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

Защищенные информационные системы

Направление подготовки 10.04.01 Информационная безопасность

Программа подготовки _____

Уровень высшего образования магистратура

Форма обучения очная

Семестр	Трудоем-кость зач. ед./час.	Лек-ций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
2	2/72	18		36	18	Зачет
3	5/180	18		36	90	Экзамен (36ч), КР
Итого	7/252	36		72	108	Зачет, экзамен (36ч), КР

ВЛАДИМИР 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защищенные информационные системы» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность».. Целью освоения дисциплины является ознакомление магистров с современным теоретическим аппаратом информационной безопасности, представление сведений о базовых моделях и алгоритмах, используемых в управлении информационной безопасностью в информационных системах, а также о процессе теоретико-методологического анализа различных механизмов и сервисов защиты информации. Задачей изучения дисциплины «Защищенные информационные системы» является изучение аппарата управления информационной безопасностью в информационных системах, освоение методов анализа программно-технических сервисов информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО МАГИСТРАТУРЫ

Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.1). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

Дисциплина изучается на 1 и 2 курсах, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.04.01 по курсам «Теоретические основы компьютерной безопасности», «Информационно-аналитические системы безопасности», «Технологии обеспечения информационной безопасности». Кроме того, требования к «входным» знаниям, умениям и готовностям обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Защита информации в корпоративных информационных системах» или аналогичных, в соответствии с программой подготовки бакалавров в следующих или смежных областях знаний: -информационная безопасность; -энергетика, энергетическое машиностроение и электротехника; -авиационная и ракетно-космическая техника; -фотоника, приборостроение, -оптические и биотехнические системы и технологии; -электронная техника, радиотехника и связь; -автоматика и управление; -информатика и вычислительная техника; -физико-технические науки и технологии; -управление в технических системах.

Курс тесно взаимосвязан с другими дисциплинами. Он может быть полезен для изучения таких дисциплин как «Управление информационной безопасностью», «Информационно-аналитические системы безопасности», «Методы и средства защиты информации в системах электронного документооборота» и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование следующих профессиональных компетенций, которыми должен обладать выпускник:

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

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

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

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

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

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

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

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

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

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

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 7 зачетных единиц, 252 часа.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1.	Информационные технологии и информационные системы. Примеры информационных технологий и информационных систем	2	1-2	2		4		2		2/33%	
2.	Проектирование и разработка защищенных информационных технологий	2	3-4	2		4		2		2/33%	
3.	Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	2	5-6	2		4		2		4/66%	Рейтинг-контроль №1
4.	Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	2	7-8	2		4		2		2/33%	
5.	Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.	2	9-10	2		4		2		4/66%	
6.	Классы в системе общих критериев. Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.	2	11-12	2		4		2		2/33%	Рейтинг-контроль №2
7.	Гарантии безопасности компьютерных систем в системе общих критериев. Понятие гарантии безопасности. Уровни гарантий.	2	13-14	2		4		2		2/33%	

№ 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		
8.	Каналы утечки и их анализ в системе общих критериев. Виды каналов утечки информации.	2	15-16	2		4		2		2/33%	
9.	Безопасное функционирование в системе общих критериев. Управление конфигурацией.	2	17-18	2		4		2		2/33%	Рейтинг-контроль №3
Всего				18		36		18		22 (41%)	Зачет
10	Основные угрозы безопасности информации в компьютерных системах.	3	1-2	2		4		10		2/33%	
11	Модель угроз. Анализ критичных технологий. Требования, предъявляемые к разработке модели угроз.	3	3-4	2		4		10		4/66%	
12	Государственная политика в области безопасности компьютерных систем. Система лицензирования и сертификации средств защиты.	3	5-6	2		4		10		2/33%	Рейтинг-контроль №1
13	Разработка политик безопасности для защищенных компьютерных систем. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.	3	7-8	2		4		10		2/33%	
14	Порядок аттестации защищенных компьютерных систем. Понятие аттестации защищенных компьютерных систем.	3	9-10	2		4		10		4/66%	

№ 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		
15	Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.	3	11-12	2		4		10		2/33%	Рейтинг-контроль №2
16	Порядок внедрения SLM-системы. Service Desk — цели, возможности, реализации. Microsoft Operations Framework (MOF).		13-14	2		4		10		4/66%	
17	Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС, техническое задание, эскизный проект, технический проект, рабочая документация	3	15-16	2		4		10		2/33%	
18	Методы и методики оценки качества ЗИС. Требования к эксплуатационной документации ЗИС. Порядок приемки защищенных ЗИС	3	17-18	2		4		10		4/66%	Рейтинг-контроль №3
Всего				18		36		90	КР	26 (48%)	Экзамен
Итого				36		72		108		48/44%	Зачет, экзамен, КР

Содержание дисциплины

Раздел 1. Информационные технологии и информационные системы. Примеры информационных технологий и информационных систем. Типы компьютерных систем, как элементов информационных технологий. Основные принципы успешного функционирования информационной (компьютерной) системы. Цель принимаемых руководством предприятия и должност-ными лицами мер по поддержке информационных технологий принятия решений. Основные принципы и методы защиты информационных процессов в компьютерных системах.

Раздел 2. Проектирование и разработка защищенных информационных технологий. Понятие защищенной информационной технологии. Основные подходы, используемые при проектировании защищенных информационных технологий. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении. Государственные стандарты на разработку и создание информационных систем в защищенном исполнении. CASE-технологии создания информационных систем. Стандарт ITIL.

Раздел 3. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга». Американский стандарт по защите информации «Оранжевая книга». Понятие гарантии защиты. Критерии оценки защищенности баз данных. Содержание классов защищенности. Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.

Раздел 4. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC. Европейский стандарт по защите информации ITSEC. Понятие гарантии защиты в соответствии с европейским стандартом. Критерии оценки защищенности. Содержание классов защищенности. Функциональные требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения защищенных информационных систем.

Раздел 5. Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты. Функции поддержки политики безопасности. Гарантии безопасности. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности. Содержание политики безопасности.

Раздел 6. Классы в системе общих критериев. Классы защищенности в системе общих критериев. Понятие аудита политики безопасности. Требования к подсистемам аудита. Подсистемы подтверждения подлинности отправки и получения сообщения. Подсистемы разграничения доступа. Подсистемы идентификации и аутентификации. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы. Подсистемы защиты связи. Требования к подсистемам, предъявляемые в каждом классе защищенности.

Раздел 7. Гарантии безопасности компьютерных систем в системе общих критериев. Понятие гарантии безопасности. Уровни гарантий. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.

Раздел 8. Каналы утечки и их анализ в системе общих критериев. Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности. Методология анализа каналов утечки информации.

Раздел 9. Безопасное функционирование в системе общих критериев. Управление конфигурацией. Безопасная установка систем защиты информационных технологий. Безопасная модернизация информационных технологий.

Раздел 10. Основные угрозы безопасности информации в компьютерных системах. Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах. Специфика возникновения угроз в открытых сетях. Особенности защиты информации на узлах компьютерной сети. Системные вопросы защиты программ и данных. Анализ рисков. Модель противника, возможности противника. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.

Раздел 11. Модель угроз. Анализ критичных технологий. Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации.

Раздел 12. Государственная политика в области безопасности компьютерных систем. Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты. Нормативная база и ответственность за защиту информации в компьютерных системах. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа

Раздел 13. Разработка политик безопасности для защищенных компьютерных систем. Требования, предъявляемые к разработке политик безопасности. Дискреционная и много-

уровневая политика безопасности. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.

Раздел 14. Порядок аттестации защищенных компьютерных систем. Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

Раздел 15. Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами. Современная структура ITIL. Преимущества внедрения ITSM. Бизнес-ориентированное управление ИТ на современном предприятии.

Раздел 16. Порядок внедрения SLM-системы. Service Desk — цели, возможности, реализации. Microsoft Operations Framework (MOF).

Раздел 17. Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС, техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие, аттестация ЗИС по требованиям безопасности, сопровождение ЗИС.

Раздел 18. Методы и методики оценки качества ЗИС. Требования к эксплуатационной документации ЗИС. Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД. Особенности эксплуатации ЗИС на объекте защиты.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины «Защищенные информационные системы» предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления магистра в области информационной безопасности.

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

разбор конкретных ситуаций;

учебную дискуссию;

электронные средства обучения (слайд-лекции).

Лекционные занятия проводятся в аудитории, оборудованной проектором, что позволяет сочетать активные и интерактивные формы проведения занятий.

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

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования по направлению подготовки 10.04.01 «Информационная безопасность» не могут составлять более 45 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

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

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

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

Примерный перечень заданий для текущих контрольных мероприятий:

Второй семестр

Вопросы рейтинг-контроля №1 Второй семестр

- Типы компьютерных систем, как элементов информационных технологий.
- Основные принципы успешного функционирования информационной (компьютерной) системы.
- Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.

- Основные принципы и методы защиты информационных процессов в компьютерных системах.
- Понятие защищенной информационной технологии.
- Основные подходы, используемые при проектировании защищенных информационных технологий.
- Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.
- Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.
- CASE-технологии создания информационных систем.
- Стандарт ITIL.
- Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
- Американский стандарт по защите информации «Оранжевая книга».
- Понятие гарантии защиты.
- Критерии оценки защищенности баз данных.
- Содержание классов защищенности.

Вопросы рейтинг-контроля №2 Второй семестр

- Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.
- Вопросы гарантий и эффективности в европейском стандарте ITSEC.
- Европейский стандарт по защите информации ITSEC.
- Понятие гарантии защиты в соответствии с европейским стандартом ITSEC.
- Критерии оценки защищенности в соответствии с европейским стандартом ITSEC. Содержание классов защищенности в соответствии с европейским стандартом ITSEC.
- Функциональные требования по защите информации, предъявляемые в каждом классе защищенности в соответствии с европейским стандартом ITSEC.
- Принципы и методы построения защищенных информационных систем.
- Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.
- Функции поддержки политики безопасности. Гарантии безопасности.
- Требования по безопасности информационных технологий. Классы защищенности.
- Компоненты подсистем поддержки политики безопасности.
- Содержание типовой политики безопасности.
- Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.
- Требования к подсистемам аудита.
- Подсистемы подтверждения подлинности отправки и получения сообщения.

Вопросы рейтинг-контроля №3 Второй семестр

- Подсистемы разграничения доступа.
- Подсистемы идентификации и аутентификации.
- Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы.
- Подсистемы защиты связи.
- Требования к подсистемам, предъявляемые в каждом классе защищенности.
- Гарантии безопасности компьютерных систем в системе общих критериев.
- Понятие гарантии безопасности. Уровни гарантий.
- Гарантии проектирования защищенных информационных систем.

- Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.
- Каналы утечки и их анализ в системе общих критериев.
- Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности.
- Методология анализа каналов утечки информации.
- Безопасное функционирование в системе общих критериев.
- Управление конфигурацией. Безопасная установка систем защиты информационных технологий.
- Безопасная модернизация информационных технологий.

Перечень вопросов к зачету 2 семестр (промежуточной аттестации по итогам освоения дисциплины):

1. Типы компьютерных систем, как элементов информационных технологий.
2. Основные принципы успешного функционирования информационной (компьютерной) системы.
3. Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.
4. Основные принципы и методы защиты информационных процессов в компьютерных системах.
5. Понятие защищенной информационной технологии.
6. Основные подходы, используемые при проектировании защищенных информационных технологий.
7. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.
8. Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.
9. CASE-технологии создания информационных систем.
10. Стандарт ITIL.
11. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
12. Американский стандарт по защите информации «Оранжевая книга».
13. Понятие гарантии защиты.
14. Критерии оценки защищенности баз данных.
15. Содержание классов защищенности.
16. Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.
17. Вопросы гарантий и эффективности в европейском стандарте ITSEC.
18. Европейский стандарт по защите информации ITSEC.
19. Понятие гарантии защиты в соответствии с европейским стандартом ITSEC.
20. Критерии оценки защищенности в соответствии с европейским стандартом ITSEC. Содержание классов защищенности в соответствии с европейским стандартом ITSEC.
21. Функциональные требования по защите информации, предъявляемые в каждом классе защищенности в соответствии с европейским стандартом ITSEC.
22. Принципы и методы построения защищенных информационных систем.
23. Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.
24. Функции поддержки политики безопасности. Гарантии безопасности.
25. Требования по безопасности информационных технологий. Классы защищенности.
26. Компоненты подсистем поддержки политики безопасности.
27. Содержание типовой политики безопасности.

28. Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.
29. Требования к подсистемам аудита.
30. Подсистемы подтверждения подлинности отправки и получения сообщения.
31. Подсистемы разграничения доступа.
32. Подсистемы идентификации и аутентификации.
33. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы.
34. Подсистемы защиты связи.
35. Требования к подсистемам, предъявляемые в каждом классе защищенности.
36. Гарантии безопасности компьютерных систем в системе общих критериев.
37. Понятие гарантии безопасности. Уровни гарантий.
38. Гарантии проектирования защищенных информационных систем.
39. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.
40. Каналы утечки и их анализ в системе общих критериев.
41. Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности.
42. Методология анализа каналов утечки информации.
43. Безопасное функционирование в системе общих критериев.
44. Управление конфигурацией. Безопасная установка систем защиты информационных технологий.
45. Безопасная модернизация информационных технологий.

Вопросы рейтинг-контроля №1 Третий семестр

- Ценности, опасности, потери, риски, угрозы в компьютерных системах.
- Основные угрозы информации в компьютерных системах.
- Специфика возникновения угроз в открытых сетях.
- Особенности защиты информации на узлах компьютерной сети.
- Системные вопросы защиты программ и данных.
- Анализ рисков. Модель противника, возможности противника.
- Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
- Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
- Требования к защите автоматизированных систем от НСД.
- Модель угроз. Анализ критичных технологий.
- Требования, предъявляемые к разработке модели угроз.
- Структура модели угроз безопасности информации.
- Анализ критичных технологий обработки информации.
- Система лицензирования и сертификации средств защиты.

Вопросы рейтинг-контроля №2 Третий семестр

- Система лицензирования и сертификации средств защиты.
- Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
- Нормативная база и ответственность за защиту информации в компьютерных системах.
- Основные руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа.
- Разработка политик безопасности для защищенных компьютерных систем.
- Требования, предъявляемые к разработке политик безопасности.

- Дискреционная и многоуровневая политика безопасности.
- Политика мандатного доступа.
- Политика защиты целостности информационных ресурсов.
- Понятие аттестации защищенных компьютерных систем.
- Руководящие документы ФСТЭК России по аттестации.
- Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
- Содержание этапов аттестационных испытаний.
- Контроль эффективности защитных мероприятий в системе аттестации.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.

Вопросы рейтинг-контроля №3 Третий семестр

- Руководящие документы ФСТЭК России по аттестации.
- Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
- Содержание этапов аттестационных испытаний.
- Контроль эффективности защитных мероприятий в системе аттестации.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.
- Современная структура ITIL.
- Преимущества внедрения ITSM.
- Бизнес-ориентированное управление ИТ на современном предприятии.
- Порядок внедрения SLM-системы.
- Service Desk — цели, возможности, реализации.
- Microsoft Operations Framework (MOF).
- Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС. Техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие.
- Сопровождение ЗИС.
- Методы и методики оценки качества ЗИС.
- Требования к эксплуатационной документации ЗИС.
- Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД.
- Особенности эксплуатации ЗИС на объекте защиты.

Перечень вопросов к экзамену 3 семестр (промежуточной аттестации по итогам освоения дисциплины):

- Ценности, опасности, потери, риски, угрозы в компьютерных системах.
- Основные угрозы информации в компьютерных системах.
- Специфика возникновения угроз в открытых сетях.
- Особенности защиты информации на узлах компьютерной сети.
- Системные вопросы защиты программ и данных.
- Анализ рисков. Модель противника, возможности противника.
- Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
- Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.
- Требования к защите автоматизированных систем от НСД.
- Модель угроз. Анализ критичных технологий.
- Требования, предъявляемые к разработке модели угроз.

- Структура модели угроз безопасности информации.
- Анализ критичных технологий обработки информации.
- Система лицензирования и сертификации средств защиты.
- Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
- Нормативная база и ответственность за защиту информации в компьютерных системах.
- Основные руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа.
- Разработка политик безопасности для защищенных компьютерных систем.
- Требования, предъявляемые к разработке политик безопасности.
- Дискреционная и многоуровневая политика безопасности.
- Политика мандатного доступа.
- Политика защиты целостности информационных ресурсов.
- Понятие аттестации защищенных компьютерных систем.
- Руководящие документы ФСТЭК России по аттестации.
- Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
- Содержание этапов аттестационных испытаний.
- Контроль эффективности защитных мероприятий в системе аттестации.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.
- Современная структура ITIL.
- Преимущества внедрения ITSM.
- Бизнес-ориентированное управление ИТ на современном предприятии.
- Порядок внедрения SLM-системы.
- Service Desk — цели, возможности, реализации.
- Microsoft Operations Framework (MOF).
- Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС. Техническое задание, эскизный проект, технический проект, рабочая документация, ввод в действие.
- Сопровождение ЗИС.
- Методы и методики оценки качества ЗИС.
- Требования к эксплуатационной документации ЗИС.
- Порядок приемки защищенных ЗИС, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД.
- Особенности эксплуатации ЗИС на объекте защиты.

Темы лабораторных работ 2 семестр:

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

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

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

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

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

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

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

Темы лабораторных работ 3 семестр:

Лабораторная работа № 1. Обнаружение узлов корпоративной СЕТИ. ICMP ECHO REQUEST (Утилиты FPING и NMAP)

Лабораторная работа № 2. Обнаружение узлов корпоративной сети. Информационные ICMP сообщения

Лабораторная работа № 3. Обнаружение узлов корпоративной сети средствами протокола TCP (TCP-PING)

Лабораторная работа № 4. Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP-PING), IP

Лабораторная работа № 5. Обнаружение узлов корпоративной сети средствами протокола ARP (ARP-PING)

Лабораторная работа № 6. Основные средства определения маршрутов IP-пакетов - PING, TRACEROUTE

Лабораторная работа № 7. Дополнительные средства определения маршрутов IP-ПАКЕТОВ - NMAP, TRACEMAP, MRT

Лабораторная работа № 8. Идентификация статуса TCP-портов (TCP-CONNECT. SYN-SCAN)

Лабораторная работа № 9. Методы скрытого сканирования (STEALTH TCP SCANNING METHODS)

Лабораторная работа № 10. Идентификация прикладных сетевых служб методом анализа особенностей реализации (SMTP)

Вопросы и задания к самостоятельной работе магистрантов 2 семестр

- ITIL – Компонент «Поддержка услуг».
- ITIL – Компонент «Предоставление услуг».
- ITIL — основа концепции управления ИТ-службами.
- Service Desk — цели, возможности, реализации.
- Аудит инфраструктуры РИС/КАС.
- Аутсорсинг.

Вопросы и задания к самостоятельной работе магистрантов 3 семестр

- Методология Penetration Testing. Open Source Security Testing Methodology Manual (OSSTMM).
- Методология Penetration Testing. Information Systems Security Assessment Framework (ISSAF).
- Методология Penetration Testing. Open Web Application Security Project (OWASP).
- Методология Penetration Testing. Web Application Security Consortium Threat Classification (WASC-TC).
- Стандарт Penetration Testing. Penetration Testing Execution Standard (PTES).
- Footprinting. Цели, задачи Footprinting. Этапы Footprinting и Reconnaissance.
- Footprinting. Открытые источники и пассивный сбор информации.
- Footprinting. Активный сбор информации.
- Footprinting. Программные инструменты Footprinting и Reconnaissance.
- Сканирование сети. Обнаружение узлов сети. Методы и программные средства.
- Сканирование сети. Обнаружение открытых портов узла сети. Методы и программные средства.
- Сканирование сети. Типы сканирования (Full Open Scan, Half-open Scan, Xmas Tree Scan). Особенности использования рассматриваемых типов сканирования.

- Сканирование сети. Типы сканирования (FIN Scan, NULL Scan, ACK Scanning). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (UDP Scanning, ARP Scan). Особенности использования рассматриваемых типов сканирования.
- Services fingerprinting. Методы Services fingerprinting.
- Services fingerprinting. Программные инструменты Services fingerprinting.
- OS Fingerprinting. Методы OS Fingerprinting. Banner Grabbing.
- OS Fingerprinting. Методы OS Fingerprinting. Пассивное исследование стека в задаче идентификации ОС.
- OS Fingerprinting. Методы OS Fingerprinting. Активное исследование стека в задаче идентификации ОС.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация ресурсов OS Windows. Методы и средства.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация ресурсов OS Linux/Unix. Методы и средства.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация посредством SNMP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация LDAP.
- Enumeration. Понятие, цели и задачи Enumeration. Инвентаризация SMTP.
- Sniffing. Цели и задачи анализа трафика. Программные инструменты анализа трафика.
- Sniffing атаки в коммутируемой сетевой среде. MAC Flooding. ARP Poisoning.
- Sniffing атаки в коммутируемой сетевой среде. MAC Spoofing.
- Sniffing атаки в коммутируемой сетевой среде. Методы и средства защиты от Sniffing атак.
- Атаки DOS. Цели и задачи атак DOS. Типы атак DOS.
- Атаки DOS. Service Request Floods. SYN Attack/Flood. ICMP Flood Attack. Программные средства проведения атак.
- Атаки DOS. Ping of Death. Teardrop. Smurf. Fraggle. Программные средства проведения атак.
- Атаки Buffer Overflow. Принципы.
- Атаки DDOS. Особенности реализации.
- Беспроводные сети. Угрозы и уязвимости Wireless Networks.
- Беспроводные сети. Аутентификация Wi-fi.
- Беспроводные сети. Атаки деаутентификации (Deauthentication Attack).
- Сканеры уязвимостей. Идентификация уязвимостей в сетях.
- Сканеры уязвимостей. Уязвимости БД.
- Средства анализа защищенности БД.
- Сканеры уязвимостей. Уязвимости WEB приложений.
- Средства анализа защищенности WEB приложений.

Примерные темы заданий к курсовой работе 3 семестр

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

9. Разработка защищенной АС структурного подразделения на современном предприятии (по выбору).
10. Разработка проекта защищенной распределенной АС подразделения на территориально-распределенном предприятии (по выбору).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Архитектура корпоративных информационных систем/АстапчукВ.А., ТерещенкоП.В. - Новосиб.: НГТУ, 2015. - 75 с.: ISBN 978-5-7782-2698-2 Режим доступа: http://znanium.com/catalog.php?bookinfo=546624
2. Информационные системы: Учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. - 2-е изд. - М.: Форум: НИЦ ИНФРА-М, 2014. - 448 с.: ISBN 978-5-91134-833-5 Режим доступа: http://znanium.com/catalog.php?bookinfo=435900
3. Информационные системы и модели. Элективный курс / Семакин И.Г. - М. : БИНОМ, 2012. http://www.studentlibrary.ru/ book/ISBN9785996309221.html
4. Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - http://www.studentlibrary.ru/book/ISBN9785991202756.html
5. Проектирование информационных систем: Учебное пособие / В.В. Коваленко. - М.: Форум: НИЦ ИНФРА-М, 2014. - 320 с.: ISBN 978-5-91134-549-5. Режим доступа: http://znanium.com/catalog.php?bookinfo=473097

б) Дополнительная литература:

1. Информационные системы: учебник для студ. учреждений высш. образования / С.А. Жданов, М.Л. Соболева, А.С. Алфимова - М. : Прометей, 2015. http://www.studentlibrary.ru/book/ISBN9785990626447.html
2. Информационные технологии: Учебное пособие / Л.Г. Гагарина, Я.О. Теплова, Е.Л. Румянцева и др.; Под ред. Л.Г. Гагариной - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. - 320 с.: ISBN 978-5-8199-0608-8. Режим доступа: http://znanium.com/catalog.php?bookinfo=471464
3. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. ISBN 978-5-8199-0411-4 Режим доступа: http://znanium.com/catalog.php?bookinfo=402686
4. Интеллектуальные системы защиты информации : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html 172 с.

в) Периодические издания:

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
3. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.
4. «Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;
5. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
3. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

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

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

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

Рабочую программу составил зав. кафедрой ИЗИ д.т.н. Монахов М.Ю.

(ФИО, подпись)

Рецензент
(представитель работодателя) к.т.н. Курысев Константин Николаевич ВРИО заместителя начальника Владимирского юридического института ФСИН России по учебной работе

(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 4 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: _____