МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета ФИТКБ
_____ /Гусев П.Ю./
28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Модели безопасности компьютерных систем»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем 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 2023

Автор программы _____ С.С. Куликов
Заведующий кафедрой информационной безопасности Систем _____ А.Г. Остапенко
Руководитель ОПОП _____ К.А. Разинкин

Воронеж 2023

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 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, овные 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	
		8	9
Аудиторные занятия (всего)	144	72	72
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	72	36	36
Самостоятельная работа	108	72	36
Курсовой проект	+		+
Виды промежуточной аттестации - зачет,	+	+	+
зачет с оценкой			
Общая трудоемкость:			
академические часы	252	144	108
зач.ед.	7	4	3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

№ п/п	Наименование темы	Содержание раздела	Лекц	Лабор. работа	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. угроз. политики и моделей	12	12	18	42
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	18	42
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	18	42
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 функциональноролевых отношений. Формальная спецификация и разновидности ролевых моделей. Индивидуальногрупповое разграничение доступа.	12	12	18	42
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	18	42
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	18	42
		Итого	**72**	**72**	**108**	**252**

5.2 Перечень лабораторных занятий

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

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

Учебным планом по дисциплине «Модели безопасности компьютерных систем» предусмотрено выполнение курсового проекта в 9-ом семестре.

Примерные темы курсового проектирования:

- Разработка модели и программного обеспечения, реализующих политику разграничения доступа в операционной системе;
- 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;
- Модель Хариссона-Руззо-Ульмана;
- Модель мандатного (полномочного) доступа Белла-ЛаПадулы;
- Субъектно-объектная модель в механизмах и процессах коллективного доступа к информационным ресурсам;
- Мандатная, или обязательная, модель (MAC);
- Ролевая схема управления доступом (RBAC);
- Модель управления на основе атрибутов (ABAC).

Курсовой проект включает в себя решение практических задач из различных разделов курса «Методы программирования». Курсовой проект выполняется студентами в соответствии с заданным вариантом, в соответствии с методическими указаниями.

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	Знает основные понятия и определения, используемые при описании моделей безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками профессиональных задач; - производить анализ и выбор эффективного алгоритма поиска и сортировки информации в различных масси-	Разрабатывает частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - средствами защиты информации, реализующими политики управления доступом	Владеет средствами защиты информации, реализующими политики управления доступом	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность	Критерии оценивания	Зачтено	Не зачтено
ОПК-11	Знать: - основные понятия и определения, используемые при описании моделей безопасности компьютерных систем - основные виды политик управления доступом и информационными потоками в компь-	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь: - разрабатывать частные политики безопасности компьютерных систем, в том числе поли-	Решение стандартных задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть: - средствами защиты информации, реализующими политики управления доступом	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

Результаты промежуточного контроля знаний в 9 семестре оцениваются по четырехбальной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ОПК-11	Знать: - основные понятия и определения, используемые при описании моделей	знание учебного материала и использован ие учебного материала в процессе выполнения заданий	Студент демонстрирует полное понимание	Студент демонстрирует значительное	Студент демонстрирует частичное понима-	1. Студент демонстрирует незначитель
	Уметь: - разрабатывать частные политики безопасности компьютерных систем, в том числе поли-	умение использовать учебный материал в процессе выполнения лабораторных работ				
	Владеть: - средствами защиты информации, реализующими политики управления доступом	применение учебного материала при решении практических задач				

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) Какие виды криптографии бывают и для чего они используются?
2) Хеширование информации
3) Что такое электронная подпись и чем отличается от хеша
4) Что такое распределенная атака типа «отказ в обслуживании» (DDoS)
5) Какие уязвимости информационных систем или ПО вы знаете
6) Дайте определение уязвимости как «Инъекция»
7) Какие средства и способы подходят для защиты удаленного доступа
8) Опишите, как работает протокол безопасности
9) Что такое протокол TLS
10) Что такое SSL и можно ли использовать только этот протокол для шифрования

7.2.2 Примерный перечень заданий для решения прикладных задач

1. Определение параметров субъектно-объектной модели разграничения доступа.
2. Разработка политики разграничения доступа субъектов к объектам в операционной системе.
3. Деревья, обход дерева. Деревья с корнем, бинарные деревья.
4. Разработка модели разграничения доступа субъектов к объектам в операционной системе в соответствии с политикой разграничения доступа.
5. Разработка программного обеспечения, реализующего модель

разграничения доступа.

6. Защита от вирусов и вредоносного ПО.
7. Вспомогательные утилиты.
8. Настройка и применение компонентов базовой защиты.
9. Модели распространения прав доступа.
10) Мандатная модель Кена Биба.

7.4 Примерный перечень вопросов для подготовки к зачету

1) Протокол безопасности
2) Хеширование информации
3) Что такое электронная подпись и чем отличается от хеша
4) Что такое распределенная атака
5) Чем различаются уязвимость, эксплойт и атака
6) Дайте определение уязвимости как «Инъекция»
7) Какие средства и способы подходят для защиты удаленного доступа
8) Опишите, как работает протокол безопасности
9) Что такое кибербезопасность
10) Назовите элементы кибербезопасности
11) История теории и практики компьютерной безопасности
12) Структура понятия компьютерная безопасность и основные направления ее обеспечения
13) Понятие защищенности (безопасности) компьютерной информации. Конфиденциальность, целостность и доступность информации.
14) Понятие угроз безопасности компьютерной информации и их классификация.
15) Таксонометрия угроз безопасности и изъянов (брешей) систем защиты
16) Человеческий фактор и модель нарушителя безопасности информации.
17) Субъектно-объектная модель компьютерной системы.
18) Понятие потока, доступа и правил разграничения доступа.
19) Основные типы политик разграничения доступа.
20) Монитор безопасности КС и гарантирование выполнение политики безопасности.

7.5 Для защиты лабораторных работ необходимо:

В тетради для лабораторных работ выполнить обработку результатов в соответствии с «Заданиями», приведенными в «Методических указаниях».

Подготовить ответы на вопросы:

- описать цель работы;
- изучить поставленные задачи;
- описать этапы выполнения работы;
- сформулировать вывод по результатам работы;
- оформить отчет по лабораторной работе;
- ответить на поставленные вопросы.

Результаты защиты оцениваются по двухбалльной системе: «зачёт», «незачёт». При ответе на 50% вопросов и более из представленных, лабораторная работа

считается выполненной и зачтенной.

7.6 Методика выставления оценки при проведении промежуточной аттестации

Зачет 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 «Зачтено» ставится в случае, если студент набрал от 15 до 20 баллов.
2. Оценка «Не зачтено» ставится в случае, если студент набрал менее15 баллов.

7.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Функциональные требования Secret Net 7	ОПК-11	Тест, защита лабораторных работ
2	Механизмы защиты Secret Net 7	ОПК-11	Тест, защита лабораторных работ
3	Принципы построения системы Secret Net Studio и способы ее развертывания	ОПК-11	Защита лабораторных работ, требования к курсовому проекту
4	Настройка и применение компонентов базовой защиты	ОПК-11	Тест, защита лабораторных работ
5	Настройка и применение компонентов локальной защиты Secret Net 7	ОПК-11	Защита лабораторных работ, требования к курсовому проекту
6	Персональный межсетевой экран	ОПК-11	Тест, защита лабораторных работ

7.2 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 методике 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 методике 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 методике выставления оценки при проведении промежуточной аттестации.

Защита курсового проекта осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 15 мин.

8 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная:

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.

Дополнительная литература:

3. 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.

4. Методические указания к курсовому проектированию подисциплине "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 "Воронежскийгосударственный технический университет", 2014. - 1 файл. - 0000.

5. 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. - 0000.

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:

Операционная система, не ниже Windows 10.

Пакет программ VMWare Workstation, VirtualBox.

Google-документы, Google- таблицы, Google-презентации.

Пакет офисных приложений TEX.

UML.

https://e.lanbook.com/book/111049 - Книга из коллекции Лань - Модели безопасности компьютерных систем - ISBN 978-5-9912-0328-9

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Для проведения лекций аудитория оснащена проектором и проекционной доской.

При изучении данной дисциплины используется учебная аудитория 201/5 кафедры СИБ с оборудованием:

Комплект учебной мебели на 26 посадочных мест из них оснащены компьютерами - 8 посадочных мест.

Компьютеры в составе:

intel CORE 2Duo E7500 2/93ГГц,3М, 1066МГц, - 8 шт.

Рабочее место преподавателя.

Для проведения лабораторных занятий, в аудитории имеется подключение к сети "Интернет".

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.

Виды учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать 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 удается разобраться в материале, необхо-
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, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения 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 три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственного за реализацию ОПОП
1			
2			
3			