвоение основополагающих нормативно-правовых актов; - умение работать с нормативно-правовой базой и применять в конкретных практических ситуациях; - приобретение навыка составления основных документов (договоров, положений, локальных актов и др.), используемых в сфере информационной безопасности; - освоение предусмотренных законодательством способов защиты информационных прав и свобод.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО МАГИСТРАТУРЫ

Данная дисциплина относится к обязательным дисциплинам вариативной части Блока Б1 (код Б1.В.ОД.3). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий.

Дисциплина изучается на 1 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курса «Правоведение», «Правовое обеспечение информационной безопасности» или аналогичных, в соответствии с программой подготовки бакалавров в следующих или смежных областях знаний: - информационная безопасность; -энергетика, энергетическое машиностроение и электротехника; -авиационная и ракетно-космическая техника; -фотоника, приборостроение, -оптические и биотехнические системы и технологии; -электронная техника, радиотехника и связь; -автоматика и управление; -информатика и вычислительная техника; -физико-технические науки и технологии; -управление в технических системах.

Курс тесно взаимосвязан с другими дисциплинами. Он может быть полезен для изучения таких дисциплин как «Управление информационной безопасностью», «Защищённые информационные системы», «Методы и средства защиты информации в системах электронного документооборота» и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование следующих профессиональных компетенций, которыми должен обладать выпускник:

ПК-10 – способностью проводить аттестацию объектов информатизации по требованиям безопасности информации;

ПК-14 – способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-15 – способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

ПК-16 – способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** - методологию организационной защиты информации, ее современные проблемы и терминологию; - основные руководящие документы по обеспечению режима и секретности на объекте; - типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; - основные документы, регламентирующую организационную безопасность на объекте; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; - правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; - правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; принципы и методы организационной защиты информации; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем (ПК-10; ПК-14; ПК-15);

2) ***Уметь:*** - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - пользоваться нормативными документами по защите информации; - оценивать состояние организационной защиты информации на объекте; - определять рациональные меры по обеспечению организационной защите на объекте; - организовать работу с персоналом с секретной (конфиденциальной) информацией; - формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости; - самостоятельно осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности (ПК-14; ПК-15; ПК-16);

3) ***Владеть:*** - навыками работы с нормативными правовыми актами; - профессиональной терминологией; навыками формирования методических и нормативных документов, тех.документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; - навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы; навыками управления информационной безопасностью простых объектов (ПК-10; ПК-14; ПК-15; ПК-16).

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

- способность прогнозировать угрозы утечки информации по организационному каналу;
- способность оценивать состояние информационной безопасности объекта с учетом действующих нормативных и методических документов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 часа.

№ 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 промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1	Информационное законодательство и его система в РФ. Основы информационного законодательства РФ	3	1-2	2	2			4		2/50%	
2	Права на результаты интеллектуальной деятельности и средства индивидуализации. Авторское право. Права, смежные с авторскими	3	3-4	2	2			4		2/50%	
3	Патентное право. Право на топологии интегральных микросхем.	3	5-6	2	2			4		1/25%	Рейтинг-контроль №1
4	Право на секрет производства (ноу-хау). Права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий.	3	7-8	2	2			4		1/25%	
5	Право использования результатов интеллектуальной деятельности в составе единой технологии.	3	9-10	2	2			4		2/50%	
6	Организационные основы защиты конфиденциальной информации на предприятии.	3	11-12	2	2			4		2/50%	Рейтинг-контроль №2
7	Организация КПиОР режимов на предприятии.	3	13-14	2	2			4		1/25%	
8	Концепция построения системы безопасности предприятия. Правовые основы деятельности СБ предприятия	3	15-16	2	2			4		2/50%	

№ 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 промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
9	Структура и функции службы безопасности предприятия.	3	17-18	2	2			4		1/25%	Рейтинг-контроль №3
Всего				18	18			36		14/39%	Зачет

Содержание дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности»

Раздел 1. Информационное законодательство и его система в Российской Федерации. Основы информационного законодательства Российской Федерации. Структура информационного законодательства. Защита информации с ограниченным доступом. Понятие и виды информации, защищаемой законодательством Российской Федерации. Правовое обеспечение защиты государственной тайны, коммерческой тайны, служебной тайны, персональных данных, профессиональной тайны.

Раздел 2. Права на результаты интеллектуальной деятельности и средства индивидуализации. Авторское право. Права, смежные с авторскими.

Раздел 3. Патентное право. Право на топологии интегральных микросхем.

Раздел 4. Право на секрет производства (ноу-хау). Права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий.

Раздел 5. Право использования результатов интеллектуальной деятельности в составе единой технологии.

Раздел 6. Организационные основы защиты конфиденциальной информации на предприятии. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.

Раздел 7. Организация внутриобъектового и пропускного режимов на предприятии. Планирование мероприятий по организационной защите информации на предприятии

Раздел 8. Концепция построения системы безопасности предприятия. Правовые основы деятельности службы безопасности предприятия.

Раздел 9. Структура и функции службы безопасности предприятия. Подразделения службы безопасности предприятия. Управление службой безопасности предприятия (СБП).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности» предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления магистра в области информационной безопасности.

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 магистрантами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, 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 по направлению подготовки 10.04.01 «Информационная безопасность» 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 МАГИСТРАНТОВ

Для промежуточной аттестации предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность магистранта в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1

- Основы законодательства Российской Федерации в области информационной безопасности и защиты информации
- Понятие и виды информации, защищаемой законодательством Российской Федерации
- Государственная тайна как особый вид защищаемой информации
- Система защиты государственной тайны
- Организационные и технические способы защиты государственной тайны
- Конфиденциальная информация и ее защита

- Правовое обеспечение защиты коммерческой тайны
- Правовое обеспечение защиты служебной и профессиональной тайны
- Становление международного законодательства и национального законодательства различных стран в области защиты персональных данных
- Законодательство РФ в области защиты персональных данных
- Нормативно-распорядительные документы, созданные во исполнение закона № 152
- Организационно-процедурный уровень защиты персональных данных
- Порядок проведения обследования ИСПДн
- Порядок проведения классификации ИСПДн
- Определение способов понижения требований по защите персональных данных

Вопросы рейтинг-контроля №2

- Защита персональных данных от утечки по техническим каналам
- Защита персональных данных от несанкционированного доступа и неправомерных действий
- Обеспечение обмена персональными данными
- Подготовка к проверкам законности обработки персональных данных
- Основы законодательства в области защиты прав на результаты интеллектуальной деятельности
- Правовое регулирование отношений в сфере авторского права
- Правовое регулирование отношений в сфере защиты прав, смежных с авторскими
- Правовое регулирование отношений в сфере патентного права
- Право на секрет производства (ноу-хау)
- Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий
- Право использования результатов интеллектуальной деятельности в составе единой технологии.
- Основные обязанности органов законодательной власти в сфере ИБ
- Основные обязанности органов исполнительной власти в сфере ИБ
- Какие информационные ресурсы предприятия не могут быть отнесены к коммерческой тайне?
- Назовите основные направления работы по защите конфиденциальной информации на предприятии.

Вопросы рейтинг-контроля №3

- Основные обязанности органов исполнительной власти в сфере ИБ
- Какие информационные ресурсы предприятия не могут быть отнесены к коммерческой тайне?
- Назовите основные направления работы по защите конфиденциальной информации на предприятии.
- Какие основные положения должно содержать техническое задание на разработку системы защиты конфиденциальной информации на предприятии?
- Назовите основные функции службы безопасности на предприятии.
- Назовите вспомогательные функции службы безопасности на предприятии.
- Назовите основные функции подразделения по защите информации на предприятии.
- Типовая структура (основные подразделения) службы безопасности на предприятии.
- Какие могут быть варианты структуры службы безопасности, предприятия и какова подчиненность подразделений службы безопасности?
- Какие предъявляются требования к уровню подготовки руководителей службы безопасности предприятия?
- Назовите основные функции подразделения по охране и режиму на предприятии.

- Назовите основные функции подразделения по ИТЗИ на предприятии.
- Назовите основные функции информационно-аналитического подразделения на предприятии.
- Назовите основные функции режимно-секретного подразделения на предприятии.
- Какие виды деятельности по защите информации на предприятии подлежат лицензированию?

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

1. Основы законодательства Российской Федерации в области информационной безопасности и защиты информации
2. Понятие и виды информации, защищаемой законодательством Российской Федерации
3. Государственная тайна как особый вид защищаемой информации
4. Система защиты государственной тайны
5. Организационные и технические способы защиты государственной тайны
6. Конфиденциальная информация и ее защита
7. Правовое обеспечение защиты коммерческой тайны
8. Правовое обеспечение защиты служебной и профессиональной тайны
9. Становление международного законодательства и национального законодательства различных стран в области защиты персональных данных
10. Законодательство РФ в области защиты персональных данных
11. Нормативно-распорядительные документы, созданные во исполнение закона № 152
12. Организационно-процедурный уровень защиты персональных данных
13. Порядок проведения обследования ИСПДн
14. Порядок проведения классификации ИСПДн
15. Определение способов понижения требований по защите персональных данных
16. Защита персональных данных от утечки по техническим каналам
17. Защита персональных данных от несанкционированного доступа и неправомерных действий
18. Обеспечение обмена персональными данными
19. Подготовка к проверкам законности обработки персональных данных
20. Основы законодательства в области защиты прав на результаты интеллектуальной деятельности
21. Правовое регулирование отношений в сфере авторского права
22. Правовое регулирование отношений в сфере защиты прав, смежных с авторскими
23. Правовое регулирование отношений в сфере патентного права
24. Право на секрет производства (ноу-хау)
25. Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий
26. Право использования результатов интеллектуальной деятельности в составе единой технологии.
27. Основные обязанности органов законодательной власти в сфере ИБ
28. Основные обязанности органов исполнительной власти в сфере ИБ
29. Какие информационные ресурсы предприятия не могут быть отнесены к коммерческой тайне?
30. Назовите основные направления работы по защите конфиденциальной информации на предприятии.
31. Какие основные положения должно содержать техническое задание на разработку системы защиты конфиденциальной информации на предприятии?
32. Назовите основные функции службы безопасности на предприятии.
33. Назовите вспомогательные функции службы безопасности на предприятии.
34. Назовите основные функции подразделения по защите информации на предприятии.
35. Типовая структура (основные подразделения) службы безопасности на предприятии.

36. Какие могут быть варианты структуры службы безопасности, предприятия и какова подчиненность подразделений службы безопасности?
37. Какие предъявляются требования к уровню подготовки руководителей службы безопасности предприятия?
38. Назовите основные функции подразделения по охране и режиму на предприятии.
39. Назовите основные функции подразделения по ИТЗИ на предприятии.
40. Назовите основные функции информационно-аналитического подразделения на предприятии.
41. Назовите основные функции режимно-секретного подразделения на предприятии.
42. Какие виды деятельности по защите информации на предприятии подлежат лицензированию?

Темы практических занятий:

Практическое занятие №1-№2 Изучение «Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» (утверждена постановлением правительства РФ от 06.02.2010 №63)

Практическое занятие №3-№4 Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации на предприятии

Практическое занятие №5 Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации при ее обработке на средствах вычислительной техники

Практическое занятие №6-№7 Изучение порядка аттестации объектов информатизации

Практическое занятие №8 Изучение форм и порядка заполнения документации по результатам аттестации объектов информатизации

Практическое занятие №9 Изучение порядка проведения организационных и технических мероприятий по ТЗИ на ОИ

Вопросы и задания к самостоятельной работе магистрантов

- Дайте характеристику основных документов ФСТЭК и «Общих критериев оценки безопасности ИТ ISO/IEC 15408» в части ЗИ.
- Законодательство в области международного информационного обмена и компьютерных преступлений
- Международные соглашения по предупреждению компьютерных преступлений
- Международный правовой опыт обеспечения безопасности негосударственных объектов экономики
- Законодательство зарубежных стран в области защиты интеллектуальной собственности
- Нормативно-правовое регулирование профессиональной тайны
- Служебная тайна и ее защита
- Правовая защита персональных данных
- Основные положения Закона «О персональных данных»
- Требования к обработке персональных данных
- Ответственность за нарушение работы с персональными данными
- Международное законодательство и национальное законодательство зарубежных стран о защите персональных данных
- Персональные данные в системе документооборота предприятия
- Авторское право
- Права, смежные с авторскими
- Патентное право
- Право на секрет производства
- Право использования результатов интеллектуальной деятельности в составе единой технологии

- Принципы государственной политики обеспечения информационной безопасности
- Ключевые проблемы информационной безопасности государства
- Информационное общество – новый этап развития человечества
- Информация – фактор существования и развития общества
- Проблема практического применения ФЗ «Об информации, информационных технологиях и о защите информации»
- Законодательство в области информационно-психологической безопасности.
- Перечислите основные характеристики процесса ЗИ
- Что понимают под устойчивостью системы ЗИ?
- Что понимают и чем обеспечивается непрерывность решения задач ЗИ?
- Что принято понимать под служебной или коммерческой тайной?
- Перечислите степень секретности (гриф), который могут иметь сведения, составляющие служебную или коммерческую тайну предприятия
- Из каких этапов состоит работа по формированию Перечня сведений, составляющих служебную или коммерческую тайну?
- Какими документами необходимо руководствоваться при составлении предварительного Перечня сведений, составляющих служебную или коммерческую тайну?
- По каким аспектам экспертная комиссия предприятия рассматривает предварительный перечень конфиденциальных сведений?
- Как определяется возможный ущерб, наступающий в результате несанкционированного распространения сведений, включаемых в обобщенный Перечень?
- Каким образом принимается и как оформляется решения о включении сведений в окончательный вариант Перечня?
- Приведите типовой примерный перечень сведений, составляющих служебную или коммерческую тайну организации.
- Для чего необходимо формировать список организаций и частных лиц, которые могут быть заинтересованы в доступе к охраняемой информации?
- Каковы критерии отнесения организаций и частных лиц к потенциальным злоумышленникам (которые могут быть заинтересованы в доступе к охраняемой информации)?
- Что должна включать в себя в обобщенном виде Концепция обеспечения ИБ?
- Что понимают под Политикой ИБ?
- Назовите причины необходимости разработки Концепции обеспечения ИБ на каждом предприятии.
- Перечислите основные элементы Концепции обеспечения ИБ на каждом предприятии.
- Какую информацию включает в себя раздел общих положений по обеспечению ИБ Концепции?
- Зачем необходим раздел с основными понятиями концепции?
- Прокомментируйте разделы Концепции, касающиеся определения состава потенциально существующих угроз безопасности информации, описания каналов вторжения в ИС, требований к системе обеспечения ИБ и методов оценки ее эффективности.
- Проанализируйте разделы Концепции: долгосрочная программа развития системы ИБ; организация и программа подготовки кадров по вопросам ИБ; организация использования системы ЗИ; кадровое обеспечение ЗИ; условия, необходимые для надежного обеспечения ЗИ.

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. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.
3. Региональная и национальная безопасность: Учебное пособие / А.Б. Логунов. - 3-е изд., перераб. и доп. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2014. - 457 с.: ISBN 978-5-9558-0310-4, Режим доступа: http://znanium.com/catalog.php?bookinfo=406872
4. Информационное право: / отв. ред. И.М. Рассолов. - М. : Проспект, 2015. - http://www.studentlibrary.ru/book/ISBN9785392173747.html.
5. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. ISBN 978-5-8199-0411-4 Режим доступа: http://znanium.com/catalog.php?bookinfo=402686
6. Современные технологии и технические средства информатизации: Учебник / О.В. Шишов. - М.: НИЦ Инфра-М, 2012. - 462 с.: ISBN 978-5-16-005369-1 Режим доступа: http://znanium.com/catalog.php?bookinfo=263337

б) Дополнительная литература:

1. Охранные подразделения / Ворона В.А., Тихонов В.А. - Вып. 6. - М. : Горячая линия - Телеком, 2012. http://www.studentlibrary.ru/book/ISBN9785991202398.html
2. Проверка и оценка деятельности по управлению информационной безопасностью Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. http://www.studentlibrary.ru/book/ISBN9785991202756.html
3. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с.: ISBN 978-5-369-01379-3 Режим доступа: http://znanium.com/catalog.php?bookinfo=476047
4. Файман, О.И. Правовое обеспечение информационной безопасности : учебное пособие / О. И. Файман, В. А. Граник, М. Ю. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2010 .— 86 с. ISBN 978-5-9984-0020-9
5. Микрюков Т.В. Службы экономической безопасности и их функции / Вестник Удмуртского университета. Серия 2. Экономика и право, Вып. 1, 2010 Режим доступа: http://znanium.com/catalog.php?bookinfo=525174
6. Кузнецов, И. Н. Бизнес-безопасность / И. Н. Кузнецов. - 3-е изд. - М.: Дашков и К, 2013. - 416 с. - ISBN 978-5-394-01438-3. Режим доступа: http://znanium.com/catalog.php?bookinfo=430343

в) Периодические издания:

1. Информационно-методический журнал «Защита информации. Конфидент» http://sec4all.net/konfj-5_03.html
2. Журнал "Алгоритм безопасности» – Режим доступа: http://www.algoritm.org/index.php;
3. Электронный научный журнал «Проблемы безопасности» – Режим доступа: http://www.pb.littera-n.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/

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 «Прокруст 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 10.04.01 «Информационная безопасность»

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 28.12.2016 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.04.01 «Информационная безопасность»

Протокол № 4 от 28.12.2016 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: _____