

2015-2016

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



\_\_\_\_\_ А.А.Панфилов

« 29 » 12 \_\_\_\_\_ 2016 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ**  
(наименование дисциплины)

Специальность 10.05.04 "Информационно-аналитические системы безопасности"  
Специализация "Автоматизация информационно-аналитической деятельности"  
Уровень высшего образования специалитет  
Форма обучения очная

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
8	7/252	36	36	36	108	Экзамен (36ч), КР
Итого	7/252	36	36	36	108	Экзамен (36ч), КР

Владимир 2016

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### Целями освоения дисциплины «Система защиты информации на предприятии»

являются обеспечение профессиональной подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана специальности 10.05.04 «Информационно-аналитические системы безопасности», формирование у студентов обобщенного представления по следующим вопросам: -изучение методологических и законодательных основ организации системы защиты информации на предприятии, а также основных аспектов практической деятельности по ее созданию, обеспечению функционирования и контролю и эффективности.

Сущность и задачи дисциплины «Система защиты информации на предприятии»: -принципы организации и этапы разработки СЗИ; -факторы, влияющие на организацию СЗИ; - определение и нормативное закрепление состава защищаемой информации; -определение объектов защиты; -анализ и оценка угроз безопасности информации; - выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию; - определение потенциальных каналов и методов несанкционированного доступа к информации; -определение возможностей несанкционированного доступа к защищаемой информации. Кроме того, изучаются вопросы: -технологическое и организационное построение СЗИ; - кадровое обеспечение функционирования СЗИ; -материально-техническое и нормативно-методическое обеспечение функционирования СЗИ; -принципы и методы планирования функционирования СЗИ; -сущность и содержание контроля функционирования СЗИ; -управление.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.24). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и практических занятий. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

Дисциплина изучается на четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации» по специальности 10.05.04 «Информационно-аналитические системы безопасности», квалификации - специалист.

Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Методология и организация информационно-аналитической деятельности», «Моделирование автоматизированных информационных систем», «Распределенные автоматизированные информационные системы», «Формализованные модели и методы решения аналитических задач».

## 3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями:

ПК-7 – способностью проводить предпроектное обследование профессиональной деятельности и информационных потребностей автоматизируемых подразделений;

ПК-9– способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах;

ПК-13 – способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;

ПК-19– способностью обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

**1) Знать:** - цели, задачи и принципы построения системы защиты информации; - требования, предъявляемые к системе защиты информации; - этапы разработки комплексной системы защиты информации; - первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; - перечень вопросов ЗИ, требующих документационного закрепления; - виды контроля функционирования системы защиты информации на предприятии (ПК-7; ПК-9; ПК-13; ПК-19);

**2) Уметь:** - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации (ПК-7; ПК-9; ПК-13; ПК-19);

**3) Владеть:** - информацией о факторах, определяющие необходимость защиты территории и здания предприятия; - информацией о взаимодействии между субъектами, защищающими и использующими информацию ограниченного доступа; - информацией о структуре технического задания на создание комплексной системы защиты информации на предприятии; - методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; - методикой определения возможностей несанкционированного доступа к защищаемой информации; - методикой разработке модели комплексной системы защиты информации (ПК-7; ПК-9; ПК-13; ПК-19).

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

- способность осуществлять комплексный подход к организации системы защиты на предприятии с учетом экономической эффективности СЗИ и требований нормативно-технических документов.

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 7 зачетных единиц, 252 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 промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы,	СРС	КП / КР		
1	Основные руководящие документы и показатели эффективности системы ЗИ	8	1-2	4	4	4		12		4 (33%)	-
2	Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них	8	3-4	4	4	4		12		4 (33%)	
3	Формирование концепции обеспечения ИБ.	8	5-6	4	4	4		12		4 (33%)	Рейтинг-контроль №1
4	Решения по ЗИ и оценка их качества.	8	7-8	4	4	4		12		4 (33%)	
5	Угрозы ИБ и оценка вероятности их реализации.	8	9-10	4	4	4		12		4 (33%)	
6	Формирование облика нарушителя	8	11-12	4	4	4		12		4 (33%)	Рейтинг-контроль №2
7	Алгоритм проведения анализа информационного риска на предприятии	8	13-14	4	4	4		12		4 (33%)	
8	Аналитические технологии управления ИБ.	8	15-16	4	4	4		12		4 (33%)	
9	План обеспечения ИБ предприятия	8	17-18	4	4	4		12		4 (33%)	Рейтинг-контроль №3
Всего				36	36	36		108		36 (33%)	Экзамен

**Содержание дисциплины «Система защиты информации на предприятии»:**

**Раздел 1.** Введение. Основные руководящие документы и показатели эффективности системы ЗИ Комплексный подход к обеспечению ИБ объекта

**Раздел 2.** Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них

**Раздел 3.** Формирование концепции обеспечения ИБ.

**Раздел 4.** Решения по ЗИ и оценка их качества. Анализ риска. Общие положения и характеристика атаки на АС.

**Раздел 5.** Угрозы ИБ и оценка вероятности их реализации.

**Раздел 6.** Формирование облика нарушителя

**Раздел 7.** Алгоритм проведения анализа информационного риска на предприятии

**Раздел 8.** Аналитические технологии управления ИБ. Обеспечение ИБ в чрезвычайных ситуациях

**Раздел 9.** План обеспечения ИБ предприятия

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления специалиста по специальности 10.05.04 «Информационно-аналитические системы 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:

- учебную дискуссию;
- электронные средства обучения (слайд-лекции, электронные тренажеры, компьютерные тесты);
- дистанционные (сетевые) технологии.

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 студентами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП специальности 10.05.04 «Информационно-аналитические системы безопасности», 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 55 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 студента в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

### Вопросы рейтинг-контроля №1

- Дать определение СЗИ.
- Что такое информационная безопасность?
- Цели информационной безопасности.
- Основные требования к комплексной системе защиты информации
- Задачи системы компьютерной безопасности
- Основные принципы организации СЗИ
- В чём заключается принцип системности?
- В чём заключается принцип комплексности?

- В чём заключается принцип непрерывности защиты?
- В чём заключается принцип разумной достаточности?
- В чём заключается гибкость системы защиты?
- Принцип простоты применения средств защиты
- Этап работ по созданию СЗИ.

### **Вопросы рейтинг-контроля №2**

- Что включает в себя обследование организации?
- Факторы, влияющие на организацию СЗИ.
- Определение состава защищаемой информации
- Нормативное закрепление состава защищаемой информации
- Виды информации.
- Необходимые свойства защищаемой информации
- Категорирование защищаемой информации.
- Определение объектов защиты.
- Что называется объектом защиты.
- Основные объекты защиты.
- Основные виды угроз информационной безопасности:
- Классификация угроз безопасности
- Неформальная модель нарушителя в АС .
- Что определяются при разработке модели нарушителя.

### **Вопросы рейтинг-контроля №3**

- Причины совершения компьютерных преступлений
- Потенциальные каналы несанкционированного доступа к защищаемой информации
- Потенциальные методы несанкционированного доступа к защищаемой информации.
- Классификация каналов проникновения в систему и утечки информации
- Физические каналы.
- Электромагнитные каналы.
- Информационные каналы
- Общая модель комплексной системы защиты информации.
- Средства защиты, используемые для создания системы защиты.
- Типы моделей управления доступом.
- Организационное направление работ по созданию СЗИ.
- Технология построения СЗИ
- Кадровое обеспечение функционирования СЗИ.
- Организационная структура, основные функции службы компьютерной безопасности.
- Концепция (политика) безопасности.

### **Перечень вопросов к экзамену (промежуточной аттестации по итогам освоения дисциплины):**

1. Дать определение СЗИ.
2. Что такое информационная безопасность?
3. Цели информационной безопасности.
4. Основные требования к комплексной системе защиты информации
5. Задачи системы компьютерной безопасности
6. Основные принципы организации СЗИ
7. В чём заключается принцип системности?
8. В чём заключается принцип комплексности?
9. В чём заключается принцип непрерывности защиты?
10. В чём заключается принцип разумной достаточности?
11. В чём заключается гибкость системы защиты?

12. Принцип простоты применения средств защиты
13. Этап работ по созданию СЗИ.
14. Что включает в себя обследование организации?
15. Факторы, влияющие на организацию СЗИ.
16. Определение состава защищаемой информации
17. Нормативное закрепление состава защищаемой информации
18. Виды информации.
19. Необходимые свойства защищаемой информации
20. Категорирование защищаемой информации.
21. Определение объектов защиты.
22. Что называется объектом защиты.
23. Основные объекты защиты.
24. Основные виды угроз информационной безопасности:
25. Классификация угроз безопасности
26. Неформальная модель нарушителя в АС .
27. Что определяются при разработке модели нарушителя.
28. Причины совершения компьютерных преступлений
29. Потенциальные каналы несанкционированного доступа к защищаемой информации
30. Потенциальные методы несанкционированного доступа к защищаемой информации.
31. Классификация каналов проникновения в систему и утечки информации
32. Физические каналы.
33. Электромагнитные каналы.
34. Информационные каналы
35. Общая модель комплексной системы защиты информации.
36. Средства защиты, используемые для создания системы защиты.
37. Типы моделей управления доступом.
38. Организационное направление работ по созданию СЗИ.
39. Технология построения СЗИ
40. Кадровое обеспечение функционирования СЗИ.
41. Организационная структура, основные функции службы компьютерной безопасности.
42. Концепция (политика) безопасности.

#### **Темы лабораторных работ:**

- Построение описания объекта информатизации. Общее описание объекта и его планировка.
- Построение описания объекта информатизации. Организационная структура предприятия и экспликация помещений отделов.
- Построение описания объекта информатизации. Перечень и характеристики информационных ресурсов.
- Построение описания объекта информатизации. Список и характеристики персонала.
- Проектирование корпоративной сети передачи данных. Список и характеристики средств хранения, обработки, передачи и представления информации.
- Проектирование корпоративной сети передачи данных. Список и характеристики средств защиты информации.
- Проектирование корпоративной сети передачи данных. Топология КСПД и схема адресации.
- Разработка слоев «информационные ресурсы», «КСПД», «персонал», «уязвимости», «угрозы» на плане объекта.
- Разработка слоев СЗИ на плане объекта.

#### **Темы практических занятий:**

1. Выполнение анализа угроз ИБ и защищённости ИС (18ч)
  - 1.1. Перечень угроз ИБ. (2ч)
  - 1.2. Перечень уязвимостей ИС с обоснованием. (4ч)

- 1.3. Перечень и характеристики существующих защитных механизмов. (4ч)
- 1.4. Произвести оценку текущего уровня защищённости от угроз ИБ согласно методике. (4ч)
- 1.5. Ранжировать список угроз по вероятностям реализации от максимальной к минимальной. Выделить на слои «угрозы» в цветовой гамме от красного к зелёному согласно списку. (4ч)
2. Построение и оценка СЗИ на предприятии. (18ч)
  - 2.1. Сделать обоснованный выбор механизмов обеспечения информационной безопасности в рамках организационно-технического, инженерно-технического и программно-аппаратного направлений. (6ч)
  - 2.2. Произвести переоценку уровня защищённости от угроз ИБ. Ранжировать угрозы в новый список. При этом выбранные механизмы защиты должны обеспечить такое снижение вероятностей реализации угроз, чтобы ни одна угроза «красного цвета» не оказалась «красной» в новом списке. (6ч)
  - 2.3. Оценить затраты на обеспечение ИБ предприятия. (6ч)

### **Темы для курсовой работы**

Тема проекта (работы): Разработка и оценка системы защиты информации на предприятии.

#### **1. Исходные данные**

- Планировки помещений объекта информатизации
- Описание организационной структуры

#### **2. Объём работы**

##### **2.1. Разработать следующие вопросы**

- Построить описание объекта информатизации.
- Спроектировать корпоративную сеть передачи данных.
- Выполнить анализ угроз ИБ и защищённости ИС
- Построить и оценить СЗИ на предприятии.

##### **2.2. Конструктивно разработать (вычертить)**

- Слой «информационные ресурсы» на плане объекта.
- Слой «корпоративная сеть передачи данных» на плане объекта.
- Слой «персонал» на плане объекта.
- Слой «уязвимости» на плане объекта.
- Слой «угрозы» на плане объекта.

### **Вопросы и задания для самостоятельной работы студентов:**

- Прокомментируйте основные направления обеспечения ИБ
- Что понимается под безопасностью информации? Что такое ЗИ?
- Дайте определение понятиям «конфиденциальность», «целостность», «доступность».
- Перечислите основные задачи системы информационной безопасности.
- В чем заключается основная цель защиты информации?
- Определите организационные проблемы информационной безопасности.
- Сформулируйте технические проблемы информационной безопасности.
- Раскройте общее содержание методологии проектирования системы ЗИ. Как понимается процесс создания оптимальной системы? Сформулируйте возможные постановки задачи оптимизации СЗИ.
- Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
- Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
- Дайте определение системы ЗИ и сформулируйте основные концептуальные требования, предъявляемые к ней.
- Приведите принятую методику построения системы ИБ предприятия



- Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность?
- Сформулируйте основные концептуальные положения теории ЗИ.
- По каким аспектам экспертная комиссия предприятия рассматривает предварительный перечень конфиденциальных сведений?
- Приведите типовой примерный перечень сведений, составляющих служебную или коммерческую тайну организации.
- Перечислите степень секретности (гриф), который могут иметь сведения, составляющие служебную или коммерческую тайну предприятия
- Что принято понимать под служебной или коммерческой тайной?
- Каковы критерии отнесения организаций и частных лиц к потенциальным злоумышленникам (которые могут быть заинтересованы в доступе к охраняемой информации)?
- Каким образом принимается и как оформляется решения о включении сведений в окончательный вариант Перечня?
- Назовите основную цель планирования в обеспечении ИБ предприятия. Охарактеризуйте стратегическое (или перспективное) и тактическое (или текущее) планирование.
- Из каких этапов состоит работа по формированию Перечня сведений, составляющих служебную или коммерческую тайну?
- Определите составляющие информационно-логической модели объекта защиты.
- Что понимают под Политикой информационной безопасности?
- Что должна включать в себя в обобщенном виде Концепция обеспечения ИБ?
- Перечислите основные элементы Концепции обеспечения ИБ на предприятии. 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.
- Что понимают под концепцией ИБ?
- Назовите причины необходимости разработки Концепции обеспечения ИБ на каждом предприятии.
- Определите основную цель и комплекс мероприятий управления ИБ предприятия. Приведите обобщенную схему процесса управления ИБ предприятия
- Охарактеризуйте основные направления деятельности администратора безопасности
- Охарактеризуйте этапы логической последовательности принятия решения в процессе управления ИБ
- Приведите структуру АРМа администратора безопасности
- Основные подразделения службы ИБ, их организационно-правовой статус.
- Приведите основные особенности и принципы построения системы управления ИБ. Охарактеризуйте основные подсистемы СУИБ.
- Приведите и прокомментируйте пакет планирующих документов по обеспечению ИБ
- С какой целью разрабатывается план мероприятий по противодействию ЧС?
- Какие мероприятия по работе с персоналом необходимо проводить для наиболее эффективного противодействия ЧС? Приведите основные методы реагирования на ЧС
- Какие ситуации называют чрезвычайными? Приведите классификацию ЧС. Охарактеризуйте наиболее распространенные угрозы в условиях чрезвычайных ситуаций
- Охарактеризуйте постоянно проводимые мероприятия защиты и мероприятия, проводимые по необходимости
- Охарактеризуйте разовые и периодически проводимые мероприятия защиты
- Охарактеризуйте источники получения информации для администратора безопасности

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Основная литература:

1. 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>
2. Интеллектуальные системы защиты информации: учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - <http://www.studentlibrary.ru/book/ISBN9785942756673.html> 172 с.
3. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - <http://www.studentlibrary.ru/book/ISBN9785940746478.html>. 474 с.

### б) Дополнительная литература:

1. Бизнес-безопасность / Кузнецов И.Н. - М. : Дашков и К, 2012. - <http://www.studentlibrary.ru/book/ISBN9785394014383.html>. 416 с.
2. Офисный шпионаж / Мелтон К., Пилиджан К., Сверчински Д. - М. : Альпина Паблишер, 2013. - <http://www.studentlibrary.ru/book/ISBN9785916712070.html>. 182 с.
3. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций / Ямалов И.У. - М. : БИНОМ, 2015. - <http://www.studentlibrary.ru/book/ISBN9785996325627.html>. 291 с.
4. Искусство управления информационными рисками / Астахов А.М. - М. : ДМК Пресс, 2010. - <http://www.studentlibrary.ru/book/ISBN9785940745747.html>. 312 с.

### в) Периодические издания :

1. «Журнал сетевых решений/LAN» -Режим доступа: <http://www.osp.ru/lan/current>;
2. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: <http://www.delpress.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 м<sup>2</sup>, 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 м<sup>2</sup>, 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 м<sup>2</sup>, 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 Chaos), 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.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.04 "Информационно-аналитические системы безопасности", специализация «автоматизация информационно-аналитической деятельности»

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

Рецензент  
(представитель работодателя) к.т.н. Абрамов Константин Германович ведущий специалист управления поддержки инфраструктуры ООО «ОМК - Информационные технологии».  
(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 по специальности 10.05.04 "Информационно-аналитические системы безопасности", специализация «автоматизация информационно-аналитической деятельности»

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)

**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: \_\_\_\_\_

г) интернет-ресурсы: \_\_\_\_\_