УТ7012-15-16

**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

## СОВРЕМЕННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ И ИХ БЕЗОПАСНОСТЬ

(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) |
|---|---|---|---|---|---|---|
| А | 3/108 | 36 | 36 | | 36 | Зачет |
| Итого | 3/108 | 36 | 36 | | 36 | Зачет |

**Владимир 2016**

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Целями освоения дисциплины «Современные платежные системы и их безопасность»** являются обеспечение профессиональной подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана специальности 10.05.04 «Информационно-аналитические системы безопасности», ознакомление студентов с современными платежными системами и перспективами их развития. В курсе дается студентам базовая подготовка по технологиям электронных систем взаиморасчетов, описываются угрозы информационной безопасности и защитные механизмы обеспечения безопасности электронных платежных систем.

Задачами изучения дисциплины является ознакомление студентов:- с теорией и практикой организации современных электронных платёжных, в том числе банковских систем России; -основными критериями показателей уровня безопасности платежных систем; -угрозах и защитных механизмах обеспечения информационной безопасности в платежных системах; - используемых стандартах и протоколах информационного обмена в электронных платежных системах; - основными источниками и видами опасностей и угроз экономической безопасности платежной системы; - с основными опасностями и угрозами бизнесу, методиками оценки хозяйственных рисков; - с возможными способами защиты от компьютерных атак на платежные системы.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.25). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

Дисциплина изучается на пятом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасности», «Безопасность информационных и аналитических систем», «Принципы построения, проектирования и эксплуатации автоматизированных информационных систем», «Техническая защита информации», «Финансы, денежное обращение и кредит» 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 «Финансовый анализ», «Основы финансового права», «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 -18 – способностью выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные;

ПСК-1.1. – способностью разрабатывать, анализировать и применять формализованные модели и методы решения аналитических задач.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

**1) Знать:** - сущность и виды экономической безопасности современных электронных платёжных систем; - внутренние и внешние угрозы в платёжных системах; - систематизацию и методы оценки угроз; - методы оценки экономических процессов (бизнес-процессов) в платёжных системах; - меры и механизмы обеспечения безопасности платёжных систем; основы организации диагностики и мониторинга безопасности платёжных систем (ПК-18; ПСК-1.1);

**2) Уметь:** - выявлять внутренние и внешние угрозы для платёжных систем, оценить их; - использовать экономические индикаторы и риски при оценке безопасности состояния платёжных систем; - выявлять основные направления повышения надежности и результативности защиты информации в платёжных системах (ПК-18; ПСК-1.1);

**3) Владеть:** - информацией о структуре современных платежных систем и проблемах их совершенствования; информацией о видах расчётов и особенностях функционирования расчётной системы Банка России, межбанковских расчётов и их современных технологий, рынок расчётных услуг банков; - приемами анализа проблем обеспечения экономической безопасности организации и безопасности платёжных систем организации; - методами оценки внутренних и внешних угроз безопасности платёжных систем, - пороговыми значениями финансовых показателей экономической безопасности для функционирования платёжных систем (ПК-18; ПСК-1.1).

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

- способность разрабатывать, оформлять и реализовывать политики информационной безопасности для современных электронных корпоративных информационных платёжных 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 промежуточной аттестации *(по семестрам)* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические занятия | Лабораторные работы | Контрольные работы, | СРС | КП / КР | | |
| 1 | Федеральный закон "О национальной платежной системе". Общие положения | А | 1 | 2 | 2 | | | 2 | | 2 (50%) | - |
| 2 | Порядок осуществления перевода денежных средств, и использования электронных средств платежа | А | 2 | 2 | 2 | | | 2 | | 1 (25%) | |
| 3 | Требования к организации и функционированию платежных систем | А | 3 | 2 | 2 | | | 2 | | 2 (50%) | |
| 4 | Стандарт Банка России (СТО БР ИББС-1.0). | А | 4 | 2 | 2 | | | 2 | | 2 (50%) | |
| 5 | Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS). | А | 5 | 2 | 2 | | | 2 | | 1 (25%) | |
| 6 | Требования стандарта PCI DSS. | А | 6 | 2 | 2 | | | 2 | | 2 (50%) | Рейтинг-контроль №1 |
| 7 | Детализация требований по защите данных платежных карт по PCI DSS. | А | 7 | 2 | 2 | | | 2 | | 2 (50%) | |
| 8 | Детализация требований по строгому контролю доступа по PCI DSS. | А | 8 | 2 | 2 | | | 2 | | 1 (25%) | |
| 9 | Детализация требований к мониторингу и тестированию. | А | 9 | 2 | 2 | | | 2 | | 2 (50%) | |
| 10 | Программа управления уязвимостями. Поддержание политики информационной безопасности. | А | 10 | 2 | 2 | | | 2 | | 1 (25%) | |
| 11 | Стратегии достижения соответствия стандарту. | А | 11 | 2 | 2 | | | 2 | | 2 (50%) | |
| 12 | Обучение и повышение осведомленности сотрудников по вопросам ИБ. | А | 12 | 2 | 2 | | | 2 | | 1 (25%) | Рейтинг-контроль №2 |
| 13 | Модельное представление систем электронных платежей | А | 13 | 2 | 2 | | | 2 | | 2 (50%) | |
| 14 | Неанонимные системы электронных платежей, работающие в реальном масштабе времени. | А | 14 | 2 | 2 | | | 2 | | 1 (25%) | |
| 15 | Анонимные системы электронных платежей, работающие в реальном масштабе времени | А | 15 | 2 | 2 | | | 2 | | 2 (50%) | |
| 16 | Системы электронных платежей на базе затемненной подписи. Защищенные каналы передачи информации. ESP в туннельном режиме. SSL | А | 16 | 2 | 2 | | | 2 | | 2 (50%) | |
| 17 | Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP). Протокол записи (SSL RP). | А | 17 | 2 | 2 | | | 2 | | 2 (50%) | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 18 | Честный обмен цифровыми подписями и его приложения. Многосторонние транзакции. Электронные аукционы | А | 18 | 2 | 2 | | | 2 | | 1 (25%) | Рейтинг-контроль №3 |
| Всего | | | | 36 | 36 | | | 36 | | 30 (42%) | Зачет |

**Содержание дисциплины «Современные платежные системы и их безопасность»**

**Раздел 1.** Федеральный закон "О национальной платежной системе". Общие положения.

**Раздел 2.** Порядок осуществления перевода денежных средств, и использования электронных средств платежа Субъекты национальной платежной системы и требования к их деятельности.

**Раздел 3.** Требования к организации и функционированию платежных систем.

**Раздел 4.** Стандарт Банка России (СТО БР ИББС-1.0). Обеспечение ИБ организаций банковской системы Российской Федерации. Общие положения, цели и задачи стандарта Стандарт Банка России (СТО БР ИББС-1.2). Обеспечение ИБ организаций банковской системы Российской Федерации. Методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.

**Раздел 5.** Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS). Цели и задачи стандарта. Обзор стандарта PCI DSS и сопутствующих стандартов.

**Раздел 6.** Требования стандарта PCI DSS. Процесс проведения аудита на соответствие требованиям PCI DSS.

**Раздел 7.** Детализация требований по защите данных платежных карт по PCI DSS.

**Раздел 8.** Детализация требований по строгому контролю доступа по PCI DSS. Детализация требований по построению и поддержанию защищенной сети по PCI DSS.

**Раздел 9.** Детализация требований к мониторингу и тестированию.

**Раздел 10.** Программа управления уязвимостями. Поддержание политики информационной безопасности.

**Раздел 11.** Стратегии достижения соответствия стандарту. Подготовка нормативной документации. Выбор оптимальных технических решений.

**Раздел 12.** Обучение и повышение осведомленности сотрудников по вопросам ИБ. Риск-ориентированный подход и PCI DSS

**Раздел 13.** Модельное представление систем электронных платежей

**Раздел 14.** Неанонимные системы электронных платежей, работающие в реальном масштабе времени. Неанонимные автономные системы электронных платежей

**Раздел 15.** Анонимные системы электронных платежей, работающие в реальном масштабе времени

**Раздел 16.** Системы электронных платежей на базе затемненной подписи. Защищенные каналы передачи информации. ESP в туннельном режиме. SSL

**Раздел 17.** Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP). Протокол записи (SSL RP).

**Раздел 18.** Честный обмен цифровыми подписями и его приложения. Схема Asokan - Slioup – Waidner. Многосторонние транзакции. Электронные аукционы

## 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**

- Федеральный закон "О национальной платежной системе". Общие положения
- Порядок осуществления перевода денежных средств, и использования электронных средств платежа
- Требования к организации и функционированию платежных систем
- Стандарт Банка России (СТО БР ИББС-1.0).
- Обеспечение ИБ организаций банковской системы Российской Федерации.
- Стандарт Банка России (СТО БР ИББС-1.2). Обеспечение ИБ организаций банковской системы Российской Федерации.

- Методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0
- Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS). Цели и задачи стандарта.

**Вопросы рейтинг-контроля №2**

- Требования стандарта PCI DSS.
- Процесс проведения аудита на соответствие требованиям PCI DSS.
- Детализация требований по защите данных платежных карт по PCI DSS.
- Детализация требований по строгому контролю доступа по PCI DSS.
- Детализация требований по построению и поддержанию защищенной сети по PCI DSS.
- Детализация требований к мониторингу и тестированию защищенной сети по PCI DSS.
- Программа управления уязвимостями по PCI DSS.
- Поддержание политики информационной безопасности для систем электронных платежей.

**Вопросы рейтинг-контроля №3**

- Стратегии достижения соответствия стандарту PCI DSS. Выбор оптимальных технических
- Риск-ориентированный подход и PCI DSS
- Модельное представление систем электронных платежей
- Системы электронных платежей на базе затемненной подписи
- Защищенные каналы передачи информации. ESP в туннельном режиме. SSL
- Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP).
- Протокол записи (SSL RP).
- Честный обмен цифровыми подписями и его приложения. Схема Asokan - Slioup - Waidner
- Многосторонние транзакции. Электронные аукционы

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

1. Федеральный закон "О национальной платежной системе". Общие положения
2. Порядок осуществления перевода денежных средств, и использования электронных средств платежа
3. Требования к организации и функционированию платежных систем
4. Стандарт Банка России (СТО БР ИББС-1.0).
5. Обеспечение ИБ организаций банковской системы Российской Федерации.
6. Стандарт Банка России (СТО БР ИББС-1.2). Обеспечение ИБ организаций банковской системы Российской Федерации.
7. Методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0
8. Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS). Цели и задачи стандарта.
9. Требования стандарта PCI DSS.
10. Процесс проведения аудита на соответствие требованиям PCI DSS.
11. Детализация требований по защите данных платежных карт по PCI DSS.
12. Детализация требований по строгому контролю доступа по PCI DSS.
13. Детализация требований по построению и поддержанию защищенной сети по PCI DSS.
14. Детализация требований к мониторингу и тестированию защищенной сети по PCI DSS.
15. Программа управления уязвимостями по PCI DSS.
16. Поддержание политики информационной безопасности для систем электронных платежей.
17. Стратегии достижения соответствия стандарту PCI DSS. Выбор оптимальных технических
18. Риск-ориентированный подход и PCI DSS

19. Модельное представление систем электронных платежей
20. Системы электронных платежей на базе затемненной подписи
21. Защищенные каналы передачи информации. ESP в туннельном режиме. SSL
22. Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP).
23. Протокол записи (SSL RP).
24. Честный обмен цифровыми подписями и его приложения. Схема Asokan - Slioup - Waidner
25. Многосторонние транзакции. Электронные аукционы

**Темы практических занятий:**

1. Обнаружение узлов корпоративной сети. Информационные ICMP сообщения, TCP (TCP-PING), UDP (UDP-PING), ARP (ARP-PING).
2. Основные средства определения маршрутов IP-пакетов - PING, TRACEROUTE. Дополнительные средства определения маршрутов IP-ПАКЕТОВ - NMAP, TRACEMAP, MRT
3. Идентификация статуса TCP-портов (TCP-CONNECT. SYN-SCAN)
4. Методы скрытого сканирования (STEALTH TCP SCANNING METHODS)
5. Идентификация прикладных сетевых служб методом анализа особенностей реализации (SMTP)
6. Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Обнаружение активных узлов сети. Анализ DNS.
7. Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Идентификация сетевых служб и операционной системы узлов сети.
8. Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Анализ трафика.
9. Программные инструменты специального дистрибутива KALI Linux для стресс тестирования о распределенной АС.

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

- Понятие платежной системы и ее элементов. Типы платежных систем.
- Система платежей и расчетов и ее основные элементы.
- Роль центрального банка в современной платежной системе
- Виды платежей и расчетов: наличные и безналичные (включая электронные);
- Виды платежей и расчетов: одногородние, иногородние, международные.
- Система безналичных расчетов и ее элементы.
- Формы безналичных расчетов - банковский перевод и открытый счет;
- Формы безналичных расчетов - аккредитивная форма расчетов;
- Формы безналичных расчетов - инкассовая форма расчетов.
- Современные платежные системы. Национальная платежная система
- Современные платежные системы. Региональные платежные системы
- Современные платежные системы. Международные системы платежей и расчетов
- Эволюция платежной системы и формирование ее современной инфраструктуры.
- Межбанковские расчеты. Безопасность межбанковских расчетов
- История, общее описание и назначение стандарта PCI DSS.
- Системы платежных карт, организации участвующие в PCI.
- Обзор документов PCI Security Standards Council (PCI SSC).
- Разделение ответственности между PCI SSC, QSA и международными платежными системами.
- Обзор сопутствующих стандартов PA DSS и PCI PED, общее описание, назначение и область применения стандартов.
- Основные требования к подтверждению соответствия PCI DSS для различных типов организаций.

- Требования по аттестации, аудиту и выявлению уязвимостей. Требования стандарта к формированию границ проверки.
- Влияние архитектуры систем на объемы и сроки аудита.
- Проведение тестов на проникновение по PCI DSS.
- Безопасность приложений по PCI DSS.
- Безопасность беспроводных сетей по PCI DSS.
- Рекомендации по выбору услуг QSA и ASV. Планирование и проведение аудита, сбор, обработка и хранение свидетельств аудита.
- Взаимодействие с QSA и ASV на разных этапах аудита. Представление отчета аудитором, методы и пути разрешения спорных вопросов.
- План устранения несоответствий (Action Plan): разработка, согласование, реализация.
- Типы данных, требования к критичным данным авторизации, защита при обработке и хранении для защиты данных платежных карт.
- Объекты и методы защиты, применение компенсационных мер защиты данных платежных карт.
- Защита данных при передаче по сетям: классификация сетей, методы защиты данных, политики и процедуры обращения с данными карт при передаче по сетям.
- Физическая безопасность: требования к помещениям, в которых обрабатывается информация карт, режим разграничения доступа в помещения, идентификация персонала и посетителей, безопасность серверного и офисного оборудования, кабельной инфраструктуры внутри офиса.
- Управление носителями информации в работе и при архивном хранении.
- Средства контроля доступа к данным, аутентификация и авторизация пользователей.
- Документирование политик управления доступом к данным, процедур хранения, резервного копирования и уничтожения, требований физической безопасности в политиках и процедурах.
- Доступ к сетевым ресурсам и данным карт, обеспечение регистрации действий сотрудников и системных событий.
- Журналы аудита событий: анализ, настройка, защита, архивация.
- Системы централизованного сбора и анализа событий.
- Системы контроля целостности и обнаружения изменений данных.
- Мониторинг беспроводных сетей и точек доступа.
- Использование сетевых систем мониторинга, обнаружения и предупреждения вторжений.
- Обеспечение целостности и синхронизации событий с разных систем сети.
- Отражение требований стандарта в регламентирующих документах.
- Регулярная идентификация, анализ, тестирование и внедрение обновлений.
- Процесс управления обновлениями. Управление конфигурациями и настройками.
- Безопасность при разработке и поддержке приложений: применимость требования стандарта, уязвимости приложений и распространенные атаки.
- Среда разработки и эксплуатации. Средства управления изменениями и конфигурациями.
- Стандарты безопасной разработки приложений. Тестирование кода приложений, сертификация и авторизация перед внедрением.
- Выявление уязвимостей: внешние и внутренние сканирования. Проведение тестов на проникновение.
- Политики использования персональных устройств, сменных носителей, систем обмена сообщениями, технологий беспроводного и удаленного доступа.
- Ответственность для сотрудников и контрагентов. Распределение обязанностей по обеспечению политики ИБ в целом, документированию и доведению политик до сотрудников и контрагентов, администрированию и контролю доступа, взаимодействию с сервис – провайдерами, мониторингу и реагированию на инциденты, проверке персонала.
- Программа повышения осведомленности сотрудников в ИБ. Пересмотр и обновление политики.

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**а) Основная литература:**

1. Мошенничество в платежной сфере: Бизнес-энциклопедия / Л.В. Лямин, Н. Пятиизбянцев, А.В. Пухов и др. - М.: Интеллектуальная Литература, 2015. - 345 с. ISBN 978-5-9907223-2-3 Режим доступа: http://znanium.com/
2. Достов, В.Л. Электронные финансы. Мифы и реальность / В.Л. Достов, П.М. Шуст, А.А. Валинурова, А.В. Пухов. - М.: КНОРУС: ЦИПСиР, 2012. - 232 с. - ISBN 978-5-406-02186-6. Режим доступа: http://znanium.com/catalog.php?bookinfo=522004
3. Платежные технологии: системы и инструменты: научно-популярное издание / Муссель К.М. - М.:ЦИПСиР, 2015. - 288 с. ISBN 978-5-406-04189-5 Режим доступа: http://znanium.com/catalog.php?bookinfo=556619
4. Алексанов, А. К. Безопасность карточного бизнеса : бизнес-энциклопедия / А. К. Алексанов, И. А. Демчев, А. М. Доронин и др. - М.: Московская финансово-промышленная академия: ЦИПСиР, 2012. - 432 с. - ISBN 978-5-4257-0018-6. Режим доступа: http://znanium.com/catalog.php?bookinfo=407828

**б) Дополнительная литература:**

1. Парамонов, Л. С. Электронные деньги и мобильные платежи. Энциклопедия / Л. С. Парамонов, М. В. Мамута, А. В. Пухов. - М. : КНОРУС : ЦИПСиР, 2009. - 368 с. - ISBN 978-5-390-00511-8. Режим доступа: http://znanium.com/catalog.php?bookinfo=408085
2. Лямин, Л. В. Дистанционное банковское обслуживание / Л. В. Лямин, А. В. Пухов. - М.: КНОРУС: ЦИПСиР, 2010. - 328 с. - ISBN 978-5-406-00350-3. Режим доступа: http://znanium.com/catalog.php?bookinfo=407882
3. Голдовский, И. М. Банковские микропроцессорные карты / И. М. Голдовский. - М.: ЦИПСиР: Альпина Паблишерз, 2010. - 686 с. - ISBN 978-5-9614-1233-8. Режим доступа: http://znanium.com/catalog.php?bookinfo=407812
4. Кочергин, Д. А. Электронные деньги : учеб. пособие / Д. А. Кочергин. - М.: Маркет ДС : ЦИПСиР, 2011. - 424 с. - ISBN 978-5-94416-126-0. Режим доступа: http://znanium.com/catalog.php?bookinfo=408083
5. Мартынов, В. Г. Электронные деньги. Интернет платежи / В. Г. Мартынов, А. Ф. Андреев, В. А. Кузнецов и др. - М.: Маркет ДС : ЦИПСиР, 2010. - 176 с. - ISBN 978-5-94416-061-4. Режим доступа: http://znanium.com/catalog.php?bookinfo=408087

**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. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
2. 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 2017/18 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: _____