УП2015-2016

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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«_29_» _12_ 2016 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## Безопасность информационных и аналитических систем

(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) |
|---|---|---|---|---|---|---|
| 7 | 6/216 | 36 | | 36 | 108 | Экзамен (36ч) |
| Итого | 6/216 | 36 | | 36 | 108 | Экзамен (36ч) |

**Владимир 2016**

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Целями освоения дисциплины** «Безопасность информационных и аналитических систем» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности», ознакомление студентов с технологиями безопасного с точки зрения возможности утечки информации интеллектуального анализа больших информационных массивов посредством и с помощью информационно-аналитических систем.

Задачами освоения дисциплины «Безопасность информационных и аналитических систем» является:

- изучение основных положений, понятий и категорий, связанных с обеспечением безопасности информационно-аналитических систем;
- изучение основных подходов к выполнению безопасного интеллектуального анализа больших массивов данных посредством современных информационных технологий;
- формирование навыков противодействия несанкционированному проникновению в защищаемые информационные и аналитические системы с использованием современных информационно-вычислительных средств и систем.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.3). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

Дисциплина изучается на 4 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по специальности 10.05.04 «Информационно-аналитические системы безопасности» по курсам «Информатика», «Основы информационной безопасности», «Безопасность операционных систем», «Криптографические методы защиты информации», «Базы данных и экспертные системы», «Программно-аппаратные средства защиты информации». Курс тесно взаимосвязан с другими дисциплинами. Он является базовым для изучения таких дисциплин как «Распределенные автоматизированные информационные системы», «Методология и организация информационно-аналитической деятельности», «Моделирование автоматизированных информационных систем», «Формализованные модели и методы решения аналитических задач», «Корпоративные информационные системы» и т.д.

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

В результате освоения дисциплины специалист должен обладать следующими профессиональными компетенциями:

ОПК-7 – способностью применять методы и средства обеспечения информационной безопасности специальных ИАС;

профессиональными компетенциями:

ПК- 3 - способностью осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности;

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

ПК- 10 - способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;

ПК- 11 - способностью разрабатывать проектные документы на создаваемые специальные ИАС, в том числе средства обеспечения их информационной безопасности;

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

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **Знать:** - активные и пассивные методы сбора информации; - информационные технологии в системе информационно-аналитического обеспечения безопасности; -- базовые криптографические протоколы и основные требования к ним; - механизмы реализации атак в компьютерных сетях; - защитные механизмы и средства обеспечения сетевой безопасности; - основные методы организационного обеспечения информационной безопасности специальных АИС; - области применения экспертных систем и этапы их проектирования; - методологические основы, методы и средства построения распределенных специальных АИС; - нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; - принципы эксплуатации и сопровождения АИС (ОПК-7; ПК-3; ПК-9; ПК-10);

2) **Уметь:** - составлять перечень сведений, содержащих коммерческую тайну; - использовать организационные, правовые и программно-аппаратные методы защиты информации; - решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; - проектировать и сопровождать типовые специальные АИС, локальные сети; - устанавливать корреспондентские отношения с источниками информации, включая взаимодействие с вычислительными системами и базами данных в телекоммуникационном режиме и работу в глобальных компьютерных сетях; - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками (ОПК-7; ПК-3; ПК-11; ПК-13);

3) **Владеть:** - навыками работы с имеющимися на рынке информационно-аналитическими системами; - навыками обработки информации в специальных АИС; - навыками выбора и обоснования критериев эффективности функционирования специальных АИС; - навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств; - методами и средствами выявления угроз безопасности компьютерным системам (ОПК-7; ПК-3; ПК-9; ПК-10; ПК-11; ПК-13).

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

- способность применять навыки обеспечения защиты информации в информационных и аналитических системах.

## 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 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. | Архитектура современных информационных и аналитических систем. Уязвимости и угрозы | 7 | 1-2 | 4 | | 4 | | 10 | | 4/50% | |
| 2. | Протоколы идентификации, аутентификации и учета | 7 | 3-4 | 4 | | 4 | | 12 | | 2/25% | |
| 3. | Протоколы идентификации и аутентификации современных информационных и аналитических системах. | 7 | 5-6 | 4 | | 4 | | 14 | | 2/25% | Рейтинг-контроль №1 |
| 4. | Управление доступом в хранилищах данных | 7 | 7-8 | 4 | | 4 | | 12 | | 4/50% | |
| 5. | Организация безопасного межсетевого взаимодействия | 7 | 9-10 | 4 | | 4 | | 10 | | 4/50% | |
| 6. | Защита удаленного доступа в АИС. Организация защищенного удаленного доступа в информационных и аналитических системах. | 7 | 11-12 | 4 | | 4 | | 12 | | 2/25% | Рейтинг-контроль №2 |
| 7. | Управление криптоключами в информационных и аналитических системах | 7 | 13-14 | 4 | | 4 | | 12 | | 4/50% | |
| 8. | Инфраструктура управления открытыми ключами PKI | 7 | 15-16 | 4 | | 4 | | 14 | | 2/25% | |
| 9. | Стандарты Public-Key Cryptography | 7 | 17-18 | 4 | | 4 | | 12 | | 4/50% | Рейтинг-контроль №3 |
| Всего | | | | 36 | | 36 | | 108 | | 28/39% | Экзамен |

**Содержание дисциплины «Безопасность информационных и аналитических систем»**

**Раздел 1**. Архитектура современных информационных и аналитических систем. Уязвимости и угрозы современных информационных и аналитических систем. Методы обеспечения ИБ информационных и аналитических систем

**Раздел 2**. Протоколы идентификации, аутентификации и учета в современных информационных и аналитических системах. Методы локальной аутентификации

**Раздел 3**. Протоколы идентификации и аутентификации современных информационных и аналитических системах. Протокол TACACS. Протокол RADIUS.

**Раздел 4**. Управление доступом в хранилищах данных информационных и аналитических систем. Иерархия прав доступа. Виды привилегий.

**Раздел 5**. Организация безопасного межсетевого взаимодействия в распределенных информационных и аналитических системах. IPSec

**Раздел 6**. Защита удаленного доступа в АИС. Организация защищенного удаленного доступа в информационных и аналитических системах. Протоколы защищенного удаленного доступа

**Раздел 7**. Управление криптоключами в информационных и аналитических системах. Цифровая подпись. Сертификат цифровой подписи.

**Раздел 8**. Управление криптоключами в информационных и аналитических системах. Инфраструктура управления открытыми ключами PKI

**Раздел 9**. Управление криптоключами в информационных и аналитических системах. Стандарты Public-Key Cryptography

## 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**

- Современные уязвимости программного обеспечения информационных и аналитических систем;
- Вредоносное программное обеспечение и программные средства сетевых атак
- Методы и средства защиты информационных и аналитических систем;
- Задачи, решаемые современными средствами идентификации и аутентификации в информационных и аналитических системах;
- Характеристики AAA.
- Конфигурирование локальной AAA аутентификации с CLI на устройствах Cisco
- Конфигурирование распределенной AAA аутентификации с CLI на устройствах Cisco
- Протокол TACACS+. Задачи и характеристики протокола

- Протокол RADIUS. Задачи и характеристики протокола
- Аутентификация средствами протокола TACACS+. Конфигурирование протокола на устройствах Cisco
- Аутентификация средствами протокола RADIUS. Конфигурирование протокола на устройствах Cisco
- Аутентификация с 802.1X

**Вопросы рейтинг-контроля №2**

- Управление доступом в хранилищах данных информационных и аналитических систем.
- Иерархия прав доступа. Создание ролей.
- Виды привилегий. Операторы представления привилегий.
- Управление паролями в хранилищах данных информационных и аналитических систем. Операторы отмены привилегий
- Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
- Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
- Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Remote-Access VPN
- Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Site-to-Site VPN
- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол IPSec.
- Протокол IPSec.Обеспечение конфиденциальности в информационных и аналитических системах.
- Протокол IPSec.Обеспечение целостности в информационных и аналитических системах.

**Вопросы рейтинг-контроля №3**

- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол AH. Особенности применения
- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол ESP. Особенности применения
- Команды и алгоритм конфигурирования Site-to-Site VPN на устройствах Cisco
- Команды и алгоритм конфигурирования Remote-Access VPN на устройствах Cisco
- Политики ISAKMP. Конфигурирование Pre-Shared Key
- Протоколы защищенного удаленного доступа в информационных и аналитических системах.
- Конфигурирование протоколов защищенного удаленного доступа в информационных и аналитических системах.
- Инфраструктура PKI. Задачи PKI
- Особенности применения ЭП в информационных и аналитических системах.
- Криптографические стандарты PKI
- Топологии PKI

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

1. Современные угрозы информационной безопасности информационных и аналитических систем;
2. Современные уязвимости программного обеспечения информационных и аналитических систем;
3. Вредоносное программное обеспечение и программные средства сетевых атак
4. Методы и средства защиты информационных и аналитических систем;
5. Задачи, решаемые современными средствами идентификации и аутентификации в информационных и аналитических системах;

6. Характеристики AAA.
7. Конфигурирование локальной AAA аутентификации с CLI на устройствах Cisco
8. Конфигурирование распределенной AAA аутентификации с CLI на устройствах Cisco
9. Протокол TACACS+. Задачи и характеристики протокола
10. Протокол RADIUS. Задачи и характеристики протокола
11. Аутентификация средствами протокола TACACS+. Конфигурирование протокола на устройствах Cisco
12. Аутентификация средствами протокола RADIUS. Конфигурирование протокола на устройствах Cisco
13. Аутентификация с 802.1X
14. Управление доступом в хранилищах данных информационных и аналитических систем.
15. Иерархия прав доступа. Создание ролей.
16. Виды привилегий. Операторы представления привилегий.
17. Управление паролями в хранилищах данных информационных и аналитических систем. Операторы отмены привилегий
18. Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
19. Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
20. Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Remote-Access VPN
21. Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Site-to-Site VPN
22. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол IPSec.
23. Протокол IPSec.Обеспечение конфиденциальности в информационных и аналитических системах.
24. Протокол IPSec.Обеспечение целостности в информационных и аналитических системах.
25. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол AH. Особенности применения
26. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол ESP. Особенности применения
27. Команды и алгоритм конфигурирования Site-to-Site VPN на устройствах Cisco
28. Команды и алгоритм конфигурирования Remote-Access VPN на устройствах Cisco
29. Политики ISAKMP. Конфигурирование Pre-Shared Key
30. Протоколы защищенного удаленного доступа в информационных и аналитических системах.
31. Конфигурирование протоколов защищенного удаленного доступа в информационных и аналитических системах.
32. Инфраструктура PKI. Задачи PKI
33. Особенности применения ЭП в информационных и аналитических системах.
34. Криптографические стандарты PKI
35. Топологии PKI

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

**ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ**

1. Общая структура информационных и аналитических систем.
2. Базовые информационные процессы в информационных и аналитических системах.
3. Аналитические системы безопасности: понятия и задачи
4. Современные методы защиты информации в информационных и аналитических системах;
5. Методики выявления основных угрозы безопасности информации, в информационных и аналитических системах;
6. Построение модели нарушителя в информационных и аналитических системах;

7. Защитные механизмы информационной безопасности информационных и аналитических системах;
8. Практика использования информационно-аналитические систем безопасности в профессиональной деятельности;
9. Направления и тенденции совершенствования в вопросах безопасности современных информационно-аналитических систем
10. Регламенты работы с информационно-аналитическими системами
11. Комплект положений, инструкций и других организационно-распорядительных документов для информационно-аналитических системам
12. организационные проблемы информационной безопасности информационно-аналитических систем
13. Технические проблемы информационной безопасности информационно-аналитических систем
14. Требования к организации и функционированию информационно-аналитических систем
15. Модельное представление информационно-аналитических систем
16. Защищенные каналы передачи информации. ESP в туннельном режиме. SSL
17. Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP).
18. Честный обмен цифровыми подписями и его приложения. Схема Asokan - Slioup - Waidner

**ВОПРОСЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ**

1. Общая структура информационных и аналитических систем.
2. Базовые информационные процессы в информационных и аналитических системах.
3. Аналитические системы безопасности: понятия и задачи
4. Современные методы защиты информации в информационных и аналитических системах;
5. Методики выявления основных угрозы безопасности информации, в информационных и аналитических системах;
6. Построение модели нарушителя в информационных и аналитических системах;
7. Защитные механизмы информационной безопасности информационных и аналитических системах;
8. Практика использования информационно-аналитические систем безопасности в профессиональной деятельности;
9. Направления и тенденции совершенствования в вопросах безопасности современных информационно-аналитических систем
10. Регламенты работы с информационно-аналитическими системами
11. Комплект положений, инструкций и других организационно-распорядительных документов для информационно-аналитических системам
12. организационные проблемы информационной безопасности информационно-аналитических систем
13. Технические проблемы информационной безопасности информационно-аналитических систем
14. Требования к организации и функционированию информационно-аналитических систем
15. Модельное представление информационно-аналитических систем
16. Защищенные каналы передачи информации. ESP в туннельном режиме. SSL
17. Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP).
18. Честный обмен цифровыми подписями и его приложения. Схема Asokan - Slioup - Waidner

**Перечень тем лабораторных работ:**

**Лабораторная работа №1.** Управление правами доступа и разрешениями к создаваемым объектам БД подсистем управления данными информационных и аналитических систем;
**Лабораторная работа №2.** Установка и конфигурирование сервера RADIUS;
**Лабораторная работа №3.** Обеспечение защищенного административного доступа с применением AAA и RADIUS;
**Лабораторная работа №4.** Практика конфигурирования AAA на маршрутизаторах Cisco;
**Лабораторная работа №5.** Практика конфигурирования site-to-site VPN;
**Лабораторная работа №6.** Практика конфигурирования защищенного доступа к удаленной сети.

## 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.
4. Мишин Д.В. Анализ защищенности распределенных информационных систем. Идентификация ресурсов корпоративной сети передачи данных : практикум для вузов по направлению "Информационная безопасность" / Д. В. Мишин, Ю. М. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2012 .— 94 с. ISBN 978-5-9984-0295-1.
5. 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=423927

**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. Воронин А.А. Вычислительные сети : учебное пособие / А. А. Воронин ; Владимирский государственный университет (ВлГУ) .— Владимир : 2011 .— 87 с.
4. Основы информационных и телекоммуникационных технологий. Сетевые информационные технологии : учеб. пособие / В.Б. Попов. - М. : Финансы и статистика, 2015. - http://www.studentlibrary.ru/book/ISBN5279030139.html 224 с.
5. Введение в сетевые технологии: Элементы применения и администрирования сетей: учеб. пособие / С.В. Никифоров.- 2-е изд. - М. : Финансы и статистика, 2007. - http://www.studentlibrary.ru/book/ISBN9785279032808.html 224 с.

**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. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.
4. «Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;
5. 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 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.

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 2017/2018 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

**АЛГОРИТМЫ НА ГРАФАХ И СЕТЯХ**
(наименование дисциплины)

Направление подготовки 10.05.04 «Информационно-аналитические системы безопасности»

Профиль / программа подготовки _____

Уровень высшего образования специалитет

Форма обучения очная

Владимир 2016

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: доцент кафедры ИЗИ к.т.н. Монахов Ю.М.
(подпись, должность, ФИО)

а) основная литература:

Дискретная оптимизация. Модели, методы, алгоритмы решения прикладных задач / Струченков В.И. - М. : СОЛОН-ПРЕСС, 2016. - http://www.studentlibrary.ru/book/ISBN9785913591814.html 192 с.

б) дополнительная литература: _____

в) периодические издания: _____

в) интернет-ресурсы: _____