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

Защита корпоративных информационных систем

Направление подготовки 10.04.01 Информационная безопасность

Программа подготовки

Уровень высшего образования магистратура

Форма обучения очная

Семестр	Трудоем-кость зач. ед./час.	Лек-ций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
3	3/108	18		36	18	Зачет
Итого	3/108	18		36	18	Зачет

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защита корпоративных информационных систем» 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 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 МАГИСТРАТУРЫ

Данная дисциплина относится к дисциплинам по выбору вариативной части Блока Б1 (код Б1.В.ДВ.3). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

Дисциплина изучается на 2 курсе, в 3 семестре требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.04.01 «Информационная безопасность» по курсам «Технологии обеспечения информационной безопасности», «Организационно-правовые механизмы обеспечения информационной безопасности», «Информационно-аналитические системы безопасности».

Курс тесно взаимосвязан с другими дисциплинами. Он может быть полезен для изучения таких дисциплин как «Управление информационной безопасностью», «Защищённые информационные системы» 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-1 – способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-2 – способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-3 – способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

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; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем (ПК-1; ПК-2; 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; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности (ПК-1; ПК-2; 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 управления информационной безопасностью простых объектов (ПК-1; ПК-2; 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 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.	Сетевая разведка. Первичный сбор информации о КИС.	3	1-2	2		4		2		2/33%	
2.	Методики и программные средства обнаружения активных узлов корпоративной сети.	3	3-4	2		4		2		2/33%	
3.	Методики сканирования сетей.	3	5-6	2		4		2		2/33%	Рейтинг-контроль №1
4.	Инвентаризация ресурсов КИС. Подходы и методики.	3	7-8	2		4		2		2/33%	
5.	Анализ сетевого трафика. Методики и программные средства.	3	9-10	2		4		2		2/33%	
6.	Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде.	3	11-12	2		4		2		2/33%	Рейтинг-контроль №2
7.	Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.	3	13-14	2		4		2		2/33%	
8.	Атаки на беспроводные сети КИС. Безопасность беспроводной сети КИС.	3	15-16	2		4		2		2/33%	
9.	Методологии тестирования на проникновение.	3	17-18	2		4		2		2/33%	Рейтинг-контроль №3
Всего				18		36		18		18/33%	Зачет

Содержание дисциплины «Защита корпоративных информационных систем»

Раздел 1. Сетевая разведка. Первичный сбор информации о КИС. Методологии Penetration Testing. Понятие Footprinting. Этапы. Методы сканирования корпоративной сети.

Раздел 2. 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.

Раздел 3. Методики сканирования сетей. Методики и программные средства идентификации операционных систем на узлах корпоративной сети. Методики и программные средства построения сетевых диаграмм КИС.

Раздел 4. Инвентаризация ресурсов КИС. Подходы и методики. Инвентаризация ресурсов Linux узлов КИС. Инвентаризация ресурсов Windows узлов КИС. Применение специальных сетевых протоколов для инвентаризации ресурсов КИС.

Раздел 5. Анализ сетевого трафика. Методики и программные средства. Особенности анализа сетевого трафика в коммутируемой среде.

Раздел 6. Атаки на КИС на основе анализа сетевого трафика в коммутируемой среде. Атаки типа отказ в обслуживании на ресурсы КИС.

Раздел 7. Программные средства проведения атак типа отказ в обслуживании на ресурсы КИС.

Раздел 8. Атаки на беспроводные сети КИС. Безопасность беспроводной сети КИС. Программные средства проведения атак на беспроводные сети КИС. Сканеры уязвимостей и методики их применения.

Рздел 9. Особенности применения сканера OpenVAS. Программные средства анализа защищенности баз данных. Программные средства анализа защищенности WEB приложений.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Защита корпоративных информационных систем» 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

- 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 зачету (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:

Лабораторная работа № 1. Обнаружение узлов корпоративной СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP)

Лабораторная работа № 2. Обнаружение узлов корпоративной сети. Информационные ICMP сообщения

Лабораторная работа № 3. Обнаружение узлов корпоративной сети средствами протокола TCP (TCP-PING)

Лабораторная работа № 4. Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP-PING), IP

Лабораторная работа № 5. Обнаружение узлов корпоративной сети средствами протокола ARP (ARP-PING)

Лабораторная работа № 6. Основные средства определения маршрутов IP-пакетов - PING, TRACEROUTE

Лабораторная работа № 7. Дополнительные средства определения маршрутов IP-ПАКЕТОВ - NMAP, TRACEMAP, MRT

Лабораторная работа № 8. Идентификация статуса TCP-портов (TCP-CONNECT. SYN-SCAN)

Лабораторная работа № 9. Методы скрытого сканирования (STEALTH TCP SCANNING METHODS)

Лабораторная работа № 10. Идентификация прикладных сетевых служб методом анализа особенностей реализации (SMTP)

Вопросы и задания к самостоятельной работе магистрантов

- 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. 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. Методы и программные средства.
- Сканирование сети. Обнаружение открытых портов узла сети. Методы и программные средства.
- Сканирование сети. Типы сканирования (Full Open Scan, Half-open Scan, Xmas Tree Scan). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (FIN Scan, NULL Scan, ACK Scanning). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (UDP Scanning, ARP Scan). Особенности использования рассматриваемых типов сканирования.
- 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. Инвентаризация ресурсов OS Windows. Методы и средства.
- Enumeration. Понятие, цели и задачи 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. ARP Poisoning.
- Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing.
- Sniffing атаки в коммутируемой сетевой среде. Методы и средства защиты от Sniffing атак.
- Атаки DOS. Цели и задачи атак DOS. Типы атак DOS.
- Атаки DOS. Service Request Floods. SYN Attack/Flood. ICMP Flood Attack. Программные средства проведения атак.
- Атаки DOS. Ping of Death. Teardrop. Smurf. Fraggle. 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.
- Сканеры уязвимостей. Уязвимости БД.
- Средства анализа защищенности БД.
- Сканеры уязвимостей. Уязвимости WEB приложений.
- Средства анализа защищенности WEB приложений.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Корпоративные информационные системы управления: Учебник / Под науч. ред. Н.М. Абдикеева, О.В. Китовой. - М.: НИЦ ИНФРА-М, 2014. - 464 с.: ISBN 978-5-16-003860-5, Режим доступа: http://znanium.com/

2. 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

3. 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

4. Архитектура корпоративных информационных систем/АстапчукВ.А., ТерещенкоП.В. - Новосиб.: НГТУ, 2015. - 75 с. ISBN 978-5-7782-2698-2 Режим доступа: http://znanium.com/catalog.php?bookinfo=546624

5. 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. 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.- ISBN 978-5-94275-667-3.

2. Информационная система предприятия: Учебное пособие/Вдовенко Л. А. - 2 изд., перераб. и доп. - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 304 с. ISBN 978-5-9558-0329-6, Режим доступа: http://znanium.com/catalog.php?bookinfo=501089

3. Проектирование информационных систем: Учебное пособие / Н.Н. Заботина. - М.: НИЦ Инфра-М, 2013. - 331 с.: ISBN 978-5-16-004509-2 Режим доступа: http://znanium.com/catalog.php?bookinfo=371912

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. Мишин Д.В.

(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 2017/18 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: _____