

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета ФИТКБ
Григорьев А.В./
28.08.2025 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Модели безопасности компьютерных систем»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2025

Автор программы

 С.С. Куликов

Заведующий кафедрой

Систем информационной
безопасности

 А.Г. Остапенко

Руководитель ОПОП

 С.С. Куликов

Воронеж 2025

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Обучение принципам формального моделирования и анализа безопасности компьютерных систем, реализующих управление доступом и информационными потоками, на основании формальных моделей обеспечения безопасности компьютерных систем (моделей компьютерной безопасности).

1.2. Задачи освоения дисциплины

- 1) изучение исходных понятий и формализации в сфере компьютерной безопасности;
- 2) освоение процессов представления, анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;
- 3) обучение методологии анализа архитектурных (схемно-технических) и программно-алгоритмических решений, применяемых в системах защиты информации современных компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Модели безопасности компьютерных систем» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Модели безопасности компьютерных систем» направлен на формирование следующих компетенций:

ОПК-11 - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-11	знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем, 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
	уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	владеть средствами защиты информации, реализующими политики управления доступом

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Модели безопасности компьютерных систем» составляет 7 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		7	8
Аудиторные занятия (всего)	144	54	90
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	72	18	54
Самостоятельная работа	144	18	126
Курсовой проект	+		+
Виды промежуточной аттестации - зачет, зачет с оценкой	+	+	+
Общая трудоемкость:			
академические часы	288	72	216
зач.ед.	8	2	6

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Исходные положения теории компьютерной безопасности	История развития теории и практики обеспечения компьютерной безопасности. Содержание и структура понятия компьютерной безопасности. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Понятие угроз безопасности, их классификация и идентификация. Методы оценивания угроз. Понятие политики и моделей безопасности информации в компьютерных системах. Субъектно-объектная модель компьютерной системы в механизмах и процессах коллективного доступа к информационным ресурсам. Монитор безопасности и основные типы политик безопасности. Гарантирование	12	12	24	48

		выполнения политики безопасности.				
2	Модели безопасности на основе дискреционной политики	Общая характеристика моделей дискреционного доступа. Пятимерное пространство Хартсона. Модели на основе матрицы доступа. Модели распространения прав доступа.	12	12	24	48
3	Модели безопасности на основе мандатной политики	Общая характеристика политики мандатного доступа. Модель Белла-ЛаПадулы и ее расширения. Основные расширения модели Белла-ЛаПадулы.	12	12	24	48
4	Модели безопасности на основе тематической и ролевой политики	Общая характеристика тематического разграничения доступа. Тематические решетки. Модель тематико-иерархического разграничения доступа. Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений. Формальная спецификация и разновидности ролевых моделей. Индивидуально-групповое разграничение доступа.	12	12	24	48
5	Модели и технологии обеспечения целостности и доступности данных	Общая характеристика моделей и технологий обеспечения целостности данных. Дискреционная модель Кларка-Вильсона. Мандатная модель Кена Биба. Технологии параллельного выполнения транзакций в клиент-серверных системах (СУБД). Резервирование, архивирование и журнализация данных. Технологии репликации данных.	12	12	24	48
6	Методы анализа и оценки защищенности компьютерных систем	Задача комплексной оценки защищенности. Модель системы с полным перекрытием. Анализ технико-экономической эффективности системы защиты. Теоретико-графовая модель системы индивидуально-групповых назначений доступа к иерархически организованным объектам. Пространственно-векторная модель и характеристики системы рабочих групп пользователей.	12	12	24	48
Итого			72	72	144	288

5.2 Перечень лабораторных работ

- 1) Функциональные требования Secret Net 7
- 2) Механизмы защиты Secret Net 7
- 3) Принципы построения системы Secret Net Studio и способы ее развертывания
- 4) Настройка и применение компонентов базовой защиты Secret Net 7
- 5) Настройка и применение компонентов локальной защиты Secret Net 7
- 6) Персональный межсетевой экран
- 7) Защита от вирусов и вредоносного ПО
- 8) Организация защиты средствами Secret Net 7
- 9) Дополнительные средства администрирования Secret Net 7. Вспомогательные утилиты и файлы настроек
- 10) Часто встречающиеся проблемы. Диагностика и решения

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 9 семестре для очной

формы обучения.

Примерная тематика курсового проекта: «Разработка модели и программного обеспечения, реализующих политику разграничения доступа в операционной системе»

Задачи, решаемые при выполнении курсового проекта:

- Определение параметров субъектно-объектной модели разграничения доступа.
- Разработка политики разграничения доступа субъектов к объектам в операционной системе.
- Разработка модели разграничения доступа субъектов к объектам в операционной системе в соответствии с политикой разграничения доступа.
- Разработка программного обеспечения, реализующего модель разграничения доступа.

Курсовой проект включают в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-11	знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем, основные виды политик	Обучающийся знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем, основные виды политик управления доступом и информационными	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренных в рабочих программах

	управления доступом и информационными потоками в компьютерных системах, основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков	потоками в компьютерных системах, основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков		
	уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Обучающийся умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренных в рабочих программах
	владеть средствами защиты информации, реализующими политики управления доступом	Обучающийся владеет средствами защиты информации, реализующими политики управления доступом	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренных в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8, 9 семестре для очной формы обучения по двух/четырёхбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие	Критерии оценивания	Зачтено	Не зачтено
-------------	--------------------------------------	---------------------	---------	------------

	сформированность компетенции			
ОПК-11	знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем, 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	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть средствами защиты информации, реализующими политики	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	управления доступом			
--	------------------------	--	--	--

или
«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-11	знать основные понятия и определения, используемые при описании моделей безопасности компьютерных систем, основные виды политик управления доступом и информационными потоками в компьютерных системах, основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов

	программной среды и безопасности информационных потоков					
	уметь разрабатывать частные политики безопасности и компьютерных систем, в том числе политики управления доступом и информационными потоками	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть средствами защиты информации, реализующими политики управления доступом	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1) В описании закрытой политики безопасности, все неопределенные виды доступа считаются...

- А) Разрешенными
- Б) Закрытыми
- В) Таких видов доступа нет
- Г) Запрещенными

2) В описании открытой политики безопасности, все неопределенные виды доступа считаются...

- А) Разрешенными
- Б) Закрытыми
- В) Запрещенными
- Г) Таких видов доступа нет

3) Сколько политик описания безопасности должен специфицировать язык описания политик безопасности?

- А) 1
- Б) 2
- В) 3
- Г) 4

4) При описании какой политики безопасности должны быть определены все запрещенные и разрешенные виды доступа?

- А) Открытая
- Б) Закрытая
- В) Гибридная политика безопасности
- Г) Гибридная политика безопасности с разрешенными противоречиями

5) Спецификация политики безопасности является корректной, если она...

- А) Полна
- Б) Непротиворечива
- В) Непротиворечива и полна
- Г) Правильного ответа нет

6) Сколько методов описания политик безопасности существует?

- А) 1
- Б) 2
- В) 3
- Г) 4

7) Что определяется для описания ПБ при аналитическом методе описания?

- А) Множества субъектов
- Б) Множества объектов
- В) Множество объектов и операции над ними
- Г) Множество субъектов, объектов и операции над ними

8) Что понимается под «состоянием графа» в графовом методе описания ПБ?

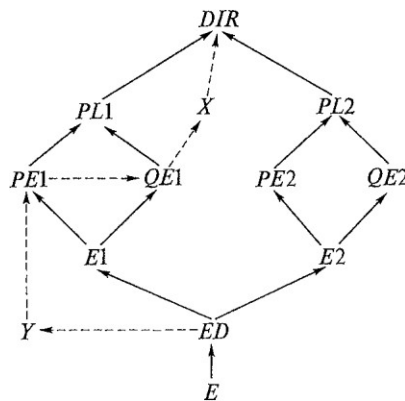
- А) Совокупность вершин
- Б) Совокупность дуг

- Г) Совокупность дуг и вершин
Д) Совокупность дуг, вершин и их атрибутов
- 9) Как называется визуальный язык объектных ограничений в графовом методе?
А) PaSco
Б) LaSCO
В) ScoLA
Г) CoLas
- 10) Каким параметром, момент состояния системы отражается в событиях?
А) Time
Б) Date
В) Event
Г) Нет правильного ответа
- 11) При каком методе описания ПБ представление и анализ ПБ проводится как объектная декомпозиция системы и оценка безопасных/небезопасных состояний?
А) Аналитический метод
Б) Объектный метод
В) Графовый метод
Г) Логический метод
- 12) Вариантом объектного подхода служит язык....
А) Delphi
Б) Londer
В) Ponder
Г) Pascal
- 13) Что обозначает служебное слово «inst» в языке моделирования Ponder?
А) Негативная авторизация
Б) Ограничения
В) Позитивная авторизация
Г) Объявление правила
- 14) В каком методе описания ПБ применяется язык моделирования Ponder?
А) Аналитический метод
Б) Объектный метод
В) Графовый метод
Г) Логический метод

- 15) Сколько фиксированных предикатов в языке авторизации ЯА?
- А) 5
Б) 7
В) 10
Г) 8

7.2.2 Примерный перечень заданий для решения стандартных задач

1) Дана нижеприведенная схема модификации иерархии ролей в АС, причем известно, что пользователь с административной ролью DSO добавил в иерархию ролей роли X и Y. Так как пользователь с административной ролью PSO1 (офицер безопасности проекта 1) может изменять иерархию ролей в интервале ролей (E1, PL1), он установил роль QE1 как старшую над ролью PE1. Таким образом административная роль PSO1 позволила определить роль X как старшую над ролью Y, несмотря на то, что эти роли не входят в определенный для PSO1 интервал ролей (E1, PL1). Определить и письменно обосновать реализацию не менее 3 подходов (или способов) по определению порядка администрирования иерархии ролей в данной ситуации.



2) Составить множество возможных прав доступа в системе. Для заданного множества субъектов и объектов построить матрицу доступов и заполнить ее в соответствии заданной политикой безопасности и с принципом минимизации привилегий. Дополнить матрицу доступов временными доменами для всех возможных действующих субъектов в системе (например, добавить строку "Программа Word, запущенная от имени первого пользователя или "Редактор формул, запущенный третьим пользователем из программы Word").

3) Настроить пароль администратора для электронного ключа eToken в

программе eToken PKI Client.

4) Настроить минимальную длину пароля в 5 символов, максимальный период использования в 30 дней, размер истории паролей в 5 паролей, обязательство использовать в пароле как минимум цифры и строчные буквы при задании пароля пользователя для электронного ключа eToken в программе eToken PKI Client.

7.2.3 Примерный перечень заданий для решения прикладных задач

1) Настроить подсистему защиты входа в систему средства защиты информации от несанкционированного доступа для операционных систем семейства Microsoft Windows Secret Net 7 с применением в качестве средства аутентификации пользователя электронного ключа eToken.

2) Настроить блокировку операционной системы семейства Microsoft Windows средством защиты информации от несанкционированного доступа Secret Net 7 при извлечении электронного ключа eToken.

3) Настроить блокировку операционной системы семейства Microsoft Windows средством защиты информации от несанкционированного доступа Secret Net 7 при извлечении съемного машинного носителя информации с сподключение мпо интерфейсу USB.

4) Настроить разрешения на доступ к каталогам операционной системы семейства Microsoft Windows в соответствии с матрицей доступа с помощью средства защиты информации от несанкционированного доступа Secret Net 7:

	<i>folder1</i>	<i>folder2</i>
<i>admin</i>	Чтение, запись, удаление, выполнение	Чтение, запись, удаление, выполнение
<i>user1</i>	Чтение, запись, удаление, выполнение	
<i>user2</i>		Чтение, запись

5) Настроить затирание удаляемых файлов с 1 циклом затирания с

помощью средства защиты информации от несанкционированного доступа Secret Net 7.

б) Настроить теневое сохранение документов, отправляемых на печать и имеющих статус конфиденциальных с помощью средства защиты информации от несанкционированного доступа Secret Net 7.

7)2.5 Примерный перечень заданий для решения прикладных задач

1. История теории и практики компьютерной безопасности
2. Структура понятия компьютерная безопасность и основные направления ее обеспечения
3. Понятие защищенности (безопасности) компьютерной информации. Конфиденциальность, целостность и доступность информации.
4. Понятие угроз безопасности компьютерной информации и их классификация.
5. Таксонометрия угроз безопасности и изъянов (брешей) систем защиты
6. Человеческий фактор и модель нарушителя безопасности информации.
7. Субъектно-объектная модель компьютерной системы. Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа.
8. Монитор безопасности КС и гарантирование выполнение политики безопасности. Изолированная программная среда.
9. Дискреционные модели безопасности компьютерных систем. Пятимерное пространство Хартсона.
10. Модели безопасности на основе матрицы доступа. Способы организации матрицы доступа и управления доступом в компьютерных системах.
11. Дискреционные модели распространения прав доступа. Модель и теоремы безопасности Харрисона-Руззо-Ульмана.
12. Модель типизированной матрицы доступа.
13. Модель TAKE-GRANT.
14. Расширенная модель TAKE-GRANT.
15. Основы политики мандатного доступа. Решетка безопасности.
16. Модель Белла-ЛаПадулы и основная теорема безопасности
17. Основные расширения модели Белла-ЛаПадулы.
18. Общая характеристика политики тематического разграничения

доступа.

19. Решетки в моделях тематического разграничения доступа. Решетка мультирубрик на иерархических рубриках.

20. Скрытые каналы утечки информации и теоретико-информационные модели безопасности. Технологии "представлений" и "разрешенных процедур".

21. Модели ролевого доступа. Иерархические системы ролей. Принципы наделения ролей полномочиями.

22. Политика и зональная модель безопасности в распределенных КС.

23. Модели обеспечения целостности. Дискреционная модель Кларка-Вильсона.

24. Модели обеспечения целостности. Мандатная модель Кена Биба.

25. Объединение мандатных моделей Белла-ЛаПадулы и Кена Биба.

26. Обеспечение целостности данных мониторами транзакций в клиент-серверных системах

27. Методы, критерии и шкалы оценки эмпирических объектов.

28. Системы многомерного шкалирования защищенности компьютерных систем.

29. Теоретико-графовые модели комплексной оценки защищенности КС. Техно-экономическое обоснование систем обеспечения безопасности.

30. Теоретико-графовые модели комплексной оценки защищенности КС. Тактико-техническое обоснование систем обеспечения безопасности.

31. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Итоговые права доступа.

32. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам.

Количественные параметры систем индивидуально-группового доступа.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент

набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Исходные положения теории компьютерной безопасности	ОПК-11	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
2	Модели безопасности на основе дискреционной политики	ОПК-11	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
3	Модели безопасности на основе мандатной политики	ОПК-11	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
4	Модели безопасности на основе тематической и ролевой политики	ОПК-11	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	Модели и технологии обеспечения целостности и доступности данных	ОПК-11	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
6	Методы анализа и оценки защищенности компьютерных систем	ОПК-11	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики

выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Остапенко А.Г. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс]: Учеб. пособие / А. Г. Остапенко, Д. Г. Плотников, С. В. Машин. - Электрон. текстовые, граф. дан. (112 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.
2. Куликов, С.С. Модели безопасности компьютерных систем [Электронный ресурс]: Учеб. пособие / С. С. Куликов. - Электрон. текстовые, граф. дан. (2,71 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.
3. Кащенко Г.А. Защита программ и данных [Электронный ресурс] / Г. А. Кащенко; Учеб. пособие. - Электрон. текстовые, граф. дан. (3,28 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.

Дополнительная литература:

1. Методические указания к практическим занятиям по дисциплине "Модели безопасности компьютерных систем" для студентов специальности 090301 "Компьютерная безопасность" очной формы обучения [Электронный ресурс] / Каф. систем

информационной безопасности; Сост. И. В. Гончаров. - Электрон. текстовые, граф. дан. (760 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.

2. Методические указания к курсовому проектированию по дисциплине "Сети и системы передачи информации" для студентов специальностей 090301 "Компьютерная безопасность", 090302 "Информационная безопасность телекоммуникационных систем", 090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. И. В. Гончаров. - Электрон. текстовые, граф. дан. (762 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.
3. Методические указания к самостоятельным работам по дисциплине «Модели безопасности компьютерных систем» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. С. С. Куликов. - Электрон. текстовые, граф. дан. (244 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Средство защиты информации от несанкционированного доступа Secret Net 7.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Компьютерный класс с количеством персональных компьютеров из расчета 1 персональный компьютер на 2 обучающихся.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Модели безопасности компьютерных систем» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомиться с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.