УП2015

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального 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

Оценка и контроль обеспечения информационной 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)
2	5/180	18		18	144	Зачет с оценкой
Итого	5/180	18		18	144	Зачет с оценкой

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Оценка и контроль обеспечения информационной 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 администрированием безопасности информационных систем, с типовой структурой корпоративной информационной системы, с методиками управления безопасностью ИС, методах анализа и активного аудита безопасности такого класса систем, а также с типовыми защитными средствами в корпоративной информационно-вычислительной среде.

Задачей дисциплины «Оценка и контроль обеспечения информационной безопасности» является изучение программно-аппаратных средств защиты информации, оценка эффективности их применения, освоение технологии администрирования безопасностью в корпоративных информационных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО МАГИСТРАТУРЫ

Данная дисциплина относится к дисциплинам по выбору вариативной части блока Б1 (код Б1.В.ДВ.2). 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 «Корпоративные информационные системы» 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 «Методы информационно-аналитической работы», «Защищённые информационные системы», «Организационно-правовые механизмы обеспечения информационной безопасности», «Управление информационной безопасностью» 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-10 – способностью проводить аттестацию объектов информатизации по требованиям безопасности информации.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** - основные понятия, цели и задачи администрирования безопасности информационных систем, сущность и составляющие; - принципы организации и этапы процессов администрирования безопасности; факторы, влияющие на организацию защиты информации; - методы анализа и оценки угроз защищаемой информации; - технологические и организационные вопросы администрирования безопасности информационной системы, администрирование системы защиты; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности (ПК-9; ПК-10);

2) ***Уметь:*** - определять состав программно-технических средств защиты информации; - выявлять угрозы защищаемой информации информационной системы, определять степень их опасности, разрабатывать стратегию администрирования системой защиты информации объектов с учетом условий ее функционирования; - использовать методы и средства, необходимые для организации управления и функционирования системы защиты информации; - реализовывать планы функционирования системы защиты информации, осуществлять ее текущее администрирование; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности (ПК-9; ПК-10);

3) ***Владеть:*** - современными программными средствами, в которых реализованы методы защиты информации информационных систем; - решать задачи профессиональной области, используя известные математические методы, программные и аппаратно-технические решения; - навыками управления информационной безопасностью простых объектов (ПК-9; ПК-10).

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

- способность проверять соответствие имеющихся защищенных информационных систем требованиям отечественных и зарубежных стандартов в области информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зачетных единицы, 180 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.	Обнаружение узлов сети. icmp echo request.	2	1-2	2		2		14		1/25%	
2.	Обнаружение узлов сети средствами протокола tcp (tcp-ping).	2	3-4	2		2		16		2/50%	
3.	Обнаружение узлов сети средствами протокола arp (arp-ping).	2	5-6	2		2		16		1/25%	Рейтинг-контроль №1
4.	Дополнительные средства определения маршрутов ip-пакетов - nmap, tracemap, mrt, идентификация статуса tcp-портов (tcp-connect. syn-scan).	2	7-8	2		2		16		2/50%	
5.	Методы скрытого сканирования (stealth tcp scanning methods).	2	9-10	2		2		18		1/25%	
6.	Сканирование ip протокола. Идентификация прикладных служб. метод анализа стандартных приглашений (banner grabbing).	2	11-12	2		2		16		1/25%	Рейтинг-контроль №2
7.	Идентификация прикладных сетевых служб методом анализа особенностей реализации (smtp).	2	13-14	2		2		18		2/50%	
8.	Идентификация службы электронной почты.	2	15-16	2		2		16		2/50%	
9.	Активное исследование стека tcp/ip.	2	17-18	2		2		14		2/50%	Рейтинг-контроль №3
Всего				18		18		144		14/39%	Зачет с оценкой

Содержание дисциплины Оценка и контроль обеспечения информационной безопасности»

Раздел 1. Обнаружение узлов сети. icmp echo request. Обнаружение узлов сети. информационные icmp сообщения.

Раздел 2. Обнаружение узлов сети средствами протокола tcp (tcp-ping). Обнаружение узлов сети средствами протоколов udp (udp-ping), ip.

Раздел 3. Обнаружение узлов сети средствами протокола arp (arp-ping). Основные средства определения маршрутов ip-пакетов - ping, traceroute.

Раздел 4. Дополнительные средства определения маршрутов ip-пакетов - nmap, tracemap, mrt, идентификация статуса tcp-портов (tcp-connect. syn-scan).

Раздел 5. Методы скрытого сканирования (stealth tcp scanning methods). Методы сканирования udp-портов (udp port scanning).

Раздел 6. Сканирование ip протокола. Идентификация прикладных служб. метод анализа стандартных приглашений (banner grabbing).

Раздел 7. Идентификация прикладных сетевых служб методом анализа особенностей реализации (smtp).

Раздел 8. Идентификация службы электронной почты методом mail-bouncing. Специализированные программные средства идентификации прикладных служб.

Раздел 9. Активное исследование стека tcp/ip. Специализированные программные средства активного исследования стека tcp/ip. Пассивное исследование стека в задаче идентификации ОС

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Оценка и контроль обеспечения информационной 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

- Что понимается под идентификацией узлов корпоративной сети передачи данных?
- Какие протоколы стека TCP/IP могут применяться при идентификации узлов?
- Протокол ICMP. Назначение, формат пакета протокола ICMP.
- Назовите основные способы обнаружения узлов сети средствами протокола ICMP.
- Синтаксис и основные опции утилиты ping.
- Назовите основные недостатки применения утилиты ping при решении задачи идентификации узлов КСПД.

- Технология PING SWEEP, достоинства и недостатки.
- Синтаксис и основные опции утилиты fping.
- Синтаксис и основные режимы сетевого сканера nmap.
- Методы обнаружения узлов сети средством информационных запросов TimeStamp Request, Information Request, Address Mask Request.
- Протокол TCP, назначение, TCP соединение, флаги.
- Формат сегмента протокола TCP, TCP-порты.

Вопросы рейтинг-контроля №2

- TCP-sweep. Достоинства и недостатки метода TCP-sweep.
- Синтаксис и основные опции утилиты hping3.
- Протокол UDP. Режим передачи данных без установления соединения.
- Формат дейтаграммы протокола UDP, UDP -порты.
- Метод UDP Discovery. Достоинства и недостатки метода.
- Протокол IP. Адресация.
- Формат пакета протокола IP.
- Метод идентификации с помощью IP фрагментов.
- Метод идентификации отправкой IP пакета ошибочной длины.
- Метод идентификации отправкой IP пакета неподдерживаемого протокола.
- Протокол ARP. Адресация канального уровня ISO OSI.
- Формат дейтаграммы ARP.
- Синтаксис и основные опции утилиты arping.

Вопросы рейтинг-контроля №3

- Протокол ARP. Адресация канального уровня ISO OSI.
- Формат дейтаграммы ARP.
- Синтаксис и основные опции утилиты arping.
- Метод arping. Достоинства и недостатки.
- Методы определения маршрутов передачи данных в сетях TCP/IP.
- Утилиты определения маршрутов передачи данных в сетях TCP/IP.
- Метод определения маршрута Record Route. Достоинства и недостатки метода.
- Утилита traceroute. Принцип определения маршрутов.
- Использование протоколов ICMP и TCP при определении маршрутов.
- Утилита tcptraceroute.
- Сканер nmap как инструмент исследования топологии.
- Утилита tracemap. Визуализация маршрутов.
- Утилита диагностики сети mtr. Синтаксис и основные опции mrt.

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

1. Что понимается под идентификацией узлов корпоративной сети передачи данных?
2. Какие протоколы стека TCP/IP могут применяться при идентификации узлов?
3. Протокол ICMP. Назначение, формат пакета протокола ICMP.
4. Назовите основные способы обнаружения узлов сети средствами протокола ICMP.
5. Синтаксис и основные опции утилиты ping.
6. Назовите основные недостатки применения утилиты ping при решении задачи идентификации узлов КСПД.
7. Технология PING SWEEP, достоинства и недостатки.
8. Синтаксис и основные опции утилиты fping.
9. Синтаксис и основные режимы сетевого сканера nmap.

10. Методы обнаружения узлов сети средством информационных запросов TimeStamp Request, Information Request, Address Mask Request.
11. Протокол TCP, назначение, TCP соединение, флаги.
12. Формат сегмента протокола TCP, TCP-порты.
13. TCP-sweep. Достоинства и недостатки метода TCP-sweep.
14. Синтаксис и основные опции утилиты hping3.
15. Протокол UDP. Режим передачи данных без установления соединения.
16. Формат дейтаграммы протокола UDP, UDP -порты.
17. Метод UDP Discovery. Достоинства и недостатки метода.
18. Протокол IP. Адресация.
19. Формат пакета протокола IP.
20. Метод идентификации с помощью IP фрагментов.
21. Метод идентификации отправкой IP пакета ошибочной длины.
22. Метод идентификации отправкой IP пакета неподдерживаемого протокола.
23. Протокол ARP. Адресация канального уровня ISO OSI.
24. Формат дейтаграммы ARP.
25. Синтаксис и основные опции утилиты arping.
26. Метод arping. Достоинства и недостатки.
27. Методы определения маршрутов передачи данных в сетях TCP/IP.
28. Утилиты определения маршрутов передачи данных в сетях TCP/IP.
29. Метод определения маршрута Record Route. Достоинства и недостатки метода.
30. Утилита traceroute. Принцип определения маршрутов.
31. Использование протоколов ICMP и TCP при определении маршрутов.
32. Утилита tcptraceroute.
33. Сканер nmap как инструмент исследования топологии.
34. Утилита tracemap. Визуализация маршрутов.
35. Утилита диагностики сети mtr. Синтаксис и основные опции mrt.

Темы лабораторных работ:

Лабораторная работа № 1.

Лабораторная работа №1.ОБНАРУЖЕНИЕ УЗЛОВ СЕТИ. ICMP ECHO REQUEST (Утилита PING)

Лабораторная работа №2. ОБНАРУЖЕНИЕ УЗЛОВ СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP)

Лабораторная работа №3. ОБНАРУЖЕНИЕ УЗЛОВ СЕТИ. ИНФОРМАЦИОННЫЕ ICMP СООБЩЕНИЯ

Лабораторная работа №4. ОБНАРУЖЕНИЕ УЗЛОВ СЕТИ СРЕДСТВАМИ ПРОТОКОЛА TCP (TCP-PING)

Лабораторная работа №5. ОБНАРУЖЕНИЕ УЗЛОВ СЕТИ СРЕДСТВАМИ ПРОТОКОЛОВ UDP (UDP-PING), IP

Лабораторная работа №6. ОБНАРУЖЕНИЕ УЗЛОВ СЕТИ СРЕДСТВАМИ ПРОТОКОЛА ARP (ARP-PING)

Практическое задание к разделу I

Лабораторная работа №7. ОСНОВНЫЕ СРЕДСТВА ОПРЕДЕЛЕНИЯ МАРШРУТОВ IP-ПАКЕТОВ - PING, TRACEROUTE

Лабораторная работа №8. ДОПОЛНИТЕЛЬНЫЕ СРЕДСТВА ОПРЕДЕЛЕНИЯ МАРШРУТОВ IP-ПАКЕТОВ - NMAP, TRACEMAP, MRT

Лабораторная работа №9. ИДЕНТИФИКАЦИЯ СТАТУСА TCP-ПОРТОВ (TCP-CONNECT. SYN-SCAN)

Лабораторная работа №10. МЕТОДЫ СКРЫТОГО СКАНИРОВАНИЯ (STEALTH TCP SCANNING METHODS)

Лабораторная работа №11. МЕТОДЫ СКРЫТОГО СКАНИРОВАНИЯ (ACK PROBE SCANNING, TCP FRAGMENTATION SCANNING)

Лабораторная работа №12. МЕТОДЫ СКАНИРОВАНИЯ UDP-ПОРТОВ (UDP PORT SCANNING). СКАНИРОВАНИЕ IP ПРОТОКОЛА

Вопросы и задания к самостоятельной работе магистрантов:

- Что понимается под идентификацией узлов корпоративной сети передачи данных?
- Какие протоколы стека TCP/IP могут применяться при идентификации узлов?
- Протокол ICMP. Назначение, формат пакета протокола ICMP.
- Назовите основные способы обнаружения узлов сети средствами протокола ICMP.
- Синтаксис и основные опции утилиты ping.
- Назовите основные недостатки применения утилиты ping при решении задачи идентификации узлов КСПД.
- Технология PING SWEEP, достоинства и недостатки.
- Синтаксис и основные опции утилиты fping.
- Синтаксис и основные режимы сетевого сканера nmap.
- Методы обнаружения узлов сети средством информационных запросов TimeStamp Request, Information Request.
- Протокол TCP, назначение, TCP соединение, флаги.
- Формат сегмента протокола TCP, TCP-порты.
- TCP-sweep. Достоинства и недостатки метода TCP-sweep.
- Синтаксис и основные опции утилиты hping3.
- Протокол UDP. Режим передачи данных без установления соединения.
- Формат дейтаграммы протокола UDP, UDP -порты.
- Метод UDP Discovery. Достоинства и недостатки метода.
- Протокол IP. Адресация.
- Формат пакета протокола IP.
- Метод идентификации с помощью IP фрагментов.
- Метод идентификации отправкой IP пакета ошибочной длины.
- Метод идентификации отправкой IP пакета неподдерживаемого протокола.
- Протокол ARP. Адресация канального уровня ISO OSI.
- Формат дейтаграммы ARP.
- Синтаксис и основные опции утилиты arping.
- Метод arping. Достоинства и недостатки.
- Методы определения маршрутов передачи данных в сетях TCP/IP.
- Утилиты определения маршрутов передачи данных в сетях TCP/IP.
- Метод определения маршрута Record Route. Достоинства и недостатки метода.
- Утилита traceroute. Принцип определения маршрутов.
- Использование протоколов ICMP и TCP при определении маршрутов.
- Утилита tcptraceroute.
- Сканер nmap как инструмент исследования топологии.
- Утилита tracemap. Визуализация маршрутов.
- Утилита диагностики сети mtr. Синтаксис и основные опции mrt.
- Методы идентификации TCP портов узла КСПД.
- Состояния TCP соединения.
- Метод TCP Connect Scanning.
- Режим сканирования TCP Connect сканера nmap.
- Метод Half-open SYN flag scanning.
- Режим сканирования Half-open SYN flag сканера nmap.
- Достоинства и недостатки методов Stealth TCP scanning.
- Методы Inverse TCP flag scanning.
- ACK flag probe scanning.
- TCP fragmentation scanning.

- Режимы Stealth TCP scanning сканера nmap.
- Методы идентификации UDP-портов узла КСПД.
- Реализация UDP Port Scanning сканером nmap. Опции и режимы сканера.
- Реализация UDP Port Scanning средствами утилит hping3 и netcat. Опции и режимы.
- Задача идентификации сетевых служб. Соответствие TCP/UDP-портов и сетевых служб.
- Методы идентификации версий прикладных служб. Services fingerprinting.
- Метод banner grabbing. Достоинства и недостатки метода.
- Методы анализа особенностей реализации прикладной службы.
- Метод mail-bouncing. Идентификация службы электронной почты.
- Сканер amap. Синтаксис, опции и режимы работы.
- Утилита strobe. Синтаксис, опции и режимы работы.
- Режимы идентификации версий прикладных служб сканера nmap.
- Задача идентификации типа и версии ОС исследуемого узла КСПД.
- Особенности методов активного исследования реализации стека протоколов TCP/IP. Достоинства и недостатки.
- Суть метода TCP|FIN сканирования.
- Суть метода исследования флагом BOGUS.
- Суть метода исследования поля Window TCP заголовка принятого пакета.
- Суть метода исследования изменения ISN ACK-пакета.
- Утилита Xpobe2. Синтаксис, опции.
- Режимы OS fingerprinting сканера nmap.
- Особенности методов пассивного исследования реализации стека протоколов TCP/IP. Достоинства и недостатки.
- Утилита p0f. Синтаксис, опции.

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. 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

б) Дополнительная литература:

1. Офисный шпионаж / Мелтон К., Пилиджан К., Сверчински Д. - М. : Альпина Паблишер, 2013. - http://www.studentlibrary.ru/book/ISBN9785916712070.html. 182 с.
2. 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.
3. 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 «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/

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 2017/2018 учебный год

Протокол заседания кафедры № 1 от 28.08.17 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

Приложение

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

Институт _____

Кафедра _____

Актуализированная
рабочая программа
рассмотрена и одобрена
на заседании кафедры
протокол № ____ от ____ 20__г.

Заведующий кафедрой

_____
(подпись, ФИО)

Актуализация рабочей программы дисциплины

_____
(наименование дисциплины)

Направление подготовки

Профиль/программа подготовки

Уровень высшего образования

Форма обучения

Владимир 20__

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: _____
(подпись, должность, ФИО)

а) основная литература: _____

б) дополнительная литература: _____

в) периодические издания: _____

в) интернет-ресурсы: _____