Уп2016

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

Теоретические основы компьютерной безопасности

Направление подготовки 10.04.01 Информационная безопасность

Программа подготовки _____

Уровень высшего образования магистратура

Форма обучения очная

Семестр	Трудоемкость зач. ед./час.	Лекций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
1	3/108	18		18	72	Зачет
Итого	3/108	18		18	72	Зачет

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Теоретические основы компьютерной безопасности» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность». Целью освоения дисциплины является ознакомление магистров с современными представлениями о теоретическом и практическом аппарате компьютерной безопасности, о базовых моделях и алгоритмах, используемых в управлении компьютерной безопасностью в информационных системах, а также о процессе теоретико-методологического анализа защищенности различных сервисов информационной системы. Задачей изучения дисциплины «Теоретические основы компьютерной безопасности» является изучение аппарата управления компьютерной безопасностью в информационных системах, освоение методов анализа защищенности программно-технических сервисов информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО МАГИСТРАТУРЫ

Данная дисциплина относится к обязательным дисциплинам вариативной части Блока Б1 (код Б1.В.ОД.6). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

Дисциплина изучается на 1 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Основы информационной безопасности», «Защита информации в информационных системах» и (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», «Информационно-аналитические системы безопасности», «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-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации;

ПК-13 – способностью организовать управление информационной безопасностью.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать***: основные концептуальные положения теории ЗИ; - содержание функций ЗИ; - классификацию средств ЗИ; - преимущества и недостатки программных, аппаратных и организационных средств ЗИ; - общее содержание методологии проектирования системы ЗИ; - методику построения системы ИБ предприятия; - метод экспертных оценок при построении системы ЗИ; - аналитическую зависимость (формулу) для оценки вероятности уязвимости информации; - модель защищенной системы Хоффмана – Клементса; - основ-

ные этапы проведения аудита информационной безопасности; - типовой набор угроз информационной безопасности объекта аудита. (ПК-9; ПК-13);

2) ***Уметь:*** решать задачу выбора системы ЗИ методом последовательных уступок; - строить формальную модель метода анализа иерархий при выборе системы ЗИ; - использовать метод экспертных оценок при построении системы ЗИ; - привести ранжированный список угроз по частоте их проявления; - сравнивать качественные и количественные методы оценки уровня защищенности; - определять вероятности защищенности информационных ресурсов; - категорировать критичные информационные ресурсы и информационные процессы предприятия (организации); - заполнять типовые формы отчетов по сбору исходной информации об информационной системе предприятия (организации); - выявлять нарушителей, уязвимости и угрозы информационной безопасности конкретного предприятия (организации). (ПК-9; ПК-13);

3) ***Владеть:*** - навыками настройки современных средств защиты информации; - программными средствами оценки защищенности компьютерных систем; - навыками управления информационной безопасностью простых объектов (ПК-9; ПК-13).

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

- способность разрабатывать, оформлять и реализовывать политики информационной безопасности для современных компьютерных систем.

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 промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1.	Математическая модель комплексного подхода к обеспечению безопасности компьютерной системы. Основы теории защиты информации	1	1-2	2		2		8		1/25%	
2.	Методика построения системы защиты информации	1	3-4	2		2		8		2/50%	
3.	Методы многопараметрической оценки эффективности системы защиты информации	1	5-6	2		2		6		1/25%	Рейтинг-контроль №1
4.	Метод экспертных оценок при анализе эффективности системы защиты информации	1	7-8	2		2		8		1/25%	
5.	Угрозы информационной безопасности и оценка вероятности их реализации	1	9-10	2		2		10		2/50%	
6.	Модель описания процесса защиты информации Хоффмана – Клементса	1	11-12	2		2		10		1/25%	Рейтинг-контроль №2
7.	Вероятностная модель оценки защищенности информационных ресурсов	1	13-14	2		2		6		2/50%	
8.	Сбор исходных данных для аудита безопасности информационной системы	1	15-16	2		2		8		1/25%	
9.	Выявление уязвимостей и идентификация защитных механизмов информационной системы	1	17-18	2		2		8		2/50%	Рейтинг-контроль №3
Всего				18		18		72		13/36%	Зачет

Содержание дисциплины «Теоретические основы компьютерной безопасности»

Раздел 1. Математическая модель комплексного подхода к обеспечению безопасности компьютерной системы. Основы теории защиты информации. Перечень полного множества функций защиты. Основные концептуальные положения теории ЗИ. Содержание функции ЗИ. Определение механизма защиты и их десять классов, образующих репрезентативное множество. Наиболее распространенные классификации средств ЗИ.

Раздел 2. Методика построения системы защиты информации. Общее содержание методологии проектирования системы ЗИ. Процесс создания оптимальной системы. Возможные постановки задачи оптимизации СЗИ. Влияние показатели защищаемой информации на структуру и подходы к проектированию системы ЗИ. Основные принципы обеспечения ИБ предприятия. Условия успешности решения проблем ИБ. Рекомендации создателям систем ИБ. Методика построения системы ИБ предприятия

Раздел 3. Методы многопараметрической оценки эффективности системы защиты информации. Модель решения задачи выбора системы ЗИ методом последовательных уступок. Формальная модель метода анализа иерархий при выборе системы ЗИ.

Раздел 4. Метод экспертных оценок при анализе эффективности системы защиты информации. Метод экспертных оценок при построении системы ЗИ. Основные этапы метода экспертных оценок при построении системы ЗИ. Метод проверки системы ЗИ с применением тестирования или «тестирования на проникновение».

Раздел 5. Угрозы информационной безопасности и оценка вероятности их реализации. Ранжированный список угроз по частоте их проявления. Обобщенная иерархическая структурная модель угроз. «Нештатные» ситуации в работе ИС. Расширенное толкование понятия «угроза». Общий подход к оценке уязвимости информационных ресурсов по каналам утечки информации. Аналитическая зависимость для оценки вероятности уязвимости информации

Раздел 6. Модель описания процесса защиты информации Хоффмана – Клементса. Качественные и количественные методы оценки уровня защищенности Модель описания процесса защиты информации Хоффмана. Модель оценки уровня защищенности, основанную на анализе рисков.Развитие модели Хоффмана. Теоретико-множественная модель защищенной системы Клементса.

Раздел 7. Вероятностная модель оценки защищенности информационных ресурсов. Общая модель процесса защиты информации в виде пятимерного кортежа элементов. Основные параметры модели процесса защиты. Уточнения и допущения модели процесса защиты. Алгоритм определения вероятности защищенности одного информационного ресурса. Достоинства предлагаемой модели процесса защиты.

Раздел 8. Сбор исходных данных для аудита безопасности информационной системы. Аудит информационной безопасности предприятия (организации). Основные этапы проведения аудита информационной безопасности. Уровни защищаемой информации для категорировании критичных информационных ресурсов и информационных процессов предприятия (организации). Основные подсистемы защиты информации и их защитные механизмы. Типовые формы отчетов по сбору исходной информации об информационной системе предприятия.

Раздел 9. Выявление уязвимостей и идентификация защитных механизмов информационной системы. Сравнительный анализ двух групп оценки рисков информационной безопасности. Методика выявления уязвимостей в анализируемой информационной системе. Методика идентификации защитных механизмов информационной системы. Категории нарушителей. Типовой набор угроз информационной безопасности объекта аудита информационной безопасности.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Теоретические основы компьютерной 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

1. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность?
2. Сформулируйте основные концептуальные положения теории ЗИ.
3. Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?

4. Сформулируйте определение механизма защиты и назовите их десять классов, образующих репрезентативное множество.
5. Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
6. Сформулируйте возможные постановки задачи оптимизации СЗИ.
7. Прокомментируйте основные принципы обеспечения ИБ предприятия
8. Приведите принятую методику построения системы ИБ предприятия
9. Приведите модель решения задачи выбора системы ЗИ методом последовательных уступок.
10. Приведите формальную модель метода анализа иерархий при выборе системы ЗИ.

Вопросы рейтинг-контроля №2

1. В чем заключается сущность метода экспертных оценок при построении системы ЗИ?
2. Приведите описание основных этапов метода экспертных оценок при построении системы ЗИ
3. Приведите ранжированный список угроз по частоте их проявления.
4. Приведите общий подход к оценке уязвимости информационных ресурсов по каналам утечки информации
5. Какие параметры и характеристики входят в вероятностную модель оценки уязвимости защищаемой информации?
6. Выведите аналитическую зависимость (формулу) для оценки вероятности уязвимости информации
7. Сравните качественные и количественные методы оценки уровня защищенности
8. Приведите модель описания процесса защиты информации Хоффмана.
9. Какие множества рассматриваются при описании системы защиты информации с полным перекрытием?
10. Приведите теоретико-множественную модель защищенной системы Клементса.

Вопросы рейтинг-контроля №3

1. Приведите общую модель процесса защиты информации в виде пятимерного кортежа элементов.
2. Приведите основные параметры модели процесса защиты
3. Приведите алгоритм определения вероятности защищенности одного информационного ресурса
4. Что понимают под аудитом информационной безопасности предприятия (организации)?
5. Приведите и прокомментируйте основные этапы проведения аудита информационной безопасности.
6. Назовите основные подсистемы защиты информации и дайте комментарий к их защитным механизмам
7. Заполните типовые формы отчетов по сбору исходной информации об информационной системе предприятия (организации), в котором работаете или проходили производственную практику.
8. В чем заключается методика выявления уязвимостей в анализируемой информационной системе?
9. Приведите методику идентификации защитных механизмов информационной системы.
10. Какие категории нарушителей следует учитывать при анализе защищенности информационной системы?

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

1. Сформулируйте основные концептуальные положения теории ЗИ.
2. Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
3. Сформулируйте определение механизма защиты и назовите их десять классов, образующих репрезентативное множество.
4. Сформулируйте возможные постановки задачи оптимизации СЗИ.
5. Прокомментируйте основные принципы обеспечения ИБ предприятия
6. Приведите принятую методику построения системы ИБ предприятия
7. Приведите модель решения задачи выбора системы ЗИ методом последовательных уступок.
8. Приведите формальную модель метода анализа иерархий при выборе системы ЗИ.
9. В чем заключается сущность метода экспертных оценок при построении системы ЗИ?
10. Приведите ранжированный список угроз по частоте их проявления.
11. Приведите общий подход к оценке уязвимости информационных ресурсов по каналам утечки информации
12. Какие параметры и характеристики входят в вероятностную модель оценки уязвимости защищаемой информации?
13. Выведите аналитическую зависимость (формулу) для оценки вероятности уязвимости информации
14. Сравните качественные и количественные методы оценки уровня защищенности
15. Приведите модель описания процесса защиты информации Хоффмана.
16. Приведите теоретико-множественную модель защищенной системы Клементса.
17. Приведите основные параметры модели процесса защиты
18. Приведите алгоритм определения вероятности защищенности одного информационного ресурса
19. Что понимают под аудитом информационной безопасности предприятия (организации)?
20. Приведите и прокомментируйте основные этапы проведения аудита информационной безопасности.
21. Назовите основные подсистемы защиты информации и дайте комментарий к их защитным механизмам
22. Заполните типовые формы отчетов по сбору исходной информации об информационной системе предприятия (организации), в котором работаете или проходили производственную практику.
23. В чем заключается методика выявления уязвимостей в анализируемой информационной системе?
24. Приведите методику идентификации защитных механизмов информационной системы.
25. Какие категории нарушителей следует учитывать при анализе защищенности информационной системы?

Темы лабораторных работ:

ЛАБОРАТОРНАЯ РАБОТА 1. Сбор исходных данных для аудита информационной безопасности

ЛАБОРАТОРНАЯ РАБОТА 2. Выявление уязвимостей компьютерной системы

ЛАБОРАТОРНАЯ РАБОТА 3. Идентификация защитных механизмов

ЛАБОРАТОРНАЯ РАБОТА 4. Идентификация нарушителей

Вопросы и задания к самостоятельной работе магистрантов:

Раздел 1.

1. Сформулируйте определение механизма защиты и назовите их десять классов, образующих репрезентативное множество.
2. Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?

Раздел 2.

1. Сформулируйте возможные постановки задачи оптимизации СЗИ.
2. Прокомментируйте основные принципы обеспечения ИБ предприятия
3. Какие должны быть условия успешности решения проблем ИБ?
4. Сформулируйте общие требования к системе ИБ объекта
5. Перечислите рекомендации создателям систем ИБ.

Раздел 3.

1. Приведите модель решения задачи выбора системы ЗИ методом последовательных уступок.
2. Приведите формальную модель метода анализа иерархий при выборе системы ЗИ.

Раздел 4.

1. В чем заключается сущность метода экспертных оценок при построении системы ЗИ?
2. Что предусматривает метод проверки системы ЗИ с применением тестирования или «тестирования на проникновение»?

Раздел 5.

1. Приведите ранжированный список угроз по частоте их проявления.
2. Какие ситуации в работе ИС называют «нештатными»?
3. Приведите общий подход к оценке уязвимости информационных ресурсов по каналам утечки информации
4. Какие параметры и характеристики входят в вероятностную модель оценки уязвимости защищаемой информации?

Раздел 6.

1. Сравните качественные и количественные методы оценки уровня защищенности
2. Приведите модель оценки уровня защищенности, основанную на анализе рисков.
3. Какие множества рассматриваются при описании системы защиты информации с полным перекрытием?

Раздел 7.

1. Приведите основные параметры модели процесса защиты
2. Какие уточнения и допущения модели процесса защиты Вы знаете?
3. Достоинства предлагаемой модели процесса защиты информации в виде пятимерного кортежа элементов

Раздел 8.

1. Заполните типовые формы отчетов по сбору исходной информации об информационной системе предприятия (организации), в котором работаете или проходили производственную практику.

Раздел 9.

2. Проведите сравнительный анализ двух групп оценки рисков информационной безопасности.
3. Выявите нарушителей, уязвимости и угрозы информационной безопасности конкретного предприятия (организации)

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Защита в операционных системах: Учебное пособие для вузов / Проскурин В.Г. - М. : Горячая линия - Телеком, 2014. - http://www.studentlibrary.ru/book/ISBN9785991203791.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. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. ISBN 978-5-8199-0331-5, Режим доступа: http://znanium.com/catalog.php?bookinfo=335362
4. 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
5. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: ISBN 978-5-00091-079-5, Режим доступа: http://znanium.com/catalog.php?bookinfo=508381

б) Дополнительная литература:

1. Аудит безопасности Intranet / Петренко С.А., Петренко А.А. - М. : ДМК Пресс, 2010. - http://www.studentlibrary.ru/book/ISBN5940741835.html
2. Операционные системы. Концепции построения и обеспечения безопасности: Учебное пособие для вузов / Мартемьянов Ю.Ф., Яковлев Ал.В., Яковлев Ан.В. - М. : Горячая линия - Телеком, 2010. - http://www.studentlibrary.ru/book/ISBN9785991201285.html
3. А.Ю. Щербаков. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с. - http://www.studentlibrary.ru/book/ISBN9785804103782.html
4. Информационные технологии: Учебное пособие / Л.Г. Гагарина, Я.О. Теплова, Е.Л. Румянцева и др.; Под ред. Л.Г. Гагариной - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. - ISBN 978-5-8199-0608-8 Режим доступа: http://znanium.com/catalog.php?bookinfo=471464
5. Информационная система предприятия: Учебное пособие/Вдовенко Л. А. - 2 изд., перераб. и доп. - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 304 с. ISBN 978-5-9558-0329-6, Режим доступа: http://znanium.com/catalog.php?bookinfo=501089

в) Периодические издания:

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
3. Информационно-методический журнал «Защита информации. Конфидент» http://sec4all.net/konfj-5_03.html
4. Научный журнал «Проблемы машиностроения и автоматизации» Режим доступа: http://ores.su/ru/journals/problemyi-mashinostroeniya-i-avtomatizatsii/
5. Каталог журналов в области охраны и безопасности. http://secandsafe.ru/jurnaly/

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. Монахов Ю.М.

(ФИО, подпись)

Рецензент
(представитель работодателя) к.т.н. Курысев Константин Николаевич ВРИО заместителя начальника Владимирского юридического института ФСИН России по учебной работе

(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 10.04.01 «Информационная безопасность»

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: _____