Уп2016

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

Технологии обеспечения информационной 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)
1	3/108	18		18	36	Экзамен (36ч)
Итого	3/108	18		18	36	Экзамен (36ч)

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Технологии обеспечения информационной 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 со структурой системы защиты информации объектов, средствах охраны и безопасности объектов; методике и технологиях организации безопасности объектов, принципы и содержание управления системой безопасности, методы обеспечения ее надежности.

Задачей изучения дисциплины «Технологии обеспечения информационной безопасности» является: • раскрытие сущности, целей и задач информационной безопасности (ИБ) объектов; • определение принципов и этапов разработки ИБ объектов; • освоение технологии установления состава защищаемой информации и объектов защиты; • овладение методами оценки уязвимости защищаемой информации; • определение показателей эффективности системы защиты информации объектов и методики ее оценки.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО МАГИСТРАТУРЫ

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.4). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

Дисциплина изучается на 1 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Основы информационной безопасности», «Техническая защита информации» 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», «Организационно-правовые механизмы обеспечения информационной безопасности», «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-1 – способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-2 – способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-3 – способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) ***Знать:*** - методы концептуального проектирования технологий обеспечения информационной безопасности; - принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по

техническим каналам, методы и средства контроля эффективности технической защиты информации; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - методы анализа и оценки угроз защищаемой информации; технологическое и организационное построение информационной защиты (ПК-1; ПК-2; ПК-3);

2) ***Уметь:*** - выбирать методы и средства, необходимые для организации и функционирования системы защиты информации;- обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; - анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; - формировать комплекс мер по информационной безопасности с учетом его технической обоснованности и реализуемости; - осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-1; ПК-2; ПК-3);

3) ***Владеть***: - навыками управления информационной безопасностью простых объектов; - методами технической защиты информации; - методами формирования требований по защите информации; -методами расчета и инструментального контроля показателей технической защиты информации; - профессиональной терминологией; -навыками поиска технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов в профессиональной деятельности;- квалифицированно использовать сетевые ресурсы с целью организации интерактивного взаимодействия, а также поиска и передачи информации в локальных и глобальных информационных сетях (ПК-1; ПК-2; ПК-3).

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

- способность проектировать системы защиты объектов от несанкционированного доступа и обеспечивать защиту информации на объекте от утечек по техническим каналам.

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, защиты информации, охраны и безопасности. Основные понятия, назначения подсистем, термины и определения. Технические средства н.с.д. к информационным ресурсам	1	1-2	2		2		4		1/25%	
2.	Организационные вопросы функционирования технических средств обеспечения информационной безопасности, защиты информации, охраны и безопасности. Внедрение ТС	1	3-4	2		2		4		2/50%	
3.	Технические средства предотвращения утечки информации по техническим Классификация каналов утечки информации	1	5-6	2		2		4		2/50%	Рейтинг-контроль №1
4.	Технические средства недопущения Н.С.Д. на объекты Технические ср-ва охранной сигнализации	1	7-8	2		2		4		1/25%	
5.	Технические средства недопущения Н.С.Д. на объекты Технические ср-ва СКУД и СВН	1	9-10	2		2		4		2/50%	
6.	Основы организации службы защиты информации на объекте, ее основные и вспомогательные функции.	1	11-12	2		2		4		1/25%	Рейтинг-контроль №2

№ 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		
7.	Защита информации в беспроводных сетях WiFi. Физические принципы функционирования. Стандарты. Способы осуществления атак. Методы защиты WiFi сетей.	1	13-14	2		2		4		2/50%	
8.	Защита информации в электронных банковских и платежных системах. Защита банкоматов и платежных терминалов. Способы осуществления атак и взломов. Методы защиты.	1	15-16	2		2		4		1/25%	
9.	Аттестация объектов информатизации и выделенных помещений. Проведение специальных проверок и специальных обследований.	1	17-18	2		2		4		1/25%	Рейтинг-контроль №3
Всего				18		18		36		13/36%	Экзамен

Содержание дисциплины «Технологии обеспечения информационной безопасности»

Раздел 1. Общая классификация технических средств обеспечения информационной безопасности, защиты информации, охраны и безопасности. Основные понятия, назначения подсистем, термины и определения. Технические средства НСД к информационным ресурсам.

Раздел 2. Организационные вопросы функционирования технических средств обеспечения информационной безопасности, защиты информации, охраны и безопасности. Внедрение технических средств.

Раздел 3. Технические средства предотвращения утечки информации по техническим каналам. Классификация каналов утечки информации.

Раздел 4. Технические средства недопущения НСД на объекты Технические средства охранной сигнализации.

Раздел 5. Технические средства защиты от НСД объекта. Средства СКУД и СВН.

Раздел 6. Основы организации службы защиты информации на объекте, ее основные и вспомогательные функции.

Раздел 7. Защита информации в беспроводных сетях WiFi. Физические принципы функционирования. Стандарты. Способы осуществления атак. Методы защиты WiFi сетей.

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.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Технологии обеспечения информационной безопасности объектов» 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 к рейтинг-контролю №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 .

Вопросы к рейтинг-контролю №2

- 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.
- 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.

Вопросы к рейтинг-контролю №3

- 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.
- Что такое «тихая тревога»?
- Что такое тревога «по принуждению»?
- Что такое самовосстанавливающиеся шлейфы сигнализации?
- Какие шлейфы сигнализации называются самовосстанавливающимися?
- Каковы основные причины ложных срабатываний ТСО?
- Какие существуют виды обследования объектов?
- Что проверяется при обследовании состояния ТСО объекта?
- 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.
- 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.

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. Общие стандарты беспроводных сетей (Bluetooth, WiFi, сотовой связи).
69. Стандарты беспроводных сетей WiFi.
70. Стандарты сетей сотовой связи.
71. Способы осуществления атак на сети Bluetooth.
72. Механизмы защиты сетей Bluetooth.
73. Способы осуществления атак на сети WiFi.
74. Механизмы защиты сетей WiFi.
75. Способы осуществления атак на сети сотовой связи.
76. Механизмы защиты сетей сотовой связи.
77. Основные требования по защите банкоматов и платежных терминалов.
78. Способы осуществления атак и взломов банкоматов и платежных терминалов.

Темы лабораторных работ:

Лабораторная работа №1 Поисковый прибор ST 031P (назначение и порядок работы)

Лабораторная работа №2 Поисковый прибор ST 031P (исследование проводных линий связи)

Лабораторная работа №3 Поисковый прибор ST 031P (Исследование акустической и виброакустической защиты помещения)

Лабораторная работа №4 Прибор проверки проводных линий «ULAN»

Лабораторная работа №5 «Исследование радиоэлектронной обстановки и радиоэлектронного канала утечки информации с помощью радиосканера «Icom IC-R1500»»

Лабораторная работа №6 «Исследование выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу с помощью программно-аппаратного комплекса «Спрут-мини-А»»

Лабораторная работа №7 «Исследование выполнения норм эффективности защиты речевой информации от утечки по виброакустическому каналу с помощью программно-аппаратного комплекса «Спрут-мини-А»»

Лабораторная работа №8 «Исследование выполнения норм эффективности защиты речевой информации от утечки за счет электроакустических преобразований в ТСПИ с помощью программно-аппаратного комплекса «Спрут-мини-А»»

Лабораторная работа №9 «Исследование выполнения норм эффективности защиты речевой информации от утечки за счет ПЭМИН от технических средств с помощью программно-аппаратного комплекса «Спрут-мини-А»»

Вопросы и задания к самостоятельной работе магистрантов:

- Организационные вопросы функционирования технических средств обеспечения информационной безопасности
- Внедрение ТСО
- Технические средства предотвращения утечки информации по техническим каналам
- Технические средства недопущения Н.С.Д. на объекты
- Технические средства СКУД и СВН
- Технические средства охранной сигнализации
- Основы организации службы защиты информации на объекте
- 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.
- Защита информации в беспроводных сетях WiFi.
- Методы защиты WiFi сетей.
- Защита информации в электронных банковских и платежных системах.
- Аттестация объектов информатизации и выделенных помещений.
- Проведение специальных проверок и специальных обследований.
- Фильтрация информационных сигналов.
- Пространственное зашумление.
- Линейное зашумление.
- Пассивные методы защиты акустической (речевой) информации.
- Активные методы защиты акустической (речевой) информации.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. 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

2. Защита в операционных системах Учебное пособие для вузов / Проскурин В.Г. - М. : Горячая линия - Телеком, 2014. - http://www.studentlibrary.ru/book/ISBN9785991203791.html

3. 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

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.

б) Дополнительная литература:

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

2. А.Ю. Щербаков. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с. - http://www.studentlibrary.ru/book/ISBN9785804103782.html

3. Охранные подразделения / Ворона В.А., Тихонов В.А. - Вып. 6. - М. : Горячая линия - Телеком, 2012. http://www.studentlibrary.ru/book/ISBN9785991202398.html

4. Офисный шпионаж / Мелтон К., Пилиджан К., Сверчински Д. - М. : Альпина Паблишер, 2013. - http://www.studentlibrary.ru/book/ISBN9785916712070.html. 182 с.

5. 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 «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. Журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html;
4. Журнал «Спецтехника и Связь», Режим доступа: http://www.st-s.su/

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 доцент кафедры ИЗИ к.т.н. Тельный А.В.

(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 28.12.16 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 28.12.16 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: _____