УП2013

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

ТЕОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ

(наименование дисциплины)

Направление подготовки 10.03.01 Информационная безопасность

Профиль / программа подготовки Комплексная защита объектов информатизации

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
5	4/144	36	36		36	Экзамен (36ч)
Итого	4/144	36	36		36	Экзамен (36ч)

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Теория защиты информации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность», ознакомление студентов с вопросами сущности и значения информационной безопасности и защиты информации, определение теоретических, концептуальных, методологических и организационных основ обеспечения информационной безопасности в компьютерных системах. Изучение основных моделей каналов утечки в компьютерных системах и моделей управления доступом в компьютерных системах.

Задачами освоения дисциплины «Теория защиты информации» является изучение следующих вопросов и тем:

- ознакомление с понятийным аппаратом в области информационной безопасности и защиты информации;

- ознакомление с формальными моделями контроля доступа, решеткой уровней конфиденциальности, автоматной моделью контроля доступа;

- изучение угроз конфиденциальности, целостности и доступности в терминах управления доступом, базовой теоремы безопасности и основных моделей каналов утечки в компьютерных системах;

- изучение дискреционной, мандатной и ролевой модели управления доступом, а также особенностей имплементации управления доступом в современных информационных системах - ОС, СУБД и др;

- ознакомление с моделью безопасности информационных потоков, автоматной и программной моделью контроля информационных потоков;

- ознакомление с субъектно-ориентированной моделью безопасности программной среды, понятиями монитора безопасности объектов, монитора безопасности субъектов;

-изучение применения моделей безопасности при построении информационных систем в защищенном исполнении. Гомоморфизм компьютерной системы и ее математической модели безопасности;

изучение вопросов реализации дискреционной политики в операционных системах Windows и GNU/Linux. Изучение реализации дискреционного управления доступом и мандатного управления доступом в СЗИ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО БАКАЛАВРИАТА

Данная дисциплина относится к базовой части Блока Б1 (Б1.Б.21). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий.

Дисциплина изучается на 3 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.03.01 «Информационная безопасность» по курсам «Информатика», «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Структуры данных», «Технологии и методы программирования». Курс тесно взаимосвязан с другими дисциплинами. Он является базовым для изучения таких дисциплин как «Защита информации в корпоративных ИС», «Программно-аппаратные средства защиты информации», «Базы данных», «Система защиты информации на предприятии», «Корпоративные информационные системы» и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр 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;

профессиональными компетенциями:

ОПК-7 – способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **Знать:** - основные виды политик управления доступом и информационными потоками в компьютерных системах; - защитные механизмы и средства обеспечения безопасности операционных систем; - средства и методы хранения и передачи аутентификационной информации (ОК-5; ОПК-7);

2) **Уметь:** - применять основные виды политик управления доступом и информационными потоками в компьютерных системах; - основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; - формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе (ОК-5; ОПК-7);

3) **Владеть:** - разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; - навыками конфигурирования и администрирования операционных систем (ОК-5; ОПК-7).

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

- способность применять навыки реализации дискреционной политики безопасности в операционных системах Windows и GNU/Linux.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1.	Введение. Основные понятия и определения, в построении формальных моделей контроля доступа	5	1	2	2			2		2/50%	
2.	Понятие об угрозах конфиденциальности, целостности и доступности в терминах управления доступом. Базовая теорема безопасности	5	2	2	2			2		1/25%	
3.	Дискреционное, мандатное и ролевое управление доступом. Ключевые особенности, специфика реализации	5	3	2	2			2		2/50%	
4.	Модель Харрисона-Руззо-Ульмана. Элементарные операторы модели. Принцип построения команд в модели ХРУ.	5	4	2	2			2		1/25%	
5.	Модель матрицы доступов. Монотонная ТМД и ее каноническая форма. Способы формирования команд в модели ТМД.	5	5	2	2			2		1/25%	
6.	Классическая модель take-grant. Де-юре правила модели. Понятие о tg-связном подграфе, теорема о пролиферации права внутри tg-связного подграфа.	5	6	2	2			2		2/50%	Рейтинг-контроль №1
7.	Расширенная модель take-grant. Де-факто правила расширенной модели.	5	7	2	2			2		1/25%	
8.	Модель мандатного управления доступом Белла-ЛаПадулы. Правила NRU и NWD. Политика low-watermark в модели	5	8	2	2			2		1/25%	

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
9.	Модель мандатного управления целостностью Биба. Угрозы целостности, решетка уровней целостности. Правила NRD и NWU.	5	9	2	2			2		1/25%	
10.	Модель системы военных сообщений (СВС). Общие положения. Терминалы и устройства доступа в модели СВС.	5	10	2	2			2		2/50%	
11.	Модели безопасности информационных потоков. Автоматная и программная модели контроля информационных потоков.	5	11	2	2			2		1/25%	
12.	Вероятностная модель контроля информационных потоков. Схема компьютерной системы в рамках понятийного аппарата этой модели.	5	12	2	2			2		1/25%	Рейтинг-контроль №2
13.	Понятие ролевого разграничения доступа. Ролевые модели доступа в СУБД.	5	13	2	2			2		1/25%	
14.	Основные положения модели администрирования РРД. Администрирование множеств авторизованных ролей пользователей.	5	14	2	2			2		2/50%	
15.	Модель мандатного РРД. Управление правами ролей в случае наличия решетки конфиденциальности. Связь между дискреционным и мандатным РРД.	5	15	2	2			2		2/50%	

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
16.	Субъектно-ориентированная модель безопасности программной среды. Изолированная программная среда.	5	16	2	2			2		2/50%	
17.	Проблемы применения моделей безопасности при построении информационных систем в защищенном исполнении. Проблема адекватности модели безопасности реальной компьютерной системе.	5	17	2	2			2		2/50%	
18.	Реализация дискреционной политики в операционных системах Windows и GNU/Linux. Реализация дискреционного управления доступом в СЗИ.	5	18	2	2			2		2/50%	Рейтинг-контроль №3
Всего				36	36			36		27/38%	Экзамен

Содержание дисциплины «Теория защиты информации»

Раздел 1. Введение. Основные понятия и определения, использующиеся в построении формальных моделей контроля доступа. Решетка уровней конфиденциальности. Автоматная модель контроля доступа

Раздел 2. Понятие об угрозах конфиденциальности, целостности и доступности в терминах управления доступом. Базовая теорема безопасности. Основные модели каналов утечки в компьютерных системах.

Раздел 3. Дискреционное, мандатное и ролевое управление доступом. Ключевые особенности, специфика реализации. Особенности имплементации управления доступом в современных информационных системах - ОС, СУБД и др.

Раздел 4. Модель Харрисона-Руззо-Ульмана. Элементарные операторы модели. Принцип построения команд в модели ХРУ. Монооперационные системы ХРУ. Вычислительная сложность верификации системы по этой модели.

Раздел 5. Модель типизированной матрицы доступов. Монотонная ТМД и ее каноническая форма. Способы формирования команд в модели ТМД. Граф порождения типов, ациклические ТМД. Алгоритм верификации ациклических моделей ТМД.

Раздел 6. Классическая модель take-grant. Де-юре правила модели. Понятие о tg-связном подграфе, теорема о пролиферации права внутри tg-связного подграфа. Понятие о мосте, распространение права по мостам. Верификация в классической модели take-grant.

Раздел 7. Расширенная модель take-grant. Де-факто правила расширенной модели. Верификация в расширенной модели. Представление систем Take-Grant системами ХРУ.
Раздел 8. Модель мандатного управления доступом Белла-ЛаПадулы. Правила NRU и NWD. Политика low-watermark в модели. Безопасность доступов, состояний и переходов. Базовая теорема безопасности для модели Белла-ЛаПадулы.
Раздел 9. Модель мандатного управления целостностью Биба. Угрозы целостности, решетка уровней целостности. Правила NRD и NWU. Политика high-watermark.
Раздел 10. Модель системы военных сообщений (СВС). Общие положения. Терминалы и устройства доступа в модели СВС. Неформальное и формальное описание функционирования модели. Элементы ролевого разграничения доступа в модели СВС.
Раздел 11. Модели безопасности информационных потоков. Автоматная и программная модели контроля информационных потоков. Функционирование контролирующего механизма защиты.
Раздел 12. Вероятностная модель контроля информационных потоков. Схема компьютерной системы в рамках понятийного аппарата этой модели. Понятия о информационной невыводимости и информационном невлиянии.
Раздел 13. Понятие ролевого разграничения доступа. Ролевые модели доступа в СУБД. Элементы объектно-ориентированного подхода при проектировании ролевых систем разграничения доступа. Базовая модель ролевого разграничения доступа (РРД).
Раздел 14. Основные положения модели администрирования РРД. Администрирование множеств авторизованных ролей пользователей. Администрирование прав доступа, которыми обладают роли. Администрирование иерархии ролей.
Раздел 15. Модель мандатного РРД. Управление правами ролей в случае наличия решетки конфиденциальности. Связь между дискреционным и мандатным РРД. Защита от угроз конфиденциальности и целостности информации в рамках мандатного РРД.
Раздел 16. Субъектно-ориентированная модель безопасности программной среды. Изолированная программная среда. Монитор безопасности объектов, монитор безопасности субъектов.
Раздел 17. Проблемы применения моделей безопасности при построении информационных систем в защищенном исполнении. Проблема адекватности модели безопасности реальной компьютерной системе. Гомоморфизм компьютерной системы и ее математической модели безопасности.
Раздел 18. Реализация дискреционной политики в операционных системах Windows и GNU/Linux. Реализация дискреционного управления доступом в СЗИ. Реализация мандатного управления доступом в СЗИ.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления бакалавра по направлению «Информационная безопасность».

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

разбор конкретных ситуаций;

учебную дискуссию;

электронные средства обучения (слайд-лекции).

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

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

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП бакалавриата по направлению 10.03.01, 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 45 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

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

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

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

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1

1. Понятия субъекта доступа, объекта доступа, права.
2. Решетка уровней конфиденциальности.
3. Автоматная модель контроля доступа
4. Понятие об угрозах конфиденциальности, целостности и доступности в терминах управления доступом.
5. Базовая теорема безопасности.
6. Канал утечки по памяти
7. Канал утечки по времени
8. Дискреционное, мандатное и ролевое управление доступом.
9. Ключевые особенности дискреционного управления доступом, специфика реализации.

10. Особенности имплементации управления доступом в современных информационных системах - ОС, СУБД и др.

Вопросы рейтинг-контроля №2

1. Модель Харрисона-Руззо-Ульмана.
2. Элементарные операторы модели ХРУ.
3. Модель типизированной матрицы доступов.
4. Монотонная ТМД и ее каноническая форма.
5. Модель мандатного управления доступом Белла-ЛаПадулы.
6. Базовая теорема безопасности для модели Белла-ЛаПадулы.
7. Модель мандатного управления целостностью Биба.
8. Правила NRD и NWU. Политика high-watermark.
9. Модель системы военных сообщений (СВС). Общие положения.
10. Элементы ролевого разграничения доступа в модели СВС.

Вопросы рейтинг-контроля №3

1. Модели безопасности информационных потоков.
2. Вероятностная модель контроля информационных потоков.
3. Понятия о информационной невыводимости и информационном невлиянии.
4. Базовая модель ролевого разграничения доступа (РРД).
5. Основные положения модели администрирования РРД.
6. Модель мандатного РРД.
7. Субъектно-ориентированная модель безопасности программной среды.
8. Проблемы применения моделей безопасности при построении информационных систем в защищенном исполнении.
9. Реализация дискреционной политики в операционных системах Windows и GNU/Linux. Реализация дискреционного управления доступом в СЗИ.
10. Реализация мандатного управления доступом в СЗИ.

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

- Основные понятия и определения, использующиеся в построении формальных моделей контроля доступа.
- Решетка уровней конфиденциальности.
- Автоматная модель контроля доступа
- Понятие об угрозах конфиденциальности, целостности и доступности в терминах управления доступом.
- Базовая теорема безопасности.
- Основные модели каналов утечки в компьютерных системах.
- Дискреционное, мандатное и ролевое управление доступом.
- Ключевые особенности, специфика реализации систем разграничения доступа.
- Особенности имплементации управления доступом в современных информационных системах - ОС, СУБД и др.
- Модель Харрисона-Руззо-Ульмана.
- Элементарные операторы модели ХРУ.
- Принцип построения команд в модели ХРУ.
- Монооперационные системы ХРУ.
- Вычислительная сложность верификации системы по модели ХРУ.
- Модель типизированной матрицы доступов.
- Монотонная ТМД и ее каноническая форма.
- Способы формирования команд в модели ТМД.
- Граф порождения типов, ациклические ТМД.
- Алгоритм верификации ациклических моделей ТМД.

- Классическая модель take-grant.
- Де-юре правила модели take-grant.
- Понятие о tg-связном подграфе, теорема о пролиферации права внутри tg-связного подграфа.
- Понятие о мосте, распространение права по мостам.
- Верификация в классической модели take-grant.
- Расширенная модель take-grant.
- Де-факто правила расширенной модели take-grant.
- Верификация в расширенной модели take-grant.
- Представление систем Take-Grant системами ХРУ.
- Модель мандатного управления доступом Белла-ЛаПадулы.
- Правила NRU и NWD. Политика low-watermark в модели Белла-ЛаПадулы.
- Безопасность доступов, состояний и переходов для модели Белла-ЛаПадулы.
- Базовая теорема безопасности для модели Белла-ЛаПадулы.
- Модель мандатного управления целостностью Биба.
- Угрозы целостности, решетка уровней целостности.
- Правила NRD и NWU. Политика high-watermark в модели Биба.
- Модель системы военных сообщений (СВС). Общие положения.
- Терминалы и устройства доступа в модели СВС.
- Неформальное и формальное описание функционирования модели.
- Элементы ролевого разграничения доступа в модели СВС.
- Модели безопасности информационных потоков.
- Автоматная и программная модели контроля информационных потоков.
- Функционирование контролирующего механизма защиты.
- Вероятностная модель контроля информационных потоков. Схема компьютерной системы в рамках понятийного аппарата этой модели.
- Понятия о информационной невыводимости и информационном невлиянии.
- Понятие ролевого разграничения доступа. Ролевые модели доступа в СУБД.
- Элементы объектно-ориентированного подхода при проектировании ролевых систем разграничения доступа.
- Базовая модель ролевого разграничения доступа (РРД).
- Основные положения модели администрирования РРД.
- Администрирование множеств авторизованных ролей пользователей. Администрирование прав доступа, которыми обладают роли. Администрирование иерархии ролей.
- Модель мандатного РРД. Управление правами ролей в случае наличия решетки конфиденциальности.
- Связь между дискреционным и мандатным РРД.
- Защита от угроз конфиденциальности и целостности информации в рамках мандатного РРД.
- Субъектно-ориентированная модель безопасности программной среды.
- Изолированная программная среда.
- Проблемы применения моделей безопасности при построении информационных систем в защищенном исполнении.
- Проблема адекватности модели безопасности реальной компьютерной системе.
- Гомоморфизм компьютерной системы и ее математической модели безопасности.
- Реализация дискреционной политики в операционных системах Windows и GNU/Linux.
- Реализация дискреционного управления доступом в СЗИ.
- Реализация мандатного управления доступом в СЗИ.

Вопросы и задания для самостоятельной работы студентов:

1. Ролевое разграничение доступа в СУБД Oracle
2. Ролевое разграничение доступа в СУБД MS SQL Server
3. Single Sign-on в Windows-сетях
4. Модель Кларка-Уилсона

5. Способы хранения аутентификаторов в Windows
6. Способы хранения аутентификаторов в GNU/Linux
7. Контексты безопасности SELinux
8. Способы организации сессий в Web-сервисах
9. Аутентификация в Web-сервисах

Перечень тем практических занятий:

Практическое занятие №1. Создание программного модуля дискреционного разграничения доступа к набору файлов, поддерживающего команды модели Харрисона-Руззо-Ульмана. Программный модуль должен поддерживать одновременную работу нескольких пользователей и позволять просматривать матрицу доступов на всем протяжении своего функционирования.

Практическое занятие №2. Создание программного модуля дискреционного разграничения доступа к набору файлов, поддерживающего команды модели ТМД. Программный модуль должен поддерживать одновременную работу нескольких пользователей и позволять строить граф порождения типов.

Практическое занятие №3. Создание программного модуля анализа графов доступов по расширенной модели Take-Grant. Модуль должен уметь достраивать недостающие ребра по де-юре и де-факто правилам, определять мосты и находить tg-связные подграфы. Входные и выходные данные должны быть в формате CSV.

Практическое занятие №4. Создание программного модуля мандатного разграничения доступа к набору файлов, поддерживающего команды модели Белла-ЛаПадулы. Программный модуль должен поддерживать одновременную работу нескольких пользователей и строго выполнять правила NRU и NWD, а также следовать политике low-watermark.

Практическое занятие №5. Создание программного модуля мандатного разграничения доступа к набору файлов, поддерживающего команды модели контроля целостности Биба. Программный модуль должен позволять выгружать информацию о состоянии системы в любой удобный для студента формат.

Практическое занятие №6. Создание программы, имитирующей контроль доступа с несколькими субъектами и терминалами по модели СВС. Программа должна отслеживать вес метки и контейнеры, создаваемые по ходу функционирования модели.

Практическое занятие №7. Установка и настройка демонстрационной версии операционной системы МСВС. Настройка должна включать в себя обеспечение и проверку функционирования дискреционного и мандатного управления доступом к пользовательским файлам.

Практическое занятие №8. Установка и настройка операционной системы Гослинукс. Настройка должна включать в себя обеспечение и проверку функционирования дискреционного и мандатного управления доступом к пользовательским файлам.

Практическое занятие №9. Установка и настройка демонстрационной версии средства защиты информации АУРА 1.2.4. Настройка должна включать в себя обеспечение и проверку функционирования дискреционного и мандатного управления доступом к пользовательским файлам.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6, Режим доступа: http://znanium.com/catalog.php?bookinfo=474838
2. 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
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.
4. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.

б) Дополнительная литература:

1. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. ISBN 978-5-369-01379-3 : Режим доступа: http://znanium.com/catalog.php?bookinfo=476047
2. Бизнес-безопасность / Кузнецов И.Н. - М. : Дашков и К, 2012. - http://www.studentlibrary.ru/book/ISBN9785394014383.html. 416 с.
3. Офисный шпионаж / Мелтон К., Пилиджан К., Сверчински Д. - М. : Альпина Паблишер, 2013. - http://www.studentlibrary.ru/book/ISBN9785916712070.html. 182 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/.

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.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Монахов Ю.М.
(ФИО, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»

к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 7 от 28.12.16 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

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: _____