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

СТАНДАРТИЗАЦИЯ И СЕРТИФИКАЦИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(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)
3	3/108	18	-	36	54	Зачет
Итого	3/108	18	-	36	54	Зачет

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины Целями освоения дисциплины «Стандартизация и сертификация в информационной безопасности» являются: знакомство обучающихся с актуальной, действующей на текущий момент нормативной базой в области информационной безопасности и действующих стандартов по информационной безопасности.

Задачей изучения дисциплины «Стандартизация и сертификация в информационной безопасности» является изучение процедур аттестации объектов информатизации и информационных систем; лицензирования деятельности в области информационной безопасности; проведения категорирования объектов информатизации, специальных проверок и обследований; сертификация в сфере защиты информации, действующие стандарты в области информационной безопасности.

В курсе рассматривается нормативная база и правоприменение Федеральных законов в области проведения сертификации, лицензирования и аттестации объектов информатизации при деятельности, связанной с секретными и конфиденциальными сведениями. В курсе рассматриваются современные действующие международные и отечественные стандарты в области обеспечения защиты информации в информационных системах. 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.4). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

Дисциплина изучается на втором курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсу «Информатика», «Документоведение» 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, 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 общепрофессиональными компетенциями:

ОПК-5 – способностью использовать нормативные правовые акты в профессиональной деятельности;

профессиональными компетенциями:

ПК-8 – способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.

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; 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 (ОПК-5; ПК-8);

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; уметь проводить процедуры аттестации, категорирования объектов информатизации; уметь пользоваться научно- технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме (ОПК-5; ПК-8);

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; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну (ОПК-5; ПК-8).

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

- способность проводить аттестацию и категорирование объектов информатизации и 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 единиц, 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 промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
1	Законодательно-правовое обеспечение информационной безопасности Российской Федерации.	3	1-2	2				6		1(50%)	
2	Правовая основа системы стандартизации, лицензирования и сертификации в РФ.	3	3-4	2		8		6		4(40%)	
3	Лицензирующие органы в области защиты информации.	3	5-6	2		4		6		3(50%)	Рейтинг - контроль №1
4	Лицензирование в области защиты информации.	3	7-8	2		4		6		3(50%)	
5	Аттестация объектов информации. Проведение специальных проверок, специальных обследований и специальных исследований.	3	9-10	2		4		6		3(50%)	
6	Сертификация в области защиты информации.	3	11-12	2		4		6		3(50%)	Рейтинг - контроль №2
7	Категорирование защищаемой информации и объектов информатизации.	3	13-14	2		4		6		3(50%)	
8	Стандартизация в сфере информационной безопасности. Отечественные и зарубежные стандарты в области информационной безопасности.	3	15-16	2		4		6		3(50%)	
9	Ответственность за нарушения законодательства в сфере нарушений лицензирования и сертификации в РФ.	3	17-18	2		4		6		3(50%)	Рейтинг - контроль №3
Всего		3		18		36		54		26(48%)	Зачет

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

- Укажите основные элементы организационной основы системы обеспечения информационной безопасности РФ.
- Какие виды деятельности в области защиты информации подлежат лицензированию?
- Порядок лицензирования, срок действия лицензии.
- Организационная структура системы сертификации в области защиты конфиденциальной информации.
- При каких организациях созданы системы сертификации в РФ?
- Порядок и требования при осуществлении сертификации средств защиты информации.
- В каких случаях сертификация носит добровольный характер?
- Кем устанавливаются формы сертификата и знака соответствия?

- Какие виды деятельности, связанные с защитой информации на предприятии подлежат лицензированию со стороны ФСТЭК?
- Какие виды деятельности, связанные с защитой информации на предприятии подлежат лицензированию со стороны ФСБ?
- Назовите основные лицензионные требования для вида деятельности «Разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем»
- Назовите основные лицензионные требования для вида деятельности «Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации»

Вопросы рейтинг-контроля №2:

- Назовите основные лицензионные требования для вида деятельности по выявлению электронных устройств, предназначенных для негласного получения информации
- Назовите основные лицензионные требования для деятельности, связанной с защитой государственной тайны
- Назовите основные лицензионные требования для деятельности по разработке и производству средств защиты конфиденциальной информации
- Основные положения стандарта ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
- Основные положения стандарта ISO/IEC 27002 — Сейчас: ISO/IEC 17799:2005. «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.
- Основные положения стандарта ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.

Вопросы рейтинг-контроля №3:

- Основные положения стандарта ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.
- Основные положения стандарта ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- Основные положения стандарта ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
- Основные положения стандарта ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
- Основные положения стандарта ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
- Основные положения стандарта ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью».

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

1. Укажите основные элементы организационной основы системы обеспечения информационной безопасности РФ.
2. Какие виды деятельности в области защиты информации подлежат лицензированию?
3. Порядок лицензирования, срок действия лицензии.
4. Организационная структура системы сертификации в области защиты конфиденциальной информации.
5. При каких организациях созданы системы сертификации в РФ?

6. Порядок и требования при осуществлении сертификации средств защиты информации.
7. В каких случаях сертификация носит добровольный характер?
8. Кем устанавливаются формы сертификата и знака соответствия?
9. Какие виды деятельности, связанные с защитой информации на предприятии подлежат лицензированию со стороны ФСТЭК?
10. Какие виды деятельности, связанные с защитой информации на предприятии подлежат лицензированию со стороны ФСБ?
11. Назовите основные лицензионные требования для вида деятельности «Разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем»
12. Назовите основные лицензионные требования для вида деятельности «Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации»
13. Назовите основные лицензионные требования для вида деятельности по выявлению электронных устройств, предназначенных для негласного получения информации
14. Назовите основные лицензионные требования для деятельности, связанной с защитой государственной тайны
15. Назовите основные лицензионные требования для деятельности по разработке и производству средств защиты конфиденциальной информации
16. Основные положения стандарта ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
17. Основные положения стандарта ISO/IEC 27002 — Сейчас: ISO/IEC 17799:2005. «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.
18. Основные положения стандарта ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.
19. Основные положения стандарта ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
20. Основные положения стандарта ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
21. Основные положения стандарта ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
22. Основные положения стандарта ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
23. Основные положения стандарта ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью».

Темы лабораторных работ

Лабораторная работа 1. Практика правоприменения и вводные задачи при лицензировании деятельности в области обеспечения ИБ;

Лабораторная работа 2. Практика правоприменения и вводные задачи при прохождении сертификации при обеспечении информационной безопасности;

Лабораторная работа 3. Вводные задачи при определении мер ответственности за нарушения в области лицензирования и сертификации при обеспечении информационной безопасности;

Лабораторная работа 4. Порядок аттестации объектов информатизации.

Лабораторная работа 5. Изучение форм и порядка заполнения документации по результатам аттестации объектов информатизации

Лабораторная работа 6. Изучение порядка проведения организационных и технических мероприятий по ТЗИ на ОИ

Вопросы и задания для самостоятельной работы студентов:

1. Изучение «Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» (утверждена постановлением правительства РФ от 06.02.2010 №63);
2. Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации на предприятии;
3. Изучение требований типовых инструкций по обеспечению сохранности конфиденциальной информации при ее обработке на средствах вычислительной техники;
4. Изучение порядка аттестации объектов информатизации;
5. Изучение форм и порядка заполнения документации по результатам аттестации объектов информатизации;
6. Изучение порядка проведения организационных и технических мероприятий по ТЗИ на ОИ;
7. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) -2001;
8. Изучение документа ФСТЭК РФ P_1994.11.25. Положение по аттестации объектов информатизации по требованиям безопасности информации;
9. Изучение документа ФСТЭК РФ P_2010.08.31_489. Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования;
10. Изучение документа ФСТЭК РФ приказ №17 от 11.02.2013 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;
11. Изучение документа ФСТЭК РФ RD_1992.03.30_1. Руководящий документ автоматизированные системы. Защита от несанкционированного доступа к информации классификация автоматизированных систем и требования по защите информации;
12. Изучение документа ФСТЭК РФ RD_1992.03.30_3. Руководящий документ защита от несанкционированного доступа к информации .термины и определения;
13. Изучение документа ФСТЭК РФ RD_1992.03.30_4. Руководящий документ концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Стандартизация. Международные стандарты

BS 7799-1:2005 — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ

BS 7799-2:2005 — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.

BS 7799-3:2006 — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности

ISO/IEC 17799:2005 — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.

ISO/IEC 27000 — Словарь и определения.

ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.

ISO/IEC 27002 — Сейчас: ISO/IEC 17799:2005. «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.

ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ.
German Information Security Agency. IT Baseline Protection Manual — Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).

Государственные (национальные) стандарты РФ

ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.

Руководящие документы

РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации - содержит описание показателей защищенности информационных систем и требования к классам защищенности.
Стандарт Банка России СТО БР ИББС-1.0-2014 - Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
PCI DSS (Payment Card Industry Data Security Standard) - Стандарт безопасности данных индустрии платёжных карт.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, 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;
2. Экономика качества, стандартизации и сертификации: Учеб./О.А.Леонов, Г.Н.Темасова и др.; Под общ. ред. проф. О.А.Леонова - М.: НИЦ ИНФРА-М, 2014 - 251с.: ISBN 978-5-16-005371-4, Режим доступа: http://znanium.com/catalog.php?bookinfo=363841;
3. 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;
4. Основы метрологии, стандартизации и сертификации: Учебное пособие / Н.Д. Дубовой, Е.М. Портнов. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 256 с. ISBN 978-5-8199-0338-4 Режим доступа: http://znanium.com/catalog.php?bookinfo=371141.

б) Дополнительная литература:

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.;ISBN 978-5-8199-0331-5, Режим доступа: http://znanium.com/catalog.php?bookinfo=423927
2. Метрология, стандартизация и сертификация: Учебное пособие / Г.М. Дехтярь. - М.: КУРС: НИЦ ИНФРА-М, 2014. - 154 с.: 60x88 1/16. (обложка) ISBN 978-5-905554-44-5. Режим доступа: http://znanium.com/catalog.php?bookinfo=429502;
3. Метрология, стандартизация и сертификация: Учебное пособие / Е.Б. Герасимова, Б.И. Герасимов. - 2-е изд. - М.: Форум: НИЦ ИНФРА-М, 2015. - 224 с. ISBN 978-5-00091-014-6 Режим доступа: http://znanium.com/catalog.php?bookinfo=493233.

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 «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 10.03.01 «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 2017/2018 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: _____