УП 2016

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«29» 12 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

(наименование дисциплины)

Специальность 10.05.04 "Информационно-аналитические системы безопасности"

Специализация "Автоматизация информационно-аналитической деятельности"

Уровень высшего образования специалитет

Форма обучения очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
1	3/108	18	18		72	Зачет
Итого	3/108	18	18		72	Зачет

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Основы информационной безопасности» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности» формирование у специалистов знаний и навыков в предметной области. Предмет курса - понятийный аппарат, а также сущность, теоретические, концептуальные, методологические аспекты и структура ИБ.

Профессиональные цели курса — раскрытие сущности и значения ИБ, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения информационной безопасности, классификация и характеристика составляющих ИБ, установление взаимосвязи и логической организации входящих в них компонентов.

К основным профессиональным задачам курса относятся:

- изучение понятийного аппарата в области ИБ;
- раскрытие базовых содержательных положений в области ИБ;
- изучение современной доктрины информационной безопасности;
- установление факторов, влияющих на ИБ;
- изучение методов определения состава защищаемой информации, классификация ее по видам тайны, материальным носителям, собственникам и владельцам;
- установление структуры угроз защищаемой информации;
- изучение направлений, видов, методов и особенностей деятельности разведывательных органов по добыванию конфиденциальной информации;
- раскрытие сущности компонентов защиты информации;
- определение назначения, сущности и структуры комплексных систем защиты информации.

Образовательные цели курса — раскрытие значения ИБ для субъектов информационных отношений (личности, общества, государства), роли защиты информации в обеспечении прав граждан, ее места в политической, экономической, военной и других областях деятельности, в безопасности функционирования различных хозяйственных и управленческих структур.

К основным образовательным задачам курса относятся:

- определение места ИБ в системе информационных отношений;
- определение направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение ИБ;
- раскрытие взаимосвязи между информационной безопасностью и удовлетворением информационных потребностей субъектов информационных отношений;
- определение значения обеспечения ИБ для предотвращения негативного информационного воздействия на субъекты информационных отношений.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.18). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий.

Дисциплина изучается на 1 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по стандартам среднего образования по курсам «Математика», «Информатика».

Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Принципы построения, проектирования и эксплуатации автоматизированных информационных систем», «Моделирование автоматизированных информационных систем», «Методы анализа данных и естественно-языковых текстов», «Базы данных и экспертные системы», «Безопасность электронного документооборота», «Безопасность операционных систем», «Лингвистическое обеспечение автоматизированных информационных систем», «Формализованные модели и методы решения аналитических задач» и др.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими общекультурными компетенциями:

ОК-5 – способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

общепрофессиональными компетенциями:

ОПК-7 способностью применять методы и средства обеспечения информационной безопасности специальных ИАС;

профессиональными компетенциями:

ПК-9 – способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах;

ПК-19 – способностью обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) Знать: - базовый понятийный аппарат в области ИБ; - виды и состав угроз информационной безопасности; - принципы и общие методы обеспечения информационной безопасности; - основные положения государственной политики обеспечения информационной безопасности; - критерии, условия и принципы отнесения информации к защищаемой; - виды носителей защищаемой информации; - виды тайн конфиденциальной информации; - виды уязвимости защищаемой информации; - источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; - каналы и методы несанкционированного доступа к конфиденциальной информации; - классификацию видов, методов и средств защиты информации (ОК-5; ОПК-7; ПК-9; ПК-19).

2) Уметь: - выявлять угрозы информационной безопасности применительно к объектам защиты; - определять состав конфиденциальной информации применительно к видам тайны; - выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия; - выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации; - определять направления и виды защиты информации с учетом характера информации и задач по ее защите; - организовывать системное обеспечение защиты информации (ОК-5; ОПК-7; ПК-9; ПК-19);

3) Владеть: - основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы (ОК-5; ОПК-7; ПК-9; ПК-19).

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

- способность применять основные закономерности развития информационных процессов для прикладных задач в области информационной безопасности с учетом действующих нормативных и методических документов.

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	Введение. Характеристика защищаемой информации	4	1-2	2	2			8		2 (50%)	
2	Значение ИБ и ее место в системе национальной безопасности	4	3-4	2	2			8		1(25%)	
3	Основные понятия и определения в области информационной безопасности и защиты информации	4	5-6	2	2			8		2(50%)	Рейтинг-контроль №1
4	Категории защищаемой информации	4	7-8	2	2			8		1(25%)	
5	Концептуальная модель системы информационной безопасности	4	9-10	2	2			8		2(50%)	
6	Действия, приводящие к незаконному овладению конфиденциальной информацией	4	11-12	2	2			8		1(25%)	Рейтинг-контроль №2
7	Угрозы конфиденциальной информации	4	13-14	2	2			8		2(50%)	
8	Способы защиты информации	4	15-16	2	2			8		1(25%)	
9	Уровни информационной безопасности	4	17-18	2	2			8		2(50%)	Рейтинг-контроль №3
Всего				18	18			72		14(39%)	Зачет

Содержание дисциплины «Основы информационной безопасности»

Раздел 1. Введение. Характеристика защищаемой информации

Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами. Структура курса. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний. Знания и умения студентов, которые должны быть получены в результате изучения курса. Признаковая структура объекта. Предметом защиты. Признаковая информация. Демаскирующие признаки объектов. Информативность демаскирующего признака. Свойства информации как предмета защиты. Основные носители признаковой информации. «Источник конфиденциальной информации».

Раздел 2. Значение ИБ и ее место в системе национальной безопасности

Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия. Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия "информационная безопасность". Значение информационной безопасности для субъектов информационных отношений. Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности. Понятие и назначение доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Виды и состав угроз информационной безопасности. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.

3. Основные понятия и определения в области информационной безопасности и защиты информации

Определение защищаемой информации. Основные признаки защищаемой информации. Собственники защищаемой информации.

4. Категории защищаемой информации

Сведения, которые могут быть отнесены к государственной тайне. Политический и экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну. Основные виды конфиденциальной информации, нуждающейся в защите. Коммерческая тайна. Банковская тайна. Основные объекты профессиональной тайны. Основные объекты интеллектуальной собственности.

5. Концептуальная модель системы информационной безопасности

Система безопасности. Основные компоненты концептуальной модели ИБ. Объекты угроз ИБ. Источники угроз . Цели угроз информации со стороны злоумышленников. Основные способы неправомерного овладения конфиденциальной информацией (способы доступа). Базовые способы защиты информации. Схема концептуальной модели системы ИБ.

6. Действия, приводящие к незаконному овладению конфиденциальной информацией

Основные способы несанкционированного доступа к конфиденциальной информации.

Обобщенная модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации. Утечка конфиденциальной информации.

«Разглашение» конфиденциальной информации.

7. Угрозы конфиденциальной информации

Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации.

Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

8. Способы защиты информации

Способ предупреждения возможных угроз. Основные действия способа выявления угроз
Способ обнаружения угроз. Способ пресечения или локализации угроз. Основные действия способа ликвидации последствий. Основные защитные действия при реализации способов ЗИ. Защита от разглашения. Защитные действия от утечки и от НСД к конфиденциальной информации. Мероприятия по технической защите информации.

9. Уровни информационной безопасности

Организационные основы как необходимые условия осуществления защиты информации. Условия, необходимые для обеспечения технологии защиты информации, а также сохранности и конфиденциальности информации. Значение методологических принципов защиты информации. Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации. Основные меры и архитектурные принципы обеспечения обслуживаемости ИС. Сервисы безопасности. Понятие и назначение технологического обеспечения защиты информации. Классификация организационно-технологических документов по защите информации. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий. Значение и виды контрольных мероприятий.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления специалиста по специальности 10.05.04 «Информационно-аналитические системы безопасности».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

- учебную дискуссию;
- электронные средства обучения (слайд-лекции, электронные тренажеры, компьютерные тесты);
- дистанционные (сетевые) технологии.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысления студентами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП специальности 10.05.04 «Информационно-аналитические системы безопасности», особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования не могут составлять более 55 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность студента в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1:

1. Что такое признаковая структура объекта?
2. Что понимают под полученной объектом информацией?
3. Какая информация является предметом защиты?
4. Что такое признаковая информация?
5. Почему семантическая информация по отношению к признаковой является вторичной?
6. Какие признаки объектов являются демаскирующими?
7. Приведите классификацию демаскирующих признаков объектов защиты.
8. Опишите опознавательные демаскирующие признаки объектов защиты.
9. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.

10. Что такое информативность демаскирующего признака?
11. Перечислите основные свойства информации как предмета защиты.
12. Почему информацию можно рассматривать как товар?
13. Изменяется ли цена информации во времени? Если да, то аргументируйте свой ответ.
14. Какой аналитической зависимостью можно аппроксимировать характер старения информации?
15. Что понимается под временем жизни информации?
16. Что такое количество информации?
17. Что такое тезаурус?
18. Почему информация способна случайным образом «растекаться» в пространстве?
19. Почему при копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается?
20. Перечислите основные носители признаковой информации.
21. Что такое «источник конфиденциальной информации»?
22. Перечислите основные источники конфиденциальной информации.
23. В чем отличие прямых источников семантической информации от косвенных?
24. Охарактеризуйте людей (сотрудники, обслуживающий персонал, продавцы, клиенты и др.) в качестве источника конфиденциальной информации.
25. Охарактеризуйте документы как источники конфиденциальной информации.
26. В чем специфика публикаций, докладов, статей, интервью, проспектов, книг и т.д. в качестве источников конфиденциальной информации?
27. Охарактеризуйте технические носители информации и документов как источники конфиденциальной информации.
28. Охарактеризуйте технические средства обработки информации - автоматизированные средства обработки информации и средства обеспечения производственной и трудовой деятельности, в том числе и средства связи в качестве источника конфиденциальной информации.
29. Охарактеризуйте выпускаемую продукцию как источник конфиденциальной информации.
30. Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации
31. Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?
32. Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
33. Дайте определение информационной безопасности, прокомментируйте его составляющие.
34. Что такое защита информации?
35. Перечислите основные категории информационной безопасности и дайте им определения.
36. Охарактеризуйте понятие доступности.
37. Охарактеризуйте понятие целостности.
38. Охарактеризуйте понятие конфиденциальности.
39. Приведите убедительные доводы того, что информационная безопасность – одна из важнейших проблем современной жизни.
40. Дайте определение национальной безопасности согласно Концепции национальной безопасности РФ.
41. В чем заключаются национальные интересы России?
42. Чем обеспечиваются национальные интересы России?
43. В чем заключаются национальные интересы России в информационной сфере?
44. Что такое государственная информационная политика?
45. Перечислите и прокомментируйте основные составляющие информационной безопасности РФ.
46. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.

47. Что такое угроза к контексте ИБ России?
48. Классифицируйте угрозы ИБ РФ по общей направленности.
49. В чем состоят угрозы ИБ для личности?
50. В чем состоят угрозы ИБ для общества?
51. В чем состоят угрозы ИБ для государства?
52. Классифицируйте угрозы ИБ РФ по происхождению и прокомментируйте их.
53. Перечислите основные принципы ИБ России согласно Доктрине.
54. Каковы функции государственной системы по обеспечению ИБ?
55. Охарактеризуйте государственную структуру органов, обеспечивающая информационную безопасность.
56. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
57. В чем специфика деятельности Федеральной службой по техническому и экспортному контролю (ФСТЭК России)?
58. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
59. В чем специфика деятельности Федеральной службы безо¬пасности?
60. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
61. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
62. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
63. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
64. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
65. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
66. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
67. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.

Вопросы рейтинг-контроля №2:

1. Какую информацию относят к защищаемой?
2. Дайте определение защищаемой информации.
3. Охарактеризуйте основные признаки защищаемой информации.
4. Перечислите и охарактеризуйте основных собственников защищаемой информации.
5. Что такое государственная тайна?
6. Приведите формальную модель определения государственных секретов
7. Перечислите сведения, которые могут быть отнесены к государственной тайне.
8. Какую информацию нельзя засекречивать как имеющую статус государст¬венной тайны?
9. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
10. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
11. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
12. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
13. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
14. Перечислите основные объекты банковской тайны.

15. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне? Перечислите и охарактеризуйте основные объекты профессиональной тайны.
16. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
17. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
18. Перечислите основные объекты интеллектуальной собственности.
19. Что понимается под системой безопасности?
20. Перечислите основные компоненты концептуальной модели ИБ.
21. Что такое объекты угроз ИБ и в чем они выражаются?
22. Каковы основные источники угроз защищаемой информации?
23. Каковы цели угроз информации со стороны злоумышленников?
24. Перечислите основные источники конфиденциальной информации.
25. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
26. Перечислите базовые способы защиты информации.
27. Изобразите графически схему концептуальной модели системы ИБ.
28. Приведите возможный перечень способов получения информации.
29. Дайте определение способа несанкционированного доступа к источникам конфиденциальной информации.
30. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
31. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
32. Что такое утечка конфиденциальной информации?
33. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
34. Как осуществляется утечка конфиденциальной информации?

Вопросы рейтинг-контроля №3:

1. Дайте определение угрозы конфиденциальной информации.
2. Что такое атака?
3. Что такое окно опасности?
4. Что такое угрозы воздействия на источник информации?
5. Что такое угрозы утечки информации?
6. Какие угрозы называются преднамеренными, а какие случайными?
7. Что такое канал несанкционированного доступа?
8. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
9. Что такое наблюдение в теории информационной безопасности?
10. Что такое подслушивание в теории информационной безопасности?
11. Что такое перехват в теории информационной безопасности?
12. Что такое технический канал утечки информации?
13. Охарактеризуйте случайный и организованный канал утечки информации.
14. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
15. Какие организации формируют структуру разведывательного сообщества США?
16. Прокомментируйте наиболее распространенные угрозы доступности.
17. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
18. Что такое отказ пользователей? Какое отношение данное понятие имеет к угрозам доступности?
19. Охарактеризуйте программные атаки на доступность.

20. Что такое вредоносное программное обеспечение?
21. Дайте определение «бомбы», «червя», «вируса».
22. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
23. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
24. Перечислите основные угрозы конфиденциальности информации
25. Что в ИБ понимают под маскарадом?
26. Дайте определение способа защиты информации.
27. Охарактеризуйте способ предупреждения возможных угроз.
28. Прокомментируйте основные действия способа выявления угроз
29. Охарактеризуйте способ обнаружения угроз.
30. Охарактеризуйте способ пресечения или локализации угроз.
31. Прокомментируйте основные действия способа ликвидации последствий.
32. Перечислите основные защитные действия при реализации способов ЗИ,
33. Что такое защита от разглашения?
34. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
35. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
36. Назовите три группы мероприятий по технической защите информации.
37. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
38. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
39. Прокомментируйте основные технические мероприятия по технической защите информации.
40. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
41. В чем заключается специфика управления, как сервиса безопасности?

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

1. Приведите классификацию демаскирующих признаков объектов защиты.
2. Опишите опознавательные демаскирующие признаки объектов защиты.
3. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
4. Почему при копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается?
5. Перечислите основные носители признаковой информации.
6. Что такое «источник конфиденциальной информации»?
7. Перечислите основные источники конфиденциальной информации.
8. В чем отличие прямых источников семантической информации от косвенных?
9. Перечислите основные категории информационной безопасности и дайте им определения.
10. Охарактеризуйте понятие доступности, целостности, конфиденциальности.
11. Дайте определение национальной безопасности согласно Концепции национальной безопасности РФ.
12. В чем заключаются и чем обеспечиваются национальные интересы России в информационной сфере?
13. Что такое государственная информационная политика?
14. Перечислите и прокомментируйте основные составляющие информационной безопасности РФ.
15. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
16. Классифицируйте угрозы ИБ РФ по общей направленности.
17. В чем состоят угрозы ИБ для личности?
18. В чем состоят угрозы ИБ для общества?
19. В чем состоят угрозы ИБ для государства?

20. Перечислите основные принципы ИБ России согласно Доктрине.
21. Охарактеризуйте государственную структуру органов, обеспечивающая информационную безопасность.
22. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
23. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
24. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
25. Охарактеризуйте основные признаки защищаемой информации.
26. Перечислите и охарактеризуйте основных собственников защищаемой информации.
27. Что такое государственная тайна?
28. Перечислите сведения, которые могут быть отнесены к государственной тайне.
29. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
30. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
31. Перечислите основные объекты банковской тайны.
32. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне? Перечислите и охарактеризуйте основные объекты профессиональной тайны.
33. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
34. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
35. Перечислите основные объекты интеллектуальной собственности.
36. Перечислите основные компоненты концептуальной модели ИБ.
37. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
38. Перечислите базовые способы защиты информации.
39. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
40. Что такое утечка конфиденциальной информации?
41. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
42. Как осуществляется утечка конфиденциальной информации?
43. Дайте определение угрозы конфиденциальной информации.
44. Какие угрозы называются преднамеренными, а какие случайными?
45. Что такое канал несанкционированного доступа?
46. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
47. Что такое наблюдение в теории информационной безопасности?
48. Что такое подслушивание в теории информационной безопасности?
49. Что такое перехват в теории информационной безопасности?
50. Что такое технический канал утечки информации?
51. Охарактеризуйте случайный и организованный канал утечки информации.
52. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
53. Прокомментируйте наиболее распространенные угрозы доступности.
54. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
55. Что такое отказ пользователей? Какое отношение данное понятие имеет к угрозам доступности?
56. Охарактеризуйте программные атаки на доступность.

57. Что такое вредоносное программное обеспечение?
58. Дайте определение способа защиты информации.
59. Охарактеризуйте способ предупреждения возможных угроз.
60. Прокомментируйте основные действия способа выявления угроз
61. Охарактеризуйте способ обнаружения угроз.
62. Охарактеризуйте способ пресечения или локализации угроз.
63. Прокомментируйте основные действия способа ликвидации последствий.
64. Перечислите основные защитные действия при реализации способов ЗИ,
65. Что такое защита от разглашения?
66. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
67. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
68. Назовите три группы мероприятий по технической защите информации.
69. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
70. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
71. Прокомментируйте основные технические мероприятия по технической защите информации.

Темы практических занятий.

1. Состав и классификация носителей защищаемой информации
2. Значение информационной безопасности и ее место в системе национальной безопасности. Современная доктрина информационной безопасности Российской Федерации
3. Критерии, условия и принципы отнесения информации к защищаемой. Классификация защищаемой информации по видам тайны и степеням конфиденциальности
4. Классификация защищаемой информации по собственникам и владельцам
5. Концептуальные основы защиты информации
6. Каналы и методы несанкционированного доступа к конфиденциальной информации
7. Понятие и структура угроз защищаемой информации. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию
8. Классификация видов, методов и средств защиты информации
9. Технологическое обеспечение защиты информации

Вопросы и задания для самостоятельной работы студентов:

Раздел 1

1. Какие признаки объектов являются демаскирующими?
2. Приведите классификацию демаскирующих признаков объектов защиты.
3. Опишите опознавательные демаскирующие признаки объектов защиты.
4. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
5. Что такое информативность демаскирующего признака?
6. Что такое тезаурус?
7. Перечислите основные носители признаковой информации.
8. Перечислите основные источники конфиденциальной информации.
9. В чем отличие прямых источников семантической информации от косвенных?
10. Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации

Раздел 2

1. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
2. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
3. В чем специфика деятельности Федеральной службы безопасности?

4. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
5. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
6. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
7. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
8. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
9. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
10. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
11. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.

Раздел 3

1. Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?
2. Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
3. Дайте определение информационной безопасности, прокомментируйте его составляющие.
4. Что такое защита информации?
5. Приведите убедительные доводы того, что информационная безопасность – одна из важнейших проблем современной жизни.

Раздел 4

1. Какую информацию нельзя засекречивать как имеющую статус государственной тайны?
2. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
3. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
4. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
5. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
6. Какая информация не может быть отнесена к коммерческой тайне?
7. Перечислите основные объекты банковской тайны.
8. Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
9. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
10. Перечислите основные объекты интеллектуальной собственности.

Раздел 5

1. Что такое объекты угроз ИБ и в чем они выражаются?
2. Каковы основные источники угроз защищаемой информации?
3. Каковы цели угроз информации со стороны злоумышленников?
4. Перечислите основные источники конфиденциальной информации.
5. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
6. Перечислите базовые способы защиты информации.
7. Изобразите графически схему концептуальной модели системы ИБ.

Раздел 6

1. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
2. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.

3. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
4. Как осуществляется утечка конфиденциальной информации?

Раздел 7

1. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
2. Что такое наблюдение в теории информационной безопасности?
3. Что такое подслушивание в теории информационной безопасности?
4. Что такое перехват в теории информационной безопасности?
5. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
6. Какие организации формируют структуру разведывательного сообщества США?
7. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
8. Охарактеризуйте программные атаки на доступность.
9. Приведите примеры «бомбы», «червя», «вируса».
10. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
11. Что в ИБ понимают под маскарадом?

Раздел 8

1. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
2. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
3. Назовите три группы мероприятий по технической защите информации.
4. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
5. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
6. Прокомментируйте основные технические мероприятия по технической защите информации.

Раздел 9

1. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
2. В чем заключается специфика управления, как сервиса безопасности?

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная 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. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: ISBN 978-5-00091-079-5, Режим доступа: http://znanium.com/catalog.php?bookinfo=508381
3. Интеллектуальные системы защиты информации : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html 172 с. -

б) Дополнительная литература:

1. 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
2. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html 474 с.
3. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. ISBN 978-5-00091-007-8. Режим доступа: http://znanium.com/catalog.php?bookinfo=491597

в) Периодические издания:

1. Отраслевой lifestyle-журнал по теме безопасности «Рубеж». Режим доступа: http://ru-bezh.ru/;
2. Журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html;
3. Журнал "Алгоритм безопасности» – Режим доступа: http://www.algoritm.org/index.php;
4. Электронный научный журнал «Проблемы безопасности» – Режим доступа: http://www.pb.littera-n.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/
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

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

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

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

Рабочую программу составил зав. кафедрой ИЗИ д.т.н., профессор 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 28.12.16 года

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

(ФИО, подпись)

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

Протокол № 4 от 28.12.16 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: _____