2015

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

Защищенные информационные системы

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	Экзамен (36ч), КР
Итого	3/108	18		36	18	Экзамен (36ч), КР

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защищенные информационные системы» 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 современным теоретическим аппаратом информационной безопасности, представление сведений о базовых моделях и алгоритмах, используемых в управлении информационной безопасностью в информационных системах, а также о процессе теоретико-методологического анализа различных механизмов и сервисов защиты информации. Задачей изучения дисциплины «Защищенные информационные системы» является изучение аппарата управления информационной безопасностью в информационных системах, освоение методов анализа программно-технических сервисов информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО МАГИСТРАТУРЫ

Данная дисциплина относится к базовой части блока Б1 (код Б1.Б.1). 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 «Анализ и моделирование информационно-телекоммуникационных сетей», «Методы и средства защиты объектов информатизации», «Методология информационной безопасности». Кроме того, требования к «входным» знаниям, умениям и готовностям обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Защита информации в корпоративных информационных системах» или аналогичных, в соответствии с программой подготовки бакалавров в следующих или смежных областях знаний: -информационная безопасность; -энергетика, энергетическое машиностроение и электротехника; -авиационная и ракетно-космическая техника; -фотоника, приборостроение, -оптические и биотехнические системы и технологии; -электронная техника, радиотехника и связь; -автоматика и управление; -информатика и вычислительная техника; -физико-технические науки и технологии; -управление в технических системах.

Курс тесно взаимосвязан с другими дисциплинами. Он может быть полезен для изучения таких дисциплин как «Управление информационной безопасностью», «Информационно-аналитические системы безопасности» 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-2 – способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-7 – способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** - основные понятия теории защиты информации в объеме, необходимом для использования и анализа сервисов информационной безопасности, основные модели доступа к информации; - основные виды информационных атак и дестабилизирующих информационных воздействий; - типовые состав ЗИС, их методы функционирования и

проектирования; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; - методы концептуального проектирования технологий обеспечения информационной безопасности (ПК-2; ПК-7; ПК-9);

2) ***Уметь:*** - ставить и решать типовые задачи в области анализа безопасности информационных потоков в распределенной информационной системе; - подбирать и использовать адекватные методы и средства защиты информации; - оценивать эффективность методов защиты информационных процессов; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;- организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности (ПК-2; ПК-7; ПК-9);

3) ***Владеть:*** - навыками применения теоретического аппарата защиты информации к текущим реальным ситуациям; - навыками обнаружения уязвимостей в распределенных информационных системах и программных комплексах; - навыками управления информационной безопасностью простых объектов (ПК-2; ПК-7; ПК-9).

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

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

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 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.	Аудит инфраструктуры ЗИС/КАС	3	1-2	2		4		2		2/33%	
2.	Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.	3	3-4	2		4		2		2/33%	
3.	Порядок внедрения SLM-системы.	3	5-6	2		4		2		4/66%	Рейтинг-контроль №1
4.	Эталонная модель Hewlett-Packard управления ИТ-услугами	3	7-8	2		4		2		2/33%	
5.	Организация технического обслуживания ИТ.	3	9-10	2		4		2		4/66%	
6.	Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС	3	11-12	2		4		2		2/33%	Рейтинг-контроль №2
7.	Методы и методики проектирования ЗИС	3	13-14	2		4		2		2/33%	
8.	Методы и методики оценки качества ЗИС	3	15-16	2		4		2		2/33%	
9.	Порядок приемки защищенных ЗИС, в том числе программных и технических (криптограф.) средств и систем защиты от НСД.	3	17-18	2		4		2		2/33%	Рейтинг-контроль №3
Всего				18		36		18	КР	22/41%	Экзамен

Содержание дисциплины

Раздел 1. Аудит инфраструктуры ЗИС/КАС (корпоративной автоматизированной системы). Пример методики аудита. Методика аудита компании Cisco Systems

Раздел 2. Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами. Современная структура ITIL. Преимущества внедрения ITSM. Бизнес-ориентированное управление ИТ на современном предприятии.

Раздел 3. Порядок внедрения SLM-системы. Service Desk — цели, возможности, реализации. Microsoft Operations Framework (MOF).

Раздел 4. Эталонная модель Hewlett-Packard управления ИТ-услугами. Содержание модели ITSM HP

Раздел 5. Организация технического обслуживания ИТ. Значение технического обслуживания. Гарантия. Программы технического обслуживания. Схемы технического обслуживания. Аутсорсинг.

Раздел 6. Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС, техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие, аттестация ЗИС по требованиям безопасности, сопровождение ЗИС.

Раздел 7. Методы и методики проектирования ЗИС: методика выявления возможных каналов НСД, последовательность работ при проектировании комплексной системы защиты информации, моделирование как инструментарий проектирования, методика построения административного управления ЗИС.

Раздел 8. Методы и методики оценки качества ЗИС. Требования к эксплуатационной документации ЗИС.

Раздел 9. Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД. Особенности эксплуатации ЗИС на объекте защиты.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Защищенные информационные системы» 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

- Бизнес-ориентированное управление ИТ на современном предприятии.
- Виды программ технического обслуживания (стандартные программы).
- Значение технического обслуживания.
- Как обслуживаются высококритичные системы.
- Концепция управления ИТ-подразделением — IT Service Management.
- Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC

- Гарантии безопасности компьютерных систем в системе общих критериев
- Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев
- Основные угрозы безопасности информации в компьютерных системах
- Государственная политика в области безопасности компьютерных систем
- Порядок сертификации средств защиты информации для разработчика СЗИ.
- Порядок сертификации защищенных информационных систем

Вопросы рейтинг-контроля №2

- Государственная политика в области безопасности компьютерных систем
- Порядок сертификации средств защиты информации для разработчика СЗИ.
- Порядок сертификации защищенных информационных систем
- Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем
- Разработка политик безопасности для защищенных компьютерных систем
- Порядок аттестации защищенных компьютерных систем
- Критерии эффективности работы ИС.
- Оперативные мероприятия.
- Организация технического обслуживания ИТ.
- Плановые мероприятия.
- Понятие гарантии.
- Порядок внедрения SLM-системы.
- Порядок осуществления гарантии.

Вопросы рейтинг-контроля №3

- Понятие гарантии.
- Порядок внедрения SLM-системы.
- Порядок осуществления гарантии.
- Преимущества внедрения ITSM.
- Причины отказа в гарантийном обслуживании.
- Программы технического обслуживания.
- Разовые мероприятия.
- Расширенные программы технического обслуживания.
- Регламентные мероприятия.
- Содержание модели ITSM HP. Процессы взаимодействия и ИТ-служб.
- Содержание модели ITSM HP. Процессы проектирования и управления услугами.
- Содержание модели ITSM HP. Процессы разработки услуг.
- Содержание модели ITSM HP. Процессы эксплуатации.
- Схемы технического обслуживания.
- Эталонная модель Hewlett-Packard управления ИТ-услугами.

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

1. Бизнес-ориентированное управление ИТ на современном предприятии.
2. Виды программ технического обслуживания (стандартные программы).
3. Значение технического обслуживания.
4. Как обслуживаются высококритичные системы.
5. Концепция управления ИТ-подразделением — IT Service Management.
6. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC
7. Гарантии безопасности компьютерных систем в системе общих критериев

8. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев
9. Основные угрозы безопасности информации в компьютерных системах
10. Государственная политика в области безопасности компьютерных систем
11. Порядок сертификации средств защиты информации для разработчика СЗИ.
12. Порядок сертификации защищенных информационных систем
13. Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем
14. Разработка политик безопасности для защищенных компьютерных систем
15. Порядок аттестации защищенных компьютерных систем
16. Критерии эффективности работы ИС.
17. Оперативные мероприятия.
18. Организация технического обслуживания ИТ.
19. Плановые мероприятия.
20. Понятие гарантии.
21. Порядок внедрения SLM-системы.
22. Порядок осуществления гарантии.
23. Преимущества внедрения ITSM.
24. Причины отказа в гарантийном обслуживании.
25. Программы технического обслуживания.
26. Разовые мероприятия.
27. Расширенные программы технического обслуживания.
28. Регламентные мероприятия.
29. Содержание модели ITSM HP. Процессы взаимодействия и ИТ-служб.
30. Содержание модели ITSM HP. Процессы проектирования и управления услугами.
31. Содержание модели ITSM HP. Процессы разработки услуг.
32. Содержание модели ITSM HP. Процессы эксплуатации.
33. Схемы технического обслуживания.
34. Эталонная модель Hewlett-Packard управления ИТ-услугами.

Темы лабораторных работ:

Лабораторная работа № 1. Сравнительный анализ различных стандартов в области защиты информационных технологий с точки зрения эффективности достижения цели построения защищенных информационных систем.

Лабораторная работа № 2. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев

Лабораторная работа № 3. Анализ рисков для информационной системы предприятия (организации) и построение модели угроз безопасности

Лабораторная работа № 4. Порядок сертификации средств защиты информации для разработчика СЗИ.

Лабораторная работа № 5. Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем для руководителя предприятия (организации) – соискателя лицензии

Лабораторная работа № 6. Разработка профиля защиты и построение политик безопасности для компьютерной системы предприятия (организации)

Лабораторная работа № 7. Проведение аттестационных испытаний компьютерных систем в защищенном исполнении и выдача «Аттестата соответствия»

Вопросы и задания к самостоятельной работе магистрантов

- ITIL – Компонент «Поддержка услуг».
- ITIL – Компонент «Предоставление услуг».
- ITIL — основа концепции управления ИТ-службами.
- Service Desk — цели, возможности, реализации.

- Аудит инфраструктуры РИС/КАС.
- Аутсорсинг.

Примерные темы заданий к курсовой работе

1. Разработка защищенного АРМ администратора безопасности.
2. Организация антивирусной защиты ЛВС.
3. Построение комплексной системы защиты информации IP-сети.
4. Анализ особенностей защиты информации в мультисервисных сетях.
5. Исследование методов построения защищенных Интернет приложений.
6. Разработка системы управления учетными записями пользователей для различных предметных областей.
7. Анализ и разработка методов построения отказоустойчивого файлового сервера организации различного профиля.
8. Разработка проекта ИТ-приложения на современном предприятии (по выбору) с проработкой механизмов защиты.
9. Разработка защищенной АС структурного подразделения на современном предприятии (по выбору).
10. Разработка проекта защищенной распределенной АС подразделения на территориально-распределенном предприятии (по выбору).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. 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

2. Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - 2-е изд. - М.: Форум: НИЦ ИНФРА-М, 2014. - 448 с.: ISBN 978-5-91134-833-5 Режим доступа: http://znanium.com/catalog.php?bookinfo=435900

3. Информационные системы и модели. Элективный курс / Семакин И.Г. - М. : БИНОМ, 2012. http://www.studentlibrary.ru/ book/ISBN9785996309221.html

4. Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - http://www.studentlibrary.ru/book/ISBN9785991202756.html

5. Проектирование информационных систем: Учебное пособие / В.В. Коваленко. - М.: Форум: НИЦ ИНФРА-М, 2014. - 320 с.: ISBN 978-5-91134-549-5. Режим доступа: http://znanium.com/catalog.php?bookinfo=473097

б) Дополнительная литература:

1. Информационные системы: учебник для студ. учреждений высш. образования / С.А. Жданов, М.Л. Соболева, А.С. Алфимова - М. : Прометей, 2015. http://www.studentlibrary.ru/book/ISBN9785990626447.html

2. Информационные технологии: Учебное пособие / Л.Г. Гагарина, Я.О. Теплова, Е.Л. Румянцева и др.; Под ред. Л.Г. Гагариной - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. - 320 с.: ISBN 978-5-8199-0608-8. Режим доступа: http://znanium.com/catalog.php?bookinfo=471464

3. 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

4. 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.

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 зав. кафедрой ИЗИ д.т.н. Монахов М.Ю.

(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 28.12.2016 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 28.12.2016 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: _____