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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

(наименование дисциплины)

Специальность 10.05.04 "Информационно-аналитические системы безопасности"

Специализация "Автоматизация информационно-аналитической деятельности"

Уровень высшего образования специалитет

Форма обучения очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
7	2/72	18		36	18	Зачет
Итого	2/72	18		36	18	Зачет

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Управление информационной безопасностью в корпоративных информационных системах» являются обеспечение профессиональной подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана специальности 10.05.04 «Информационно-аналитические системы безопасности». Целью освоения дисциплины является формирование теоретических знаний и практических навыков по управлению информационной безопасностью в корпоративных информационных системах. Задачами дисциплины являются Управление информационной безопасностью в корпоративных информационных системах»: освоение принципов реализации и основных подходов к оптимальному управлению различными механизмами информационной безопасности в системах. В процессе освоения дисциплины изучаются следующие вопросы: - основные руководящие документы и показатели эффективности системы защиты информации в КИС; -комплексный подход к обеспечению ИБ в КИС; -цели, стратегии и политика информационной безопасности; -организационные аспекты информационной безопасности в КИС; - функции управления информационной безопасностью в КИС; - процессный подход для управления информационной безопасностью в КИС; - система ответственности в области информационной безопасности; -организация и методика проведения аудита системы управления информационной безопасностью в КИС; -алгоритм проведения анализа информационных рисков в КИС предприятия; -аналитические технологии управления ИБ в КИС; -обеспечение управления ИБ в КИС в чрезвычайных ситуациях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

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. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

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», «Безопасность информационных и аналитических систем» «Принципы построения, проектирования и эксплуатации автоматизированных информационных систем», «Техническая защита информации» по специальности 10.05.04 «Информационно-аналитические системы безопасности», квалификации - специалист.

Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Система защиты информации на предприятии», «Моделирование автоматизированных информационных систем», «Распределенные автоматизированные информационные системы».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями:

ПК-13 – способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;

ПК -17 – способностью организовывать работу малых коллективов исполнителей, принимать и реализовывать управленческие решения в сфере профессиональной деятельности.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) Знать: - основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной 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-13; ПК-17);

2) Уметь: - строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных 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-13; ПК-17);

3) Владеть: - методами и средствами выявления угроз безопасности автоматизированным 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-13; ПК-17).

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 2 зачетных единицы, 72 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	Введение. Основные руководящие документы и показатели эффективности системы ЗИ	7	1-2	2		4		2		3 (50%)	-
2	Комплексный подход к обеспечению ИБ объекта	7	3-4	2		4		2		2 (33%)	
3	Цели, стратегии и политика информационной безопасности. Организационные аспекты информационной безопасности	7	5-6	2		4		2		3 (50%)	Рейтинг-контроль №1
4	Функции управления информационной безопасностью	7	7-8	2		4		2		2 (33%)	
5	Процессный подход для управления информационной безопасностью	7	9-10	2		4		2		3 (50%)	
6	Система ответственности в области информационной безопасности	7	11-12	2		4		2		2 (33%)	Рейтинг-контроль №2
7	Аудит системы управления информационной безопасностью	7	13-14	2		4		2		3 (50%)	
8	Алгоритм проведения анализа информационного риска на предприятии	7	15-16	2		4		2		2 (33%)	
9	Аналитические технологии управления ИБ. Обеспечение ИБ в чрезвычайных ситуациях	7	17-18	2		4		2		2 (33%)	Рейтинг-контроль №3
Всего		7		18		36		18		22 (40%)	ЗАЧЕТ

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

- Дать определение СЗИ.
- Что такое информационная безопасность?
- Цели информационной безопасности.
- Основные требования к комплексной системе защиты информации
- Задачи системы компьютерной безопасности
- Основные принципы организации СЗИ
- В чём заключается принцип системности?
- В чём заключается принцип комплексности?

- В чём заключается принцип непрерывности защиты?
- В чём заключается принцип разумной достаточности?
- В чём заключается гибкость системы защиты?
- Принцип простоты применения средств защиты
- Этап работ по созданию СЗИ.

Вопросы рейтинг-контроля №2

- Что включает в себя обследование организации?
- Факторы, влияющие на организацию СЗИ.
- Определение состава защищаемой информации
- Нормативное закрепление состава защищаемой информации
- Виды информации.
- Необходимые свойства защищаемой информации
- Категорирование защищаемой информации.
- Определение объектов защиты.
- Что называется объектом защиты.
- Основные объекты защиты.
- Основные виды угроз информационной безопасности:
- Классификация угроз безопасности
- Неформальная модель нарушителя в АС .
- Что определяются при разработке модели нарушителя.

Вопросы рейтинг-контроля №3

- Причины совершения компьютерных преступлений
- Потенциальные каналы несанкционированного доступа к защищаемой информации
- Потенциальные методы несанкционированного доступа к защищаемой информации.
- Классификация каналов проникновения в систему и утечки информации
- Физические каналы.
- Электромагнитные каналы.
- Информационные каналы
- Общая модель комплексной системы защиты информации.
- Средства защиты, используемые для создания системы защиты.
- Типы моделей управления доступом.
- Организационное направление работ по созданию СЗИ.
- Технология построения СЗИ
- Кадровое обеспечение функционирования СЗИ.
- Организационная структура, основные функции службы компьютерной безопасности.
- Концепция (политика) безопасности.

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

1. Дать определение СЗИ.
2. Что такое информационная безопасность?
3. Цели информационной безопасности.
4. Основные требования к комплексной системе защиты информации
5. Задачи системы компьютерной безопасности
6. Основные принципы организации СЗИ
7. В чём заключается принцип системности?
8. В чём заключается принцип комплексности?
9. В чём заключается принцип непрерывности защиты?
10. В чём заключается принцип разумной достаточности?
11. В чём заключается гибкость системы защиты?

12. Принцип простоты применения средств защиты
13. Этап работ по созданию СЗИ.
14. Что включает в себя обследование организации?
15. Факторы, влияющие на организацию СЗИ.
16. Определение состава защищаемой информации
17. Нормативное закрепление состава защищаемой информации
18. Виды информации.
19. Необходимые свойства защищаемой информации
20. Категорирование защищаемой информации.
21. Определение объектов защиты.
22. Что называется объектом защиты.
23. Основные объекты защиты.
24. Основные виды угроз информационной безопасности:
25. Классификация угроз безопасности
26. Неформальная модель нарушителя в АС .
27. Что определяются при разработке модели нарушителя.
28. Причины совершения компьютерных преступлений
29. Потенциальные каналы несанкционированного доступа к защищаемой информации
30. Потенциальные методы несанкционированного доступа к защищаемой информации.
31. Классификация каналов проникновения в систему и утечки информации
32. Физические каналы.
33. Электромагнитные каналы.
34. Информационные каналы
35. Общая модель комплексной системы защиты информации.
36. Средства защиты, используемые для создания системы защиты.
37. Типы моделей управления доступом.
38. Организационное направление работ по созданию СЗИ.
39. Технология построения СЗИ
40. Кадровое обеспечение функционирования СЗИ.
41. Организационная структура, основные функции службы компьютерной безопасности.
42. Концепция (политика) безопасности.

Темы лабораторных работ:

- Построение описания объекта информатизации. Общее описание объекта и его планировка. Построение описания объекта информатизации. Организационная структура предприятия и экспликация помещений отделов.
- Построение описания объекта информатизации. Перечень и характеристики информационных ресурсов. Построение описания объекта информатизации. Список и характеристики персонала.
- Проектирование корпоративной сети передачи данных. Список и характеристики средств хранения, обработки, передачи и представления информации. Список и характеристики средств защиты информации.
- Проектирование корпоративной сети передачи данных. Топология КСПД и схема адресации.
- Разработка слоев «информационные ресурсы», «КСПД», «персонал», «уязвимости», «угрозы» на плане объекта. Разработка слоев СЗИ на плане объекта.
- Выполнение анализа угроз ИБ и защищённости ИС. Перечень угроз ИБ. Перечень уязвимостей ИС с обоснованием.
- Выполнение анализа угроз ИБ и защищённости ИС. Перечень и характеристики существующих защитных механизмов. Произвести оценку текущего уровня защищённости от угроз ИБ.
- Ранжирование списка угроз по вероятностям реализации от максимальной к минимальной. Выделить на слое «угрозы» в цветовой гамме от красного к зелёному согласно списку.

• Построение и оценка СЗИ па предприятии. Выбор механизмов обеспечения информационной безопасности в рамках организационно-технического, инженерно-технического и программно-аппаратного направлений.

Вопросы и задания для самостоятельной работы студентов:

- Прокомментируйте основные направления обеспечения ИБ
- Что понимается под безопасностью информации? Что такое ЗИ?
- Дайте определение понятиям «конфиденциальность», «целостность», «доступность».
- Перечислите основные задачи системы информационной безопасности.
- В чем заключается основная цель защиты информации?
- Определите организационные проблемы информационной безопасности.
- Сформулируйте технические проблемы информационной безопасности.
- Раскройте общее содержание методологии проектирования системы ЗИ. Как понимается процесс создания оптимальной системы? Сформулируйте возможные постановки задачи оптимизации СЗИ.
- Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
- Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
- Дайте определение системы ЗИ и сформулируйте основные концептуальные требования, предъявляемые к ней.
- Приведите принятую методику построения системы ИБ предприятия
- Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность?
- Сформулируйте основные концептуальные положения теории ЗИ.
- По каким аспектам экспертная комиссия предприятия рассматривает предварительный перечень конфиденциальных сведений?
- Приведите типовой примерный перечень сведений, составляющих служебную или коммерческую тайну организации.
- Перечислите степень секретности (гриф), который могут иметь сведения, составляющие служебную или коммерческую тайну предприятия
- Что принято понимать под служебной или коммерческой тайной?
- Каковы критерии отнесения организаций и частных лиц к потенциальным злоумышленникам (которые могут быть заинтересованы в доступе к охраняемой информации)?
- Каким образом принимается и как оформляется решения о включении сведений в окончательный вариант Перечня?
- Назовите основную цель планирования в обеспечении ИБ предприятия. Охарактеризуйте стратегическое (или перспективное) и тактическое (или текущее) планирование.
- Из каких этапов состоит работа по формированию Перечня сведений, составляющих служебную или коммерческую тайну?
- Определите составляющие информационно-логической модели объекта защиты.
- Что понимают под Политикой информационной безопасности?
- Что должна включать в себя в обобщенном виде Концепция обеспечения ИБ?
- Перечислите основные элементы Концепции обеспечения ИБ на предприятии. Зачем необходим раздел с основными понятиями концепции?
- Прокомментируйте разделы Концепции, касающиеся определения состава потенциально существующих угроз безопасности информации, описания каналов вторжения в ИС, требований к системе обеспечения ИБ и методов оценки ее эффективности.
- Что понимают под концепцией ИБ?

- Назовите причины необходимости разработки Концепции обеспечения ИБ на каждом предприятии.
- Определите основную цель и комплекс мероприятий управления ИБ предприятия. Приведите обобщенную схему процесса управления ИБ предприятия
- Охарактеризуйте основные направления деятельности администратора безопасности
- Охарактеризуйте этапы логической последовательности принятия решения в процессе управления ИБ
- Приведите структуру АРМа администратора безопасности
- Основные подразделения службы ИБ, их организационно-правовой статус.
- Приведите основные особенности и принципы построения системы управления ИБ. Охарактеризуйте основные подсистемы СУИБ.
- Приведите и прокомментируйте пакет планирующих документов по обеспечению ИБ
- С какой целью разрабатывается план мероприятий по противодействию ЧС?
- Какие мероприятия по работе с персоналом необходимо проводить для наиболее эффективного противодействия ЧС? Приведите основные методы реагирования на ЧС
- Какие ситуации называют чрезвычайными? Приведите классификацию ЧС. Охарактеризуйте наиболее распространенные угрозы в условиях чрезвычайных ситуаций
- Охарактеризуйте постоянно проводимые мероприятия защиты и мероприятия, проводимые по необходимости
- Охарактеризуйте разовые и периодически проводимые мероприятия защиты
- Охарактеризуйте источники получения информации для администратора безопасности

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. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=463061
3. 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.
4. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.

б) Дополнительная литература:

1. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков: учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т. 2010. - 144 с. Режим доступа: http://znanium.com/catalog.php?bookinfo=463037
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 сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;
2. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

г) Программное обеспечение и Интернет-ресурсы:

1. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
2. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.04 "Информационно-аналитические системы безопасности", специализация «автоматизация информационно-аналитической деятельности»

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Мишин Д.В.
(ФИО, подпись)

Рецензент
(представитель работодателя) к.т.н. Абрамов Константин Германович ведущий специалист управления поддержки инфраструктуры ООО «ОМК - Информационные технологии»,
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 7 от 28.12.2016 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии по специальности 10.05.04 "Информационно-аналитические системы безопасности", специализация «автоматизация информационно-аналитической деятельности»

Протокол № 4 от 28.12.2016 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 28.08.2017 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)

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: _____