Уп2015

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

Информационно-аналитические системы безопасности

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	2/72	18		36	18	Зачет
Итого	2/72	18		36	18	Зачет

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационно-аналитические системы безопасности» 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 информационно – аналитическими системами безопасности, с типовой структурой корпоративной информационной системы, с методиками анализа и активного аудита безопасности такого класса систем, а также с наиболее вероятными угрозами информационной безопасности в корпоративной информационно-вычислительной среде.

Дисциплина обеспечивает необходимые знания для организации и управления службой безопасности на предприятии, комплектования ее профессионально подготовленными кадрами. Задачей изучения дисциплины «Информационно-аналитические системы безопасности» является: - подготовка специалистов для научно-исследовательской деятельности в создании технологий обработки, хранения, передачи и защиты информации, в организации распределённых и высокопроизводительных вычислений, в вычислительной математике и моделировании, а так же для применения современных информационных технологий для науки, экономики на основе фундаментального образования, позволяющего выпускникам быстро адаптироваться к меняющимся потребностям общества; развитие у студентов личностных качеств и формирование общекультурных и профессиональных компетенций в соответствии с ФГОС ВО по данному направлению подготовки.

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 «Анализ и моделирование информационно-телекоммуникационных сетей», «Методы и средства защиты объектов информатизации», «Методология информационной безопасности», «Оценка и контроль обеспечения информационной безопасности», «Методы информационно-аналитической работы». 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», «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-8 – способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

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

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** - теоретико-методологические основы защиты информации в информационно-аналитических системах; - базовые принципы организации технологического процесса обработки информации; - назначение и принципы функционирования технических средств защиты информации в информационно-аналитических системах; - основы архитектуры информационных систем, типовые подходы к анализу бизнес-процессов предприятия; - информационные источники и аналитические методы конкурентной разведки, систему мер противодействия промышленному шпионажу (ПК-8; ПК-9);

2) ***Уметь:*** - внедрять и настраивать типовые средства защиты информации в информационно-аналитических системах; - составлять типовые формы документов, проектировать простые базы данных, соотносящиеся с документооборотом; - составлять IDEF0 и IDEF3 диаграммы бизнес-процессов, строить карты информационных систем и информационных потоков; - анализировать и составлять политики информационной безопасности для информационно-аналитических систем; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; - использовать организационные, правовые и программно-аппаратные методы защиты информации в информационно-аналитических системах (ПК-8; ПК-9);

3) ***Владеть:*** - навыками управления информационной безопасностью простых объектов; - навыками работы с одной из имеющихся на рынке информационно-аналитических систем (ПК-8; ПК-9).

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

- способность оценивать эффективность функционирования информационно-аналитических систем безопасности и проверять соответствие имеющихся информационно-аналитических систем безопасности требованиям отечественных и зарубежных стандартов в области информационной безопасности.

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 промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1.	Основные направления обеспечения безопасности объекта.	3	1-2	2		4		2		2/33%	
2.	Концептуальная модель безопасности предприятия (фирмы).	3	3-4	2		4		2		2/33%	
3.	Информационно-аналитическое обеспечение предпринимательской деятельности и безопасности бизнеса.	3	5-6	2		4		2		4/66%	Рейтинг-контроль №1
4.	Построение системы защиты коммерческой тайны на предприятии.	3	7-8	2		4		2		2/33%	
5.	Персонал и безопасность предприятия.	3	9-10	2		4		2		4/66%	
6.	Психологическое обеспечение безопасности предпринимательской деятельности.	3	11-12	2		4		2		2/33%	Рейтинг-контроль №2
7.	Финансовая составляющая безопасности предприятия.	3	13-14	2		4		2		2/33%	
8.	Криминальные сообщества, недобросовестная конкуренция и безопасность предприятия.	3	15-16	2		4		2		2/33%	
9.	Методические основы обеспечения информационной безопасности объекта. План защиты объекта и его реализация	3	17-18	2		4		2		2/33%	Рейтинг-контроль №3
Всего				18		36		18		22/41%	Зачет

Содержание дисциплины «Информационно-аналитические системы безопасности»

Раздел 1. Основные направления обеспечения безопасности объекта.

Раздел 2. Концептуальная модель безопасности предприятия (фирмы).

Раздел 3. Информационно-аналитическое обеспечение предпринимательской деятельности и безопасности бизнеса.

Раздел 4. Построение системы защиты коммерческой тайны на предприятии.

Раздел 5. Персонал и безопасность предприятия.

Раздел 6. Психологическое обеспечение безопасности предпринимательской деятельности.

Раздел 7. Финансовая составляющая безопасности предприятия.

Раздел 8. Криминальные сообщества, недобросовестная конкуренция и безопасность предприятия.

Раздел 9. Методические основы обеспечения информационной безопасности объекта. План защиты объекта и его реализация.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Информационно-аналитические системы безопасности» 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

- Назовите основные направления обеспечения безопасности предприятия.
- Определите цели и задачи системы безопасности предприятия.
- Представьте возможную структуру службы безопасности предприятия.
- Что такое и зачем необходима концепция безопасности предприятия?
- Что такое «угроза» безопасности предприятия?
- Приведите основные параметры концептуальной модели безопасности предприятия.
- Прокомментируйте организацию информационного процесса в компании.

• Перечислите классические объекты наблюдения и информационные источники фактографических данных.
• Охарактеризуйте основные каналы получения информации.
• Назовите и прокомментируйте основные положения правовых документов (Законов РФ), регламентирующих законную основу сбора информации о предприятиях сторонними субъектами.
• Назовите основные легальные, полулегальные и нелегальные методы сбора информации.

Вопросы рейтинг-контроля №2

• Почему качественный подбор и расстановка кадров является условием обеспечения безопасности организации.
• Предложите перечень сведений при проверке личности кандидата на работу.
• Назовите качества и особенности личности, могущие способствовать вовлечению в деятельность, направленную на нанесение ущерба организации.
• Прокомментируйте мошенничество как угрозу безопасности предприятию (причины, способы и формы проявления).
• Определите сущность финансовой составляющей экономической безопасности предприятия.
• Назовите составные части обеспечения финансовой составляющей экономической безопасности предприятия.
• Приведите вид карты расчета эффективности принимаемых мер по обеспечению финансовой составляющей экономической безопасности предприятия.

Вопросы рейтинг-контроля №3

• Определите объекты и субъекты информационной безопасности предприятия.
• Охарактеризуйте понятие угрозы информационной безопасности предприятия и прокомментируйте ее основные свойства.
• Что понимают под ущербом, наносимым предприятию в результате воздействия угроз информационной безопасности.
• Систематизируйте и проанализируйте организационные каналы передачи и обмена информацией.
• Охарактеризуйте основные методы, силы и средства, используемые для организации системы защиты информации.
• Как обеспечить безопасность компании при найме персонала? Критерии пригодности, этапы отбора кандидатов.
• Как обеспечить проверку работника на лояльность фирме, на честность в работе, на возможные связи с криминальными структурами, на соблюдение коммерческой тайны.
• Какие новые психотехнологии работы с персоналом могут обеспечить безопасность предприятия.
• Недобросовестная конкуренция, ее место в современной экономики.
• Основные методы противодействия недобросовестной конкуренции.

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

1. Назовите основные направления обеспечения безопасности предприятия.
2. Определите цели и задачи системы безопасности предприятия.
3. Представьте возможную структуру службы безопасности предприятия.
4. Что такое и зачем необходима концепция безопасности предприятия?
5. Что такое «угроза» безопасности предприятия?
6. Приведите основные параметры концептуальной модели безопасности предприятия.
7. Прокомментируйте организацию информационного процесса в компании.

8. Перечислите классические объекты наблюдения и информационные источники фактографических данных.
9. Охарактеризуйте основные каналы получения информации.
10. Назовите и прокомментируйте основные положения правовых документов (Законов РФ), регламентирующих законную основу сбора информации о предприятиях сторонними субъектами.
11. Назовите основные легальные, полулегальные и нелегальные методы сбора информации.
12. Почему качественный подбор и расстановка кадров является условием обеспечения безопасности организации.
13. Предложите перечень сведений при проверке личности кандидата на работу.
14. Назовите качества и особенности личности, могущие способствовать вовлечению в деятельность, направленную на нанесение ущерба организации.
15. Прокомментируйте мошенничество как угрозу безопасности предприятию (причины, способы и формы проявления).
16. Определите сущность финансовой составляющей экономической безопасности предприятия.
17. Назовите составные части обеспечения финансовой составляющей экономической безопасности предприятия.
18. Приведите вид карты расчета эффективности принимаемых мер по обеспечению финансовой составляющей экономической безопасности предприятия.
19. Определите объекты и субъекты информационной безопасности предприятия.
20. Охарактеризуйте понятие угрозы информационной безопасности предприятия и прокомментируйте ее основные свойства.
21. Что понимают под ущербом, наносимым предприятию в результате воздействия угроз информационной безопасности.
22. Систематизируйте и проанализируйте организационные каналы передачи и обмена информацией.
23. Охарактеризуйте основные методы, силы и средства, используемые для организации системы защиты информации.
24. Как обеспечить безопасность компании при найме персонала? Критерии пригодности, этапы отбора кандидатов.
25. Как обеспечить проверку работника на лояльность фирме, на честность в работе, на возможные связи с криминальными структурами, на соблюдение коммерческой тайны.
26. Какие новые психотехнологии работы с персоналом могут обеспечить безопасность предприятия.
27. Недобросовестная конкуренция, ее место в современной экономики.
28. Основные методы противодействия недобросовестной конкуренции.

Темы лабораторных работ:

Лабораторная работа №1 Поиск информации в Internet, поисковых системах и социальных сетях

Лабораторная работа №2 Изучение информационно-аналитической платформы Deductor 5.0. Знакомство с аналитической платформой «Deductor» .

Лабораторная работа №3 Изучение информационно-аналитической платформы Deductor 5.0. Реализация алгоритма построения деревьев решений …

Лабораторная работа №4 Изучение информационно-аналитической платформы Deductor 5.0. Логистическая регрессия и ROC-анализ

Лабораторная работа №5 Изучение информационно-аналитической платформы Deductor 5.0. Применение алгоритма кластеризации: самоорганизующиеся карты Кохонена

Лабораторная работа №6 Изучение информационно-аналитической платформы Deductor 5.0. Поиск ассоциативных правил

Вопросы и задания к самостоятельной работе магистрантов

- Информационно-аналитическая деятельность в системе безопасности.
- Задачи аналитиков служб безопасности.
- Требования к информационно-аналитической системе службы безопасности.
- Выявление связей и отношений объекта анализа с прочими объектами.
- Работа с внешними источниками, как коммерческого характера, так и предоставляемых в качестве обмена прочими структурами;
- Работа с неструктурированной информацией;
- Представление данных в ходе анализа, а также его результатов в виде диаграмм и схем.
- Формулирование умозаключений и выводов об объектах анализа.
- Оформление результатов анализа в виде аналитических записок и отчетов.
- Использование специализированных аналитических функций.
- Цели и задачи конкурентной разведки.
- Создание Конкурентной разведки на предприятии.
- Интернет и компьютеры как инструменты конкурентной разведки.
- Элементы контрразведывательной деятельности в работе службы безопасности предприятия.
- Координация деятельности структурных подразделений предприятия по выявлению агентуры конкурента, «агентов влияния» и т.д.
- Привлечение сотрудников своего предприятия к участию в работе службы безопасности.
- Инсайдеры. Методы борьбы с инсайдерами.
- Информационные технологии в системе информационно-аналитического обеспечения безопасности.
- Группа поисковых роботов (в Рунете — на русском языке, в Интернете -на основных европейских языках).
- Требования к информационно-аналитической системе службы безопасности.
- Работа с различными типажами объектов. Выявление связей и отношений объекта анализа с прочими объектами.
- Оформление результатов анализа в виде аналитических записок и отчетов.
- Использование специализированных аналитических функций.
- Конкурентная разведка. Разведка в бизнесе. Задачи конкурентной разведки. Разведывательный цикл обработки информации.
- Принципы организации информационной работы в компании.
- Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 "Обеспечение ИБ организаций банковской системы РФ. Общие положения"
- Исследование службой безопасности предприятия анонимных текстов на предмет выявления их авторов.
- Организация работ по обеспечению безопасности информации на предприятии.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Информационные аналитические системы: учебник / Т. В. Алексеева, Ю. В. Амириди, В. В. Дик и др.; под ред. В. В. Дика. - М.: МФПУ Синергия, 2013. - 384 с. ISBN 978-5-4257-0092-6. Режим доступа: http://znanium.com/catalog.php?bookinfo=451186

2. 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

3. 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

4. Информационно-аналитическая работа в государственном и муниципальном управлении: Учебное пособие / А.В. Зобнин. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2015. - 176 с.: ISBN 978-5-9558-0398-2. Режим доступа: http://znanium.com/catalog.php?bookinfo=470914

б) Дополнительная литература:

1. Информационный менеджмент / Под науч. ред. Н.М. Абдикеева. - М.: ИНФРА-М, 2009. - 400 с.: (Научная мысль). ISBN 978-5-16-003940-4 Режим доступа: http://znanium.com/catalog.php?bookinfo=182722

2. Конкурентная разведка в Internet. Советы аналитика / Дудихин В.В., Дудихина О.В. - М. : ДМК Пресс, 2009. - http://www.studentlibrary.ru/book/ISBN5940741789.html 192 с.

3. Аудит безопасности Intranet / Петренко С.А., Петренко А.А. - М. : ДМК Пресс, 2010. - http://www.studentlibrary.ru/book/ISBN5940741835.html

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. 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: _____