УП 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 учебно-методической работе
_____ А.А.Панфилов
«29» 12 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Распределенные автоматизированные информационные системы

Специальность 10.05.04 "Информационно-аналитические системы безопасности"

Специализация "Автоматизация информационно-аналитической деятельности"

Уровень высшего образования специалитет

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)
8	6/216	36	18	36	90	Экзамен(36ч)
Итого	6/216	36	18	36	90	Экзамен(36ч)

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Распределенные автоматизированные информационные системы» являются обеспечение профессиональной подготовки студентов в соответствии с требованиями ФГОС ВО и учебного плана по специальности 10.05.04; формирование у студентов по специальности 10.05.04 «Информационно-аналитические системы безопасности» обобщенного теоретического и практического представления о современном теоретическом аппарате разработки и функционирования распределенных автоматизированных информационных систем; знакомство студентов с современными подходами к разработке распределенных систем и баз данных, предназначенных для функционирования в локальных и глобальных сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.24). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ, ориентированных на освоение студентами современных методологий проектирования и разработки распределенных автоматизированных информационных систем, а также способов развертывания и сопровождения. Курс тесно взаимосвязан с другими дисциплинами данного цикла «Моделирование автоматизированных информационных систем», «Методология и организация информационно-аналитической деятельности», «Лингвистическое обеспечение автоматизированных информационных систем».

Дисциплина изучается на четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам Технологии и методы программирования», «Языки программирования», «Основы информационной безопасности», «Базы данных и экспертные системы», «Информатика» по специальности 10.05.04 «Информационно-аналитические системы безопасности», квалификации - специалист.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями:

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

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

ПСК-1.3. – способностью решать задачи анализа данных больших объемов.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) Знать: основные понятия теории распределенных систем в объеме, необходимом для использования существующих распределенных автоматизированных информационных систем (РАИС), основные модели доступа к распределенной информации, основные проблемы и способы их преодоления, типовые архитектуры РАИС, методы функционирования и проектирования РАИС (ПК-10; ПСК-1.1; ПСК-1.3);

2) Уметь: ставить и решать типовые задачи в области проектирования и разработки РАИС; использовать инструментальные средства, направленные на автоматизацию этапов проектирования и управления разработкой РАИС; эффективно пользоваться существующими РАИС (ПК-10; ПСК-1.1; ПСК-1.3);

3) Владеть: навыками работы с инструментальными средствами автоматизации этапов проектирования и управления разработкой РАИС; набором технологий для разворачивания и сопровождения РАИС (ПК-10; ПСК-1.1; ПСК-1.3).

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

- способность выбора оптимального системного программного обеспечения для решения прикладных задач в области обеспечения информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 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 РАИС	8	1,2	4	2	4		10		4/50%	
2.	Методики сканирования сетей РАИС	8	3,4	4	2	4		10		2/25%	
3.	Инвентаризация ресурсов РАИС	8	5,6	4	2	4		10		2/25%	Рейтинг-контроль №1
4.	Атаки типа отказ в обслуживании на ресурсы РАИС	8	7,8	4	2	4		10		4/50%	
5.	Анализ сетевого трафика. Методики и программные средства. Особенности анализа сетевого трафика в коммутируемой среде РАИС.	8	9,10	4	2	4		10		2/25%	
6.	Атаки типа отказ в обслуживании на ресурсы РАИС.	8	11, 12	4	2	4		10		2/25%	Рейтинг-контроль №2
7.	Методики анализа защищенности беспроводной сети РАИС	8	13, 14	4	2	4		10		2/25%	
8.	Методики анализа защищенности WEB приложений и БД РАИС.	8	15, 16	4	2	4		10		4/50%	
9.	Стандарты тестирования на проникновение	8	17, 18	4	2	4		10		2/25%	Рейтинг-контроль №3
Всего		8		36	18	36		90		24/33%	ЭКЗАМЕН

Содержание дисциплины «Распределенные автоматизированные информационные системы»:

Раздел 1. Сетевая разведка. Первичный сбор информации о РАИС

Раздел 2. Методики сканирования сетей РАИС

Раздел 3. Инвентаризация ресурсов РАИС.

Раздел 4. Атаки типа отказ в обслуживании на ресурсы РАИС

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

Раздел 6. Атаки типа отказ в обслуживании на ресурсы РАИС

Раздел 7. Методики анализа защищенности беспроводной сети РАИС.

Раздел 8. Методики анализа защищенности WEB приложений и БД РАИС.

Раздел 9. Стандарты тестирования на проникновение.

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

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

Вопросы рейтинг-контроля №3

- Атаки типа отказ в обслуживании на ресурсы РАИС.
- Программные средства проведения атак типа отказ в обслуживании на ресурсы РАИС.
- Атаки на беспроводные сети РАИС.
- Программные средства проведения атак на беспроводные сети РАИС.
- 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 РАИС.
- Инвентаризация ресурсов РАИС. Подходы и методики.
- Инвентаризация ресурсов Linux узлов РАИС.
- Инвентаризация ресурсов Windows узлов РАИС.
- Применение специальных сетевых протоколов для инвентаризации ресурсов РАИС.
- Анализ сетевого трафика. Методики и программные средства.
- Особенности анализа сетевого трафика в коммутируемой среде.
- Атаки на РАИС на основе анализа сетевого трафика в коммутируемой среде.
- Атаки типа отказ в обслуживании на ресурсы РАИС.
- Программные средства проведения атак типа отказ в обслуживании на ресурсы РАИС.
- Атаки на беспроводные сети РАИС.
- Программные средства проведения атак на беспроводные сети РАИС.
- Сканеры уязвимостей и методики их применения.
- Особенности применения сканера OpenVAS.
- Программные средства анализа защищенности баз данных.
- Программные средства анализа защищенности WEB приложений.

Перечень лабораторных работ:

1. Обнаружение узлов корпоративной СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP). Обнаружение узлов корпоративной сети. Информационные ICMP сообщения
2. Обнаружение узлов корпоративной сети средствами протокола TCP (TCP-PING). Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP-PING). IP
3. Обнаружение узлов корпоративной сети средствами протокола ARP (ARP-PING)
4. Основные средства определения маршрутов IP-пакетов - PING, TRACEROUTE. Дополнительные средства определения маршрутов IP-ПАКЕТОВ - NMAP, TRACEMAP, MRT
5. 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
6. 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
7. 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
8. Специальное ПО анализа уязвимостей OpenVas.

Перечень тем практических занятий:

Тема 1. Атаки типа отказ в обслуживании на ресурсы РАИС
Тема 2. Анализ сетевого трафика. Методики и программные средства. Особенности анализа сетевого трафика в коммутируемой среде РАИС
Тема 3. Атаки типа отказ в обслуживании на ресурсы РАИС
Тема 4. Методики анализа защищенности беспроводной сети РАИС.
Тема 5. Методики анализа защищенности WEB приложений и БД РАИС.
Тема 6. Стандарты тестирования на проникновение.

Вопросы 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 РАИС. Анализ DNS.
- Программные инструменты специального дистрибутива KALI Linux для сбора информации о РАИС. 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 РАИС.
- 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 РАИС.
- 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. 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. Мишин Д.В. Анализ защищенности распределенных информационных систем. Идентификация ресурсов корпоративной сети передачи данных : практикум для вузов по направлению "Информационная безопасность" / Д. В. Мишин, Ю. М. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир :, 2012 .— 94 с. : ISBN 978-5-9984-0295-1.
3. 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
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. 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. 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.
3. 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
4. Проектирование информационных систем: Учебное пособие / Н.Н. Заботина. - М.: НИЦ Инфра-М, 2013. - 331 с.: Режим доступа: http://znanium.com/catalog.php?bookinfo=371912

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: к.т.н., доцент каф. ИЗИ Мишин Д.В.

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»

к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 7 от 28.12.2016 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

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 28.12.2016 года
Председатель комиссии д.т.н., профессор /М.Ю. Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017/2018 учебный год
Протокол заседания кафедры № 1 от 23.03.2017 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)

Специальность

Специализация

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: _____