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

Методы и средства защиты объектов информатизации

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)
2	3/108	18	-	18	36	Экзамен (36ч)
Итого	3/108	18	-	18	36	Экзамен (36ч)

Владимир, 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Методы и средства защиты информации в системах электронного документооборота» 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 со сведениями о структуре и назначении системы электронного документооборота (СЭД), раскрытие сущности защиты информации в системе электронного документооборота, методики и технологии ее организации, принципов и содержания управления системой электронного документооборота, методов обеспечения ее безопасности. Задачами изучения дисциплины «Методы и средства защиты информации в системах электронного документооборота» является изучение вопросов:

- раскрытие сущности, целей и задач защиты информации в системах электронного документооборота (СЭД);
- определение принципов и этапов разработки защиты информации в СЭД;
- овладение методами оценки уязвимости защищаемой информации в СЭД;
- определение состава мероприятий по обеспечению функционирования защиты информации в СЭД;
- раскрытие структуры и методов управления защитой информации в СЭД.

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, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.04.01 «Информационная бкзопасность» по курсам «Технологии обеспечения информационной безопасности», «Теоретические основы компьютерной безопасности», «Информационно-аналитические системы безопасности». Кроме того, требования к «входным» знаниям, умениям и готовностям обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Документооборот» 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-2 – способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-14 – способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-15 – способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** - многообразие систем электронного документооборота, их функциональные возможности и сферы применения; задачи анализа предметной области и методы их решения; - правила оформления организационно-распорядительной документации; - правила организации защиты документооборота на предприятии и порядок прохождения документов; - подходы к построению систем обработки и защиты документов и место этих систем в информационной системе предприятия; - современные технологии, методы и средства защиты информации в области электронного делопроизводства и документооборота; - основные тенденции развития информационных систем в области делопроизводства и документооборота; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем (ПК-2; ПК-14; ПК-15);

2) ***Уметь:*** - устанавливать программные продукты для построения приложений автоматизации управленческих и документных процессов; - устанавливать дополнительное программное обеспечение, упрощающие рутинные задачи администратора баз данных; - использовать в работе с документами современные системы управления базами данных; - обеспечивать необходимый уровень безопасности при работе с информацией и документами; - управлять этапами жизненного цикла документа и бизнес-процессами электронного документооборота; - организовывать систему защиты документооборота на базе современных программных продуктов; - выполнять анализ современных систем электронного документооборота по степени защиты; - выполнять работы по сопровождению информационных систем, ориентированных на работу с электронными документами; - иметь представление об использовании электронной цифровой подписи; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности (ПК-2; ПК-14; ПК-15);

3) ***Владеть:*** - организацией контроля защищенности электронных документов; - современными информационными технологиями в области защиты электронного делопроизводства и документооборота; - правилами работы с электронными документами в соответствии со стандартами; - типовыми бизнес-процессами электронного документооборота; - моделированием информационных процессов в области электронного документооборота; - проектированием систем защиты документооборота, ориентированных на работу с электронными документами; - методами защиты современных систем электронного документооборота; - методами сопровождения информационных систем, ориентированных на работу с электронными документами (ПК-2; ПК-14; ПК-15).

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

- способность проверять соответствие имеющихся систем электронного документооборота 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.	Общая классификация технических средств обеспечения информационной безопасности	3	1-2	2		2		4		1/25%	
2.	Внедрение ТС проектирование, , монтаж ТС, пуско-наладочные работы).	3	3-4	2		2		4		2/50%	
3.	Технические средства предотвращения утечки информации по техническим каналам.	3	5-6	2		2		4		2/50%	Рейтинг-контроль №1
4.	Технические средства недопущения НСД.	3	7-8	2		2		4		1/25%	
5.	Технические средства СКУД.	3	9-10	2		2		4		1/25%	
6.	Технические средства СВН.	3	11-12	2		2		4		2/50%	Рейтинг-контроль №2
7.	Основы организации службы защиты информации на объекте, ее основные и вспомогательные функции.	3	13-14	2		2		4		1/25%	
8.	Защита информации в электронных банковских и платежных системах.	3	15-16	2		2		4		1/25%	
9.	Аттестация объектов информатизации и выделенных помещений. Проведение специальных проверок и специальных обследований.	3	17-18	2		2		4		2/50%	Рейтинг-контроль №3
Всего				18		18		36		13/36%	Экзамен

Содержание дисциплины «Методы и средства защиты объектов информатизации»

Раздел 1. Общая классификация технических средств обеспечения информационной безопасности, защиты информации, охраны и безопасности.

Раздел 2. Внедрение ТС проектирование, , монтаж ТС, пуско-наладочные работы). Эксплуатационно-техническое обслуживание ТС Ремонты ТС. Обучение и профподготовка кадров.

Раздел 3. Технические средства предотвращения утечки информации по техническим каналам. Общая классификация. Понятия каналов утечки информации по техническим каналам Акустоэлектрические преобразования. Утечка информации по каналам связи.

Раздел 4. Технические средства недопущения Н.С.Д. на объекты и в помещения Средства ОТС, определения. Требования по обеспечению ИТУ объектов. Классификация типов защиты ИТУ объектов по классам защиты. Классификация извещателей, СПИ и оповещателей.

Раздел 5. Технические средства СКУД. Классификация типов СКУД, основные определения. Структура СКУД, типы устройств. Виды считывателей и идентификаторов. Биометрическая идентификация.

Раздел 6. Технические средства СВН. Классификация типов СВН, основные определения. Видеокамеры и объективы, классификация, типы, основные характеристики. Мультиплексоры, коммутаторы, видеорегистраторы, назначение и основные ТТД.

Раздел 7. Основы организации службы защиты информации на объекте, ее основные и вспомогательные функции. Организация постов и маршрутов. Дисклокация нарядов, обеспечение средствами связи, специальными средствами, средствами активной обороны, вооружением. Контроль за несением службы.

Раздел 8. Защита информации в электронных банковских и платежных системах. Защита банкоматов и платежных терминалов. Способы осуществления атак и взломов. Методы защиты.

Раздел 9. Аттестация объектов информатизации и выделенных помещений. Проведение специальных проверок и специальных обследований. Специальные исследования.
Технический контроль эффективности мер по организации защиты информации от утечек по техническим каналам.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Методы и средства защиты объектов информатизации» предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления магистра по направлению 10.04.01 «Информационная безопасность».

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 СТУДЕНТОВ

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

- Дайте классификацию акустоэлектрических преобразователей.
- Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
- Принцип действия емкостных акустоэлектрических преобразователей.
- Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
- Классификация каналов утечки информации.
- Физическая сущность и основные свойства оптического канала утечки информации.

- Физическая сущность акустического канала утечки информации.
- Физическая сущность радиоэлектронного канала утечки информации.
- Физическая сущность акустооптического канала утечки информации.
- Физическая сущность акусто-вибрационного канала утечки информации.
- Классификация методов защиты от утечки по техническим каналам.
- Технические мероприятия по защите информации с помощью пассивных технических средств.
- Технические мероприятия по защите информации с помощью активных технических средств.
- Электростатическое экранирование технических средств.
- Магнитостатическое экранирование технических средств.
- Электромагнитное экранирование технических средств.
- Заземление технических средств.
- Развязывание информационных сигналов .
- Фильтрация информационных сигналов.
- Пространственное зашумление.
- Линейное зашумление.
- Пассивные методы защиты акустической (речевой) информации.
- Активные методы защиты акустической (речевой) информации.
- Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи.
- Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения.
- Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи.
- Защита телефонных линий компенсационным методом и методом "выжигания".
- Какие бывают категории (группы объектов), какие объекты к какой категории относятся?
- Основные требования по технической укрепленности периметров охраняемых территорий.

Вопросы рейтинг-контроля №2

- Какие существуют категории объектов и какие объекты относятся к группе Б1?
- Какие существуют категории объектов и какие объекты относятся к группе А1?
- Какие существуют категории объектов и какие объекты относятся к группе А2?
- Что является рубежом охраны? Сколько есть рубежей охраны, что они защищают и какие извещатели используются в рубежах охраны?
- Что защищает 1 рубеж охраны? Какие извещатели используются в 1 рубеже охраны, какие строительные конструкции и каким образом они защищают, как устанавливаются?
- Что защищает 2 рубеж охраны? Какие извещатели используются во 2 рубеже охраны, что и каким образом они защищают, как устанавливаются?
- Что защищает 3 рубеж охраны? Какие извещатели используются в 3 рубеже охраны, что и каким образом они защищают, как устанавливаются?
- Классификация охранных извещателей.
- Какие бывают извещатели для защиты окон на разбитие? Каким образом они защищают окна, как устанавливаются, приведите примеры.
- Какие бывают извещатели для защиты окон и дверей на открытие? Каким образом они устанавливаются, приведите примеры.
- Классификация приемно-контрольных приборов.
- Классификация СПИ. Приведите примеры разных типов СПИ.
- Задачи технической эксплуатации ТСО.

- Составные части технической эксплуатации ТСО.
- Назначение параметра «время на вход» для шлейфа сигнализации.

Вопросы рейтинг-контроля №3

- Классификация идентификаторов по физическому принципу действия.
- Идентификация на основе проксимити карт.
- Идентификация с использованием штрихкодов.
- Идентификация с использованием карт Виганда.
- Идентификация с использованием магнитных карт.
- Идентификация с использованием смарт-карт.
- Идентификация с использованием электронных таблеток Touch Memory.
- Квазидинамические и статические биометрические признаки.
- Связанные точки доступа СКУД.
- Основные технические характеристики СКУД.
- Исполнительные устройства СКУД.
- Преграждающие устройства СКУД.
- Основные технические характеристики видеокамер.
- Классификация видеокамер.
- Основные технические характеристики объективов видеокамер.
- Общая структурная схема видеокамеры, назначение составных частей.
- Какова цель задачи обнаружения в системах охранного телевидения?
- Какова цель задачи различения в системах охранного телевидения?
- Какова цель задачи идентификации в системах охранного телевидения?
- Каково назначение диафрагмы. Какие существуют способы управления диафрагмой?
- Дайте определение и поясните физический смысл понятия разрешающей способности видеокамеры.
- Что такое гамма-коррекция видеокамеры?
- Дайте определение и поясните физический смысл понятия чувствительности видеокамеры.
- Основные технические характеристики объективов видеокамер.
- Дайте определение и поясните физический смысл понятия фокусного расстояния и апертуры объектива.
- Понятие геометрической (сферической) и хроматической аберрации объектива.
- Классификация объективов по способу управления диафрагмой объектива.
- Классификация объективов по фокусному расстоянию и углу обзора.
- Какие существуют объективы по способу крепления к камере?
- Общие стандарты беспроводных сетей (Bluetooth, WiFi, сотовой связи).
- Стандарты беспроводных сетей WiFi.
- Стандарты сетей сотовой связи.
- Способы осуществления атак на сети Bluetooth.
- Механизмы защиты сетей Bluetooth.
- Способы осуществления атак на сети WiFi.
- Механизмы защиты сетей WiFi.
- Способы осуществления атак на сети сотовой связи.
- Механизмы защиты сетей сотовой связи.
- Основные требования по защите банкоматов и платежных терминалов.
- Способы осуществления атак и взломов банкоматов и платежных терминалов.
- Нормативное обеспечение аттестации объектов информатизации и выделенных помещений;
- Порядок проведения аттестации объектов информатизации и выделенных помещений;

- Документация составляемая по итогам проведения аттестации объектов информатизации и выделенных помещений;
- Проведение специальных проверок объектов информатизации и выделенных помещений;
- Проведение специальных обследований объектов информатизации и выделенных помещений;
- Проведение категорирования объектов информатизации и выделенных помещений;
- Проведение категорирования информационных систем.

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

1. Дайте классификацию акустоэлектрических преобразователей.
2. Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
3. Принцип действия емкостных акустоэлектрических преобразователей.
4. Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
5. Классификация каналов утечки информации.
6. Физическая сущность и основные свойства оптического канала утечки информации.
7. Физическая сущность акустического канала утечки информации.
8. Физическая сущность радиоэлектронного канала утечки информации.
9. Физическая сущность акустооптического канала утечки информации.
10. Физическая сущность акусто-вибрационного канала утечки информации.
11. Классификация методов защиты от утечки по техническим каналам.
12. Технические мероприятия по защите информации с помощью пассивных технических средств.
13. Технические мероприятия по защите информации с помощью активных технических средств.
14. Электростатическое экранирование технических средств.
15. Магнитостатическое экранирование технических средств.
16. Электромагнитное экранирование технических средств.
17. Заземление технических средств.
18. Развязывание информационных сигналов .
19. Фильтрация информационных сигналов.
20. Пространственное зашумление.
21. Линейное зашумление.
22. Пассивные методы защиты акустической (речевой) информации.
23. Активные методы защиты акустической (речевой) информации.
24. Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи.
25. Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения.
26. Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи.
27. Защита телефонных линий компенсационным методом и методом "выжигания".
28. Какие бывают категории (группы объектов), какие объекты к какой категории относятся?
29. Основные требования по технической укрепленности периметров охраняемых территорий.
30. Какие существуют категории объектов и какие объекты относятся к группе Б1?
31. Какие существуют категории объектов и какие объекты относятся к группе А1?
32. Какие существуют категории объектов и какие объекты относятся к группе А2?
33. Что является рубежом охраны? Сколько есть рубежей охраны, что они защищают и какие извещатели используются в рубежах охраны?

34. Что защищает 1 рубеж охраны? Какие извещатели используются в 1 рубеже охраны, какие строительные конструкции и каким образом они защищают, как устанавливаются?
35. Что защищает 2 рубеж охраны? Какие извещатели используются во 2 рубеже охраны, что и каким образом они защищают, как устанавливаются?
36. Что защищает 3 рубеж охраны? Какие извещатели используются в 3 рубеже охраны, что и каким образом они защищают, как устанавливаются?
37. Классификация охранных извещателей.
38. Какие бывают извещатели для защиты окон на разбитие? Каким образом они защищают окна, как устанавливаются, приведите примеры.
39. Какие бывают извещатели для защиты окон и дверей на открытие? Каким образом они устанавливаются, приведите примеры.
40. Классификация приемно-контрольных приборов.
41. Классификация СПИ. Приведите примеры разных типов СПИ.
42. Задачи технической эксплуатации ТСО.
43. Составные части технической эксплуатации ТСО.
44. Назначение параметра «время на вход» для шлейфа сигнализации.
45. Что такое «тихая тревога»?
46. Что такое тревога «по принуждению»?
47. Что такое самовосстанавливающиеся шлейфы сигнализации?
48. Какие шлейфы сигнализации называются самовосстанавливающимися?
49. Каковы основные причины ложных срабатываний ТСО?
50. Какие существуют виды обследования объектов?
51. Что проверяется при обследовании состояния ТСО объекта?
52. Классификация идентификаторов по физическому принципу действия.
53. Идентификация на основе проксимити карт.
54. Идентификация с использованием штрихкодов.
55. Идентификация с использованием карт Виганда.
56. Идентификация с использованием магнитных карт.
57. Идентификация с использованием смарт-карт.
58. Идентификация с использованием электронных таблеток Touch Memory.
59. Квазидинамические и статические биометрические признаки.
60. Связанные точки доступа СКУД.
61. Основные технические характеристики СКУД.
62. Исполнительные устройства СКУД.
63. Преграждающие устройства СКУД.
64. Основные технические характеристики видеокамер.
65. Классификация видеокамер.
66. Основные технические характеристики объективов видеокамер.
67. Общая структурная схема видеокамеры, назначение составных частей.
68. Какова цель задачи обнаружения в системах охранного телевидения?
69. Какова цель задачи различения в системах охранного телевидения?
70. Какова цель задачи идентификации в системах охранного телевидения?
71. Каково назначение диафрагмы. Какие существуют способы управления диафрагмой?
72. Дайте определение и поясните физический смысл понятия разрешающей способности видеокамеры.
73. Что такое гамма-коррекция видеокамеры?
74. Дайте определение и поясните физический смысл понятия чувствительности видеокамеры.
75. Основные технические характеристики объективов видеокамер.
76. Дайте определение и поясните физический смысл понятия фокусного расстояния и апертуры объектива.
77. Понятие геометрической (сферической) и хроматической аберрации объектива.
78. Классификация объективов по способу управления диафрагмой объектива.

79. Классификация объективов по фокусному расстоянию и углу обзора.
80. Какие существуют объективы по способу крепления к камере?
81. Общие стандарты беспроводных сетей (Bluetooth, WiFi, сотовой связи).
82. Стандарты беспроводных сетей WiFi.
83. Стандарты сетей сотовой связи.
84. Способы осуществления атак на сети Bluetooth.
85. Механизмы защиты сетей Bluetooth.
86. Способы осуществления атак на сети WiFi.
87. Механизмы защиты сетей WiFi.
88. Способы осуществления атак на сети сотовой связи.
89. Механизмы защиты сетей сотовой связи.
90. Основные требования по защите банкоматов и платежных терминалов.
91. Способы осуществления атак и взломов банкоматов и платежных терминалов.
92. Нормативное обеспечение аттестации объектов информатизации и выделенных помещений;
93. Порядок проведения аттестации объектов информатизации и выделенных помещений;
94. Документация составляемая по итогам проведения аттестации объектов информатизации и выделенных помещений;
95. Проведение специальных проверок объектов информатизации и выделенных помещений;
96. Проведение специальных обследований объектов информатизации и выделенных помещений;
97. Проведение категорирования объектов информатизации и выделенных помещений;
98. Проведение категорирования информационных систем.

Перечень лабораторных работ:

Лабораторная работа №1. Организация и проведение обследования объектов на предмет состояния инженерно-технического укрепления

Лабораторная работа №2. Проектирование охранно-тревожной сигнализации объектов на основе оборудования интегрированной системы безопасности (ИСБ) «Орион» НВП «Болид»

Лабораторная работа №3. Программирование аппаратуры безопасности (ИСБ) «Орион» НВП «Болид»

Лабораторная работа №4. Изучение программного обеспечения АРМ ИСБ «Орион-Pro»

Лабораторная работа №5. Проектирование охранно-тревожной сигнализации объектов на основе радиоканального оборудования ВОРС «Стрелец»

Практическая работа №6. Программирование оборудования ВОРС «Стрелец» утилитой «WirelEx»

Вопросы и задания к самостоятельной работе магистрантов:

- Общая классификация технических средств обеспечения информационной безопасности, защиты информации, охраны и безопасности.
- Внедрение ТС (предпроектное обследование, проектирование, составление сметной документации, монтаж ТС, пуско-наладочные работы).
- Эксплуатационно-техническое обслуживание ТС (плановое и внеплановое обслуживание, периодичность и объем обслуживания, контроль ЭТО, ведение э/технической документации). Ремонты ТС (гарантии, обменный фонд и др.).
- Плановые замены ТС (сроки эксплуатации и сертификации).
- Обучение и профподготовка кадров.
- Ложные срабатывания ТС. Обследование объектов и технический надзор.
- Акустоэлектрические преобразования.
- Утечка информации по каналам связи. Понятия ОТСС и ВТСС.

- Пассивные ТС защиты (маскировка, экранирование, заземление, фильтрация и др.). Активные ТС защиты (линейное и пространственное зашумление, средства подавления диктофонов, защиты линий связи).
- Оборудование нелегального съема информации (телефонные закладки и их классификация, микрофоны, средства видеонаблюдения, комплексы радиоконтроля).
- Оборудование поиска закладных устройств (индикаторы поля, радиосканеры, интерсепторы, анализаторы спектра и частотомеры, комплексы радиоконтроля, нелинейные локаторы, оборудование защиты проводных линий, средства поиска диктофонов и видеокамер, радиолоаторы и пеленгаторы и т.д.).
- Требования по обеспечению инженерно-технического укрепления объектов.
- Классификация типов защиты ИТУ объектов по классам защиты.
- Классификация извещателей, СП и оповещателей.
- СПИ (принцип действия, ТТД, способ применения и эксплуатации).
- Понятия ИСБ.
- Тактика охраны объектов (основные понятия).
- Технические средства недопущения Н.С.Д. на объекты и в помещения.
- Виды считывателей и идентификаторов.
- Биометрическая идентификация. Типы исполнительных устройств. Типы заграждающих устройств.
- Технические средства СВН.
- Мультиплексоры, коммутаторы, видеорегистраторы, назначение и основные ТТД. Способы передачи видеосигнала.
- Основы организации службы защиты информации на объекте, ее основные и вспомогательные функции.
- Организация постов и маршрутов. Дисклокация нарядов, обеспечение средствами связи, специальными средствами, средствами активной обороны, вооружением.
- Контроль за несением службы. Технические средства контроля за несением службы.
- Обеспечение контрольно-пропускного и объектового режимов. Правила и порядок проведения досмотра.
- Защита информации в беспроводных сетях WiFi. Физические принципы функционирования. Стандарты. Способы осуществления атак.
- Методы защиты WiFi сетей. Защита информации в мобильных устройствах сотовой связи. Физические принципы функционирования. Стандарты.
- Защита информации в электронных банковских и платежных системах.
- Защита банкоматов и платежных терминалов. Способы осуществления атак и взломов. Методы защиты.
- Аттестация объектов информатизации и выделенных помещений.
- Проведение специальных проверок и специальных обследований.
- Специальные исследования акустических и виброакустических каналов. Специальные исследования ПЭМИН.
- Технический контроль эффективности мер по организации защиты информации от утечек по техническим каналам. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИН.
- Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.
- Методы контроля побочных электромагнитных излучений генераторов технических средств.
- Контроль технических средств и систем на соответствие установленным нормам на параметры в речевом диапазоне частот

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ».

а) Основная литература:

1. Тельный, А.В. Технические средства охраны : практикум для вузов / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова .— Владимир :2012 .— 139 с.
2. Тельный, А.В.. Инженерно-техническая защита информации. Системы охранного телевидения : учебное пособие / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова .— Владимир 2013 .— 143 с.
3. 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. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2, Режим доступа: http://znanium.com/catalog.php?bookinfo=405000
2. Соколов, А.И. Технические средства защиты информации : технические каналы утечки информации : учебное пособие / А. И. Соколов, М. Ю. Монахов ; ВлГУ .— Владимир:, 2007 .— 71 с.
3. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2015. - 322 с. ISBN 978-5-369-01450-9. Режим доступа: http://znanium.com/catalog.php?bookinfo=495249
4. Бугаков, В.П. Технические средства охраны : системы контроля и управления доступом : учебное пособие / В. П. Бугаков, А. В. Тельный ; Владимирский государственный университет (ВлГУ) .— Владимир : 2007 .— 147 с. :

в) Периодические издания:

1. Информационно-методический журнал «Защита информации. Конфидент» http://sec4all.net/konfj-5_03.html
2. Журнал «Алгоритм безопасности» http://www.algoritm.org/
3. Журнал " Information Security/Информационная безопасность" http://www.itsec.ru/insec-about.php
4. Журнал «Охрана: служба, технические средства, экономика» http://nicohrana.ru/o-zhurnale.html
5. Каталог журналов в области охраны и безопасности. http://secandsafe.ru/jurnaly/

г) Программное обеспечение и Интернет-ресурсы:

1. Сайты производителей оборудования ТСО (www.bolid.ru; www.argus-spectr.ru; www.rielta.ru; www.tinko.ru; www.secur.ru).
2. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
3. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
4. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
5. 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.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 10.04.01 «Информационная безопасность»

Рабочую программу составил: к.т.н., доцент каф. ИЗИ Тельный А.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 28.12.16 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.04.01 «Информационная безопасность»

Протокол № 4 от 28.12.16 года

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

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

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: _____