УП 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)**

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«29» 12 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность информационных систем

(наименование дисциплины)

Направление подготовки 10.03.01 Информационная безопасность

Профиль / программа подготовки Комплексная защита объектов информатизации

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
7	7/252	36	-	36	144	Экзамен (36ч)
Итого	7/252	36	-	36	144	Экзамен (36ч)

Владимир 2015

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Безопасность информационных систем» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность». Целью освоения дисциплины является формирование теоретических знаний и практических навыков по обеспечению информационной безопасности информационных систем.

Задачами дисциплины являются: освоение принципов реализации и основных подходов к оптимальному управлению различными механизмами информационной безопасности в информационных системах. В процессе освоения дисциплины изучаются следующие вопросы: - основные руководящие документы и показатели эффективности системы защиты информации; -комплексный подход к обеспечению ИБ; -цели, стратегии и политика информационной безопасности; -организационные аспекты информационной безопасности; - функции управления информационной безопасностью; - процессный подход для управления информационной безопасностью; - система ответственности в области информационной безопасности; -организация и методика проведения аудита системы управления информационной безопасностью; -алгоритм проведения анализа информационных рисков в КИС предприятия; -аналитические технологии управления ИБ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО БАКАЛАВРИАТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.2). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

Дисциплина изучается на четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасности», «Сети и системы передачи информации», «Методы формализации и моделирования объектов информатизации» «Программно-аппаратные средства защиты информации» по направлению 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Математика»; «Информатика». Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Корпоративные информационные системы», «Техническая защита информации», «Система защиты информации на предприятии».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ

В результате освоения дисциплины бакалавр должен обладать следующими профессиональными компетенциями:

ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-3 – способностью администрировать подсистемы информационной безопасности объекта защиты;

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; - основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; - методы аттестации уровня защищенности информационных систем; - основные методы управления информационной безопасностью (ПК-1; ПК-3);

2) ***Уметь:*** - строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем;- разрабатывать модели угроз и нарушителей информационной безопасности

информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем (ПК-1; ПК-3);

3) ***Владеть***: - методами и средствами выявления угроз безопасности информационным системам; - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экспертизе состояния защищенности информации на объекте защиты; - методами управления информационной безопасностью информационных систем; - методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; - навыками организации и обеспечения режима секретности (ПК-1; ПК-3).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей: - способность разрабатывать, оформлять и реализовывать политики информационной безопасности для современных КИС предприятия.

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	Сетевая разведка. Первичный сбор информации о КИС	7	1-2	4		4		12		4 (50%)	-
2	Методологии Penetration Testing.	7	3	2		2		16		1 (25%)	
3	Методики сканирования сетей	7	4-5	4		4		14		2 (25%)	Рейтинг-контроль №1
4	Инвентаризация ресурсов КИС	7	6-7	4		4		16		4 (50%)	
5	Атаки типа отказ в обслуживании на ресурсы КИС	7	8-9	4		4		12		2 (25%)	
6	Анализ сетевого трафика. Методики и программные средства. Особенности анализа сетевого трафика в коммутируемой среде.	7	10-11	4		4		14		4 (50%)	Рейтинг-контроль №2
7	Атаки типа отказ в обслуживании на ресурсы КИС.	7	12-13	4		4		14		2 (25%)	
8	Методики анализа защищенности беспроводной сети КИС	7	14-15	4		4		16		4 (50%)	
9	Методики анализа защищенности WEB приложений и БД.	7	16-17	4		4		16		2 (25%)	
10	Стандарты тестирования на проникновение	7	18	2		2		14		2 (50%)	Рейтинг-контроль №3
Всего				36		36		144		27 (38%)	Экзамен

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления бакалавра по направлению «Информационная безопасность».

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 бакалаврами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП бакалавриата по направлению 10.03.01, 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 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 СТУДЕНТОВ

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность бакалавра в различных видах учебной деятельности, степень сформированности у бакалавра общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1:

- Методологии Penetration Testing.
- Понятие Footprinting. Этапы.
- Методы сканирования корпоративной сети.
- Методики и программные средства обнаружения активных узлов корпоративной сети.
- Методики и программные средства сканирования TCP/UDP портов узлов корпоративной сети.
- Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.

- Методики и программные средства идентификации операционных систем на узлах корпоративной сети.

Вопросы рейтинг-контроля №2 :

- Методики и программные средства построения сетевых диаграмм КИС.
- Инвентаризация ресурсов КИС. Подходы и методики.
- Инвентаризация ресурсов Linux узлов КИС.
- Инвентаризация ресурсов Windows узлов КИС.
- Применение специальных сетевых протоколов для инвентаризации ресурсов КИС.
- Анализ сетевого трафика. Методики и программные средства.
- Особенности анализа сетевого трафика в коммутируемой среде.
- Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.

Вопросы рейтинг-контроля №3:

- Атаки типа отказ в обслуживании на ресурсы КИС.
- Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.
- Атаки на беспроводные сети КИС.
- Программные средства проведения атак на беспроводные сети КИС.
- Сканеры уязвимостей и методики их применения.
- Особенности применения сканера OpenVAS.
- Программные средства анализа защищенности баз данных.
- Программные средства анализа защищенности WEB приложений.

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

- Методологии Penetration Testing.
- Понятие Footprinting. Этапы.
- Методы сканирования корпоративной сети.
- Методики и программные средства обнаружения активных узлов корпоративной сети.
- Методики и программные средства сканирования TCP/UDP портов узлов корпоративной сети.
- Методики и программные средства идентификации сетевых служб на узлах корпоративной сети.
- Методики и программные средства идентификации операционных систем на узлах корпоративной сети.
- Методики и программные средства построения сетевых диаграмм КИС.
- Инвентаризация ресурсов КИС. Подходы и методики.
- Инвентаризация ресурсов Linux узлов КИС.
- Инвентаризация ресурсов Windows узлов КИС.
- Применение специальных сетевых протоколов для инвентаризации ресурсов КИС.
- Анализ сетевого трафика. Методики и программные средства.
- Особенности анализа сетевого трафика в коммутируемой среде.
- Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.
- Атаки типа отказ в обслуживании на ресурсы КИС.
- Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.
- Атаки на беспроводные сети КИС.
- Программные средства проведения атак на беспроводные сети КИС.
- Сканеры уязвимостей и методики их применения.
- Особенности применения сканера OpenVAS.
- Программные средства анализа защищенности баз данных.
- Программные средства анализа защищенности WEB приложений.

Темы лабораторных работ:

- Обнаружение узлов корпоративной СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP)
- Обнаружение узлов корпоративной сети. Информационные ICMP сообщения
- Обнаружение узлов корпоративной сети средствами протокола TCP (TCP-PING)
- Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP-PING), IP
- Обнаружение узлов корпоративной сети средствами протокола ARP (ARP-PING)
- Основные средства определения маршрутов IP-пакетов - PING, TRACEROUTE
- Дополнительные средства определения маршрутов IP-ПАКЕТОВ - NMAP, TRACEMAP, MRT
- Идентификация статуса TCP-портов (TCP-CONNECT. SYN-SCAN)
- Методы скрытого сканирования (STEALTH TCP SCANNING METHODS)
- Методы сканирования UDP-портов (UDP PORT SCANNING). сканирование IP протокола
- Идентификация прикладных служб. метод анализа стандартных приглашений (BANNER GRABBING)
- Идентификация прикладных сетевых служб методом анализа особенностей реализации (SMTP)
- Идентификация службы электронной почты методом MAIL-BOUNCING
- Специализированные программные средства идентификации прикладных служб
- Активное исследование стека TCP/IP
- Специализированные программные средства активного исследования стека TCP/IP
- Пассивное исследование стека в задаче идентификации ОС
- Специальное ПО анализа уязвимостей OpenVas.
- Список вопросов для проработки в рамках СРС:

Темы и задания для самостоятельной работы студентов:

- Методология Penetration Testing. Open Source Security Testing Methodology Manual (OSSTMM).
- Методология Penetration Testing. Information Systems Security Assessment Framework (ISSAF).
- Методология Penetration Testing. Open Web Application Security Project (OWASP).
- Методология Penetration Testing. Web Application Security Consortium Threat Classification (WASC-TC).
- Стандарт Penetration Testing. Penetration Testing Execution Standard (PTES).
- Footprinting. Цели, задачи Footprinting.
- Footprinting. Этапы Footprinting и Reconnaissance.
- Footprinting. Открытые источники и пассивный сбор информации.
- Footprinting. Активный сбор информации.
- Footprinting. Программные инструменты Footprinting и Reconnaissance.
- Сканирование сети. Обнаружение узлов сети.
- Сканирование сети. Методы и программные средства сканирования сети.
- Сканирование сети. Обнаружение открытых портов узла сети.
- Сканирование сети. Методы и программные средства обнаружения открытых портов узла сети.
- Сканирование сети. Тип сканирования Full Open Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования Half-open Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования Xmas Tree Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования FIN Scan. Особенности использования

рассматриваемого типа сканирования.

- Сканирование сети. Тип сканирования NULL Scan. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования ACK Scanning. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования UDP Scanning. Особенности использования рассматриваемого типа сканирования.
- Сканирование сети. Тип сканирования ARP Scan. Особенности использования рассматриваемого типа сканирования.
- Services fingerprinting. Основные понятия.
- Services fingerprinting. Методы Services fingerprinting.
- Services fingerprinting. Программные инструменты Services fingerprinting.
- OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing.
- OS Fingerprinting. Методы OS Fingerprinting. Пассивное исследование стека в задаче идентификации ОС.
- OS Fingerprinting. Методы OS Fingerprinting. Активное исследование стека в задаче идентификации ОС.
- Построение карты сети. Программные средства Drawing Network Diagrams.
- Enumeration. Понятие, цели и задачи Enumeration.
- Enumeration. Инвентаризация ресурсов OS Windows. Методы и средства.
- Enumeration. Инвентаризация ресурсов OS Linux/Unix. Методы и средства.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация посредством SNMP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация LDAP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация SMTP.
- Sniffing. Цели и задачи анализа трафика. Программные инструменты анализа трафика.
- Sniffing атаки в коммутируемой сетевой среде. MAC Flooding.
- Sniffing атаки в коммутируемой сетевой среде. ARP Poisoning.
- Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing.
- Sniffing атаки в коммутируемой сетевой среде.
- Методы и средства защиты от Sniffing атак в коммутируемой сетевой среде.
- Атаки DOS. Цели и задачи атак DOS.
- Атаки DOS. Типы атак DOS.
- Атаки DOS. Service Request Floods.
- Атаки DOS. SYN Attack/Flood.
- Атаки DOS. ICMP Flood Attack.
- Атаки DOS. Программные средства проведения атак.
- Атаки DOS. Ping of Death.
- Атаки DOS. Teardrop.
- Атаки DOS. Smurf. Атаки DOS. Fraggle.
- Атаки DOS. Программные средства проведения атак.
- Атаки Buffer Overflow. Принципы.
- Атаки DDOS. Особенности реализации.
- Беспроводные сети. Угрозы и уязвимости Wireless Networks.
- Беспроводные сети. Аутентификация Wi-fi.
- Беспроводные сети. Атаки деаутентификации (Deauthentication Attack).
- Сканеры уязвимостей. Идентификация уязвимостей в сетях.
- OpenVAS. Методика сканирования.
- Сканеры уязвимостей. Уязвимости БД.
- Средства анализа защищенности БД.
- Сканеры уязвимостей. Уязвимости WEB приложений.
- Средства анализа защищенности WEB приложений.
- Программные инструменты специального дистрибутива KALI Linux для сбора

информации о КИС. Анализ DNS.

- Программные инструменты специального дистрибутива KALI Linux для сбора информации о КИС. Обнаружение активных узлов сети.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Идентификация сетевых служб и операционной системы узлов сети.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о распределенной АС. Анализ трафика.
- Программные инструменты специального дистрибутива KALI Linux для стресс тестирования КИС.
- Методики обнаружения межсетевых экранов в корпоративной сети.
- Программные средства обнаружения межсетевых экранов в корпоративной сети.
- Методики обнаружения IDS в корпоративной сети.
- Программные средства обнаружения IDS в корпоративной сети.
- Атаки на протоколы удаленного управления устройствами КИС.
- Распределенные атаки DDOS в корпоративной сетевой среде.
- Моделирование атак DDOS в корпоративной сетевой среде.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. 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

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. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. SBN 978-5-369-01379-3: Режим доступа: http://znanium.com/catalog.php?bookinfo=476047

б) Дополнительная литература:

1. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. ISBN 978-5-91134-627-0, Режим доступа: http://znanium.com/catalog.php?bookinfo=420047

2. Монахов Ю.М. Функциональная устойчивость информационных систем : учебное пособие : в 3 ч. / Ю. М. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир 2011 ISBN 973-5-9984-0189-1

3. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: учеб. пособие / В.Б. Попов. - М. : Финансы и статистика, 2008. - http://www.studentlibrary.ru/book/ISBN5279030074.html 176 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. 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.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

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 направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»
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: _____