МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
математического моделирования
М.Ш. Бурлуцкая
16.04.2024г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.12 Модели безопасности компьютерных систем

1. Код и наименование специальности:

10.05.04 Информационно-аналитические системы безопасности

2. Специализация:

Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника:Специалист по защите информации

4. Форма обучения:Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра математического моделирования

6. Составитель программы:Бурлуцкая Мария Шаукатовна, д.ф.-м.н., доцент

7. Рекомендована:Научно-методическим советом математического факультета,протокол № 0500-03 от 28.03.2024

8. Учебный год:2027/2028 **Семестр:**8

9. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- обучение принципам формального моделирования и анализа безопасности компьютерных систем, реализующих управление доступом и информационными потоками.

Задачи учебной дисциплины:

- изучение основ устройства и принципов функционирования, методологии проектирования и построения защищенных компьютерных систем;
- изучение теоретико-графовых моделей комплексной оценки защищенности КС;
- изучение методов анализа и оптимизации индивидуально-групповых систем разграничения доступа.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина «Модели безопасности компьютерных систем» относится к части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули).

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-2	Способен организовывать работы по выполнению в информационно-аналитических системах требований защиты информации ограниченного доступа	ПК-2.1	Способен анализировать безопасность информации с помощью формальных моделей	Знать: способы и методы анализа безопасности информации с помощью формальных моделей; Уметь: моделировать угрозы безопасности информации; Владеть: навыкамианализа защищенности информационных систем.
		ПК-2.2	Способен моделировать угрозы безопасности информации	

12. Объем дисциплины в зачетных единицах/час.— 3/108.

Форма промежуточной аттестации:экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			8 семестр	
Контактная работа		48	48	
в том числе:	лекции	16	16	
	практические	0	0	
	лабораторные	32	32	
	курсовая работа			
	контрольные работы			
Самостоятельная работа		24	24	
Промежуточная аттестация		36	36	
Итого:		**108**	**108**	

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Введение. Основные понятия и определения	Угрозы безопасности информации. Политика безопасности. Понятие политики безопасности. Модель нарушителя.	
1.2	Модели компьютерных систем с дискреционным управлением доступом	Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Модель типизированной матрицы доступов (ТМД). Монотонные системы ТМД и их каноническая форма. Классическая модель Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста. Условия передачи прав доступа в произвольном графе доступов при отсутствии ограничений на кооперацию субъектов. Расширенная модель Take-Grant. Де-факто правила преобразования графов доступов и информационных потоков. Условия реализации информационных потоков. Алгоритм построения замыкания графа доступов и информационных потоков. Представление систем Take-Grant системами ХРУ и ТМД.	
1.3	Модели компьютерных систем с мандатным управлением доступом	Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности. Модель систем военных сообщений. Неформальное и формальное описания модели систем военных сообщений. Безопасное состояние. Безопасность переходов. Потенциальная модификация сущности с источником. Смыслы безопасности функции переходов.	
1.4	Модели безопасности информационных потоков и изолированной программной среды	Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм защиты. Вероятностная модель безопасности информационных потоков. Информационное невлияние. Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.	
1.5	Модели компьютерных систем с ролевым управлением доступом	Базовая модель ролевого управления доступом. Модель администрирования ролевого управления доступом. Описание базовой модели ролевого управления доступом. Иерархия ролей. Механизм ограничений. Модель администрирования ролевого управления доступом. Администрирование множеств авторизованных ролей пользователей, прав доступа, которыми обладает роли, иерархии ролей. Модель мандатного ролевого управления доступом.	
1.6	Развитие формальных моделей безопасности компьютерных систем	Взаимосвязь положений классических формальных моделей безопасности КС. Критический анализ классических моделей. Проблема адекватности реализации модели безопасности в реальной КС. Семейство моделей безопасности логического управления доступом и информационными потоками (ДП-моделей). Развитие формальных моделей.	

2. Лабораторные занятия			
2.1	Введение. Основные понятия и определения	Модель нарушителя. Основные виды политик управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков.	
2.2	Модели компьютерных систем с дискреционным управлением доступом	Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ. Граф создания. Ациклические монотонные ТМД и алгоритм проверки их безопасности. Алгоритм построения замыкания графа доступов и информационных потоков. Представление систем Take-Grant системами ХРУ и ТМД.	
2.3	Модели компьютерных систем с мандатным управлением доступом	Интерпретации модели Белла-ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла-ЛаПадулы. Примеры реализации запрещенных информационных потоков по памяти или по времени.	
2.4	Модели безопасности информационных потоков и изолированной программной среды	Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм защиты. Вероятностная модель безопасности информационных потоков. Информационное невлияние. Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.	
2.5	Модели компьютерных систем с ролевым управлением доступом	Задание иерархии ролей и ограничений в соответствии с требованиями либерального или строгого мандатного управления доступом. Безопасность информационных потоков. Защита от угроз конфиденциальности и целостности информации.	
2.6	Развитие формальных моделей безопасности компьютерных систем	Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом. Доверенные и недоверенные субъекты. Анализ информационных потоков по памяти или по времени. Функционально или параметрически ассоциированные с субъектами сущности.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практи-ческие	Лабора-торные	Самостоя-тельная работа	Всего
1	1. Введение. Основные понятия и определения	**6**		**6**	**4**	**16**
	2. Модели компьютерных систем с дискреционным управлением доступом	**6**		**6**	**4**	**16**
	3. Модели компьютерных систем с мандатным управлением доступом	**6**		**6**	**4**	**16**
	4. Модели безопасности информационных потоков и изолированной программной среды	**4**		**4**	**4**	**12**
2	5. Модели компьютерных систем с ролевым управлением доступом	**6**		**6**	**4**	**16**
3	6. Развитие формальных моделей безопасности компьютерных систем	**4**		**4**	**4**	**12**

	Итого:	**16**	**-**	**32**	**24**	**72**

14. Методические указания для обучающихся по освоению дисциплины:

Освоение дисциплины предполагает не только обязательное посещение обучающимся аудиторных занятий (лекций илабораторных занятий) и активную работу на них, но и самостоятельную учебную деятельность, на которую отводится 24 часа.

Самостоятельная учебная деятельность студентов по дисциплине «Модели безопасности компьютерных систем» предполагает выполнение следующих заданий:

1) самостоятельное изучение учебных материалов по разделам дисциплины с использованием основной и дополнительной литературы, информационно-справочных и поисковых систем;

2) подготовку к текущим аттестациям: выполнение практических заданий, поиск необходимых для работы материалов в Интернете.

Особое внимание обучающихся направляется на освоение необходимого в дальнейшим математического аппарата.

Вопросы лекционных и практических занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и лабораторным занятиям, обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать свои знания и кругозор, умение логически построить ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям.

Все выполняемые студентами самостоятельно задания (выполнение контрольных и самостоятельных/лабораторных работ) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации.

В случае необходимости перехода на дистанционный режим обученияиспользуется электронный курс «Модели безопасности компьютерных систем»на портале «Электронный университет ВГУ»:https://edu.vsu.ru.

Там жеразмещены необходимые для усвоения курса материалы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1.	Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. — М.: Горячая линия - Телеком, 2020. – 352 с.
2.	Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие Екатеринбург: изд-во Урал. Унта 2008. – 212 с.
3.	

б) дополнительная литература:

№ п/п	Источник
4.	Кабанов А.С., Лось А.Б., Першаков А.С. Теоретические основы компьютер-ной безопасности, М: РИО МИЭМ.- 2012.- 245 с.
5.	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей, М: ИД

	«Форум». - 2010 г. .- 415 с.
6.	

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет):

№ п/п	Ресурс
7.	Сайт математического факультета ВГУ. Раздел, на котором размещены методические издания:https://math.vsu.ru/wp/?page_id=937.
8.	ЭБС «Университетская библиотека онлайн».
9.	Электронный каталог ЗНБ ВГУ :http://www.lib.vsu.ru .
10.	Электронный университет ВГУ: https://edu.vsu.ru/course/view.php?id=19958.

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1.	Богульская, Нина Александровна. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров ; М-во науки и высш. образования Рос. Федер.,Сиб. федер. ун-т, Ин-т космич. и информ. технологий. - Красноярск : СФУ, 2019. - 204 с. : рис., табл. - Библиогр.: с. 204.
2.	
3.	Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ»(https://edu.vsu.ru).

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации; специализированная мебель.

Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно-правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

Перечень необходимого программного обеспечения:

Ubuntu (бесплатное и/или свободное ПО, лицензия: https://ubuntu.com/download/desktop),

VisualStudioCommunity (бесплатное и/или свободное ПО, лицензия https://visualstudio.microsoft.com/ru/vs/community/)

LibreOffice (GNU LesserGeneralPublicLicense (LGPL), бесплатное и/или свободное ПО, лицензия: https://ru.libreoffice.org/about-us/license/)

Foxit Reader, браузер Mozilla Firefox, Opera или Internet.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочныесредства
1	Введение. Основные понятия и определения	ОПК-4	ОПК-4.3	Тест
2	Модели компьютерных систем с			Тест

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочныесредства
	дискреционным управлением доступом			
3	Модели компьютерных систем с мандатным управлением доступом	ОПК-8	ОПК-8.1	Тест
4	Модели безопасности информационных потоков и изолированной программной среды		ОПК-8.2	Контрольная работа
				Перечень вопросов к зачету

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочныесредства
1	Модели компьютерных систем с ролевым управлением доступом	ПК-2	ПК-2.1	Практическое задание
2	Развитие формальных моделей безопасности компьютерных систем		ПК-2.2	Контрольная работа
Промежуточная аттестация Форма контроля –экзамен				Перечень вопросов к экзамену

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: устных опросов, проверки домашних заданий, самостоятельных работ, контрольной работы.

Для оценивания текущего контроля успеваемости и оценивания самостоятельной работы используются следующие ***показатели:***

1) знание основных понятий и методов;
2) умение применять полученные знания и навыки для решения задач, проводить анализ полученных решений;
3) владение навыками хранения, поиска, сбора, систематизации, обработки и использования информации.

Шкала оценок:

Зачтено: Выполнение заданий соответствует перечисленным показателям, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует умение решать задачи, возможно с некоторыми ошибками.

Не зачтено:Ответы не соответствуют ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или их отсутствие.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется в форме собеседования по билетам с помощью нижеприведенных оценочных средств (перечень вопросов к экзамену).

В билет включаются теоретический вопрос и задача из примерного перечня задач для контрольной работы.

В случае посещения обучающимся всех аудиторных занятий (лекций и лабораторных занятий) и активной работы на них, успешного выполнения элементов текущей аттестации (самостоятельные работы), оценка за промежуточнуюаттестацию может быть выставлена по результатам текущих аттестаций.

Перечень вопросов к экзамену:

1.Угрозы безопасности информации. Политика безопасности.
2. Понятие политики безопасности. Модель нарушителя.
3. Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ).
4 Модель типизированной матрицы доступов (ТМД). Монотонные системы ТМД и их каноническая форма.
5.Классическая модель Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста. Условия передачи прав доступа в произвольном графе доступов при отсутствии ограничений на кооперацию субъектов.
6. Расширенная модель Take-Grant. Де-факто правила преобразования графов доступов и информационных потоков. Условия реализации информационных потоков. Алгоритм построения замыкания графа доступов и информационных потоков. Представление систем Take-Grant системами ХРУ и ТМД.
7. Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности.
8. Модель систем военных сообщений. Неформальное и формальное описания модели систем военных сообщений. Безопасное состояние. Безопасность переходов. Потенциальная модификация сущности с источником. Смыслы безопасности функции переходов.
9. Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм защиты.
10. Вероятностная модель безопасности информационных потоков. Информационное невлияние.
11. Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.
12. Базовая модель ролевого управления доступом. Модель администрирования ролевого управления доступом. Описание базовой модели ролевого управления доступом
13. Иерархия ролей. Механизм ограничений.
14. Модель администрирования ролевого управления доступом. Администрирование множеств авторизованных ролей пользователей, прав доступа, которыми обладает роли, иерархии ролей.
15. Модель мандатного ролевого управления доступом.
16. Взаимосвязь положений классических формальных моделей безопасности КС. Критический анализ классических моделей. Проблема адекватности реализации модели безопасности в реальной КС.
17. Семейство моделей безопасности логического управления доступом и информационными потоками (ДП-моделей).
18. Развитие формальных моделей.

Для оценивания результатов обучения на зачете используются следующие **показатели:**

1) знание теоретических основ;
2) умение решать задачи;
3) умение работать с алгоритмами методов и информационными ресурсами;
4) успешное прохождение текущей аттестации.

Для оценивания результатов экзамена используется ***шкала:*** «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения показаны в следующей таблице:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Полное соответствие обучающимся всем перечисленным показателям по каждому из вопросов контрольно-измерительного материала. Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, применять теоретические знания для решения практических задач в области курса, студент умеет работать с различными источниками научной информации,грамотно и правильно представляет свои результаты, правильно отвечает на вопросы КИМ	Повышенный уровень	Отлично
Несоответствие ответа обучающегося одному из перечисленных выше показателей (к одному из вопросов контрольно-измерительного материала) и правильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым двум из перечисленных показателей (либо двум к одному вопросу, либо по одному к каждому вопросу контрольно-измерительного материала) и правильные ответы на два дополнительных вопроса в пределах программы.	Базовый уровень	Хорошо
Несоответствие ответа обучающегося любым двум из перечисленных показателей и неправильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым трем из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	Пороговый уровень	Удовлетвори-тельно
Несоответствие ответа обучающегося любым из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	–	Неудовлетвори тельно

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1) закрытые задания (тестовые):

1. При полномочной политике безопасности совокупность меток с одинаковыми значениями образует: +а) уровень безопасности; б) область равного доступа; в) область равной критичности; г) уровень доступности

2. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности: + а) LWM; б) на основе угроз; в) Лендвера; г) с полным перекрытием.

3. Недостатком модели конечных состояний политики безопасности является: а) изменение линий связи; б) статичность; + в) сложность реализации; г) низкая степень надёжности.
4. «При избирательной политике безопасности в матрице доступа на пересечении столбца и строки указывается: а) субъект системы; + б) тип разрешенного доступа; в) факт доступа; г) объект системы.
5. Основу политики безопасности составляет: + а) способ управления доступом; б) управление риском; в) программное обеспечение; г) выбор каналов связи.

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания закрытого типа (множественный выбор):

- 2 балла – указаны все верные ответы;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):

- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

5) Задания открытого типа (число):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).