Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.23 Модели безопасности компьютерных систем»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2021

Рабочая программа дисциплины «*Б1.Д.Б.23 Модели безопасности компьютерных систем*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 8 от "5" апреля 2021 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
профессор — М.Ю.Нестеренко
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись Н.Н. Бигалиева
расшифровка подписи

Уполномоченный по качеству факультета
личная подпись И.В. Крючкова
расшифровка подписи

№ регистрации 125674

© Нестеренко М.Ю., 2021
© ОГУ, 2021

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Изучение теоретических основ моделей безопасности компьютерных систем, получение навыков их программной реализации. Изучение математических моделей контроля и управления доступом, получение навыков их программной реализации.

Задачи:

- изучить дискреционные, мандатные и ролевые модели безопасности компьютерных систем;

- изучить модели безопасности информационных потоков, модели изолированной программной среды;

- получить практические навыки программной реализации данных моделей.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.13 Информатика, Б1.Д.Б.19 Операционные системы, Б1.Д.Б.20 Компьютерные сети, Б1.Д.Б.37 Администрирование информационных систем*

Постреквизиты дисциплины: *Б1.Д.Б.26 Основы построения защищенных компьютерных сетей, Б1.Д.Б.27 Основы построения защищенных баз данных, Б1.Д.В.2 Технология построения защищенных автоматизированных систем, Б1.Д.В.Э.4.1 Безопасные распределенные системы, Б2.П.В.П.2 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6-В-4 Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем ОПК-6-В-5 Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем	**Знать:** - руководящие и нормативно-правовые документы по оценке уровня защищенности информации в компьютерных системах. **Уметь:** - оценивать уровень защищенности информации в компьютерных системах в части используемых моделей безопасности компьютерных систем. **Владеть:** - навыками составления отчетов по результатам проводимых оценок.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования 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	ОПК-11-В-1 Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем ОПК-11-В-2 Знает основные виды политик управления доступом и информационными потоками в компьютерных системах ОПК-11-В-3 Знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков ОПК-11-В-4 Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем ОПК-11-В-5 Умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками ОПК-11-В-6 Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах	**Знать**: - типовые модели безопасности компьютерных систем. **Уметь**: - разрабатывать модели безопасности управления доступом и информационными потоками. **Владеть**: - владеть навыками реализации моделей безопасности в рамках информационных систем.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 7 зачетных единиц (252 академических часа).

Вид работы	Трудоемкость, академических часов		
	9 семестр	10 семестр	всего
Общая трудоёмкость	**144**	**108**	**252**
Контактная работа:	**84,25**	**61,25**	**145,5**
Лекции (Л)	34	30	64
Лабораторные работы (ЛР)	50	30	80
Консультации		1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25	0,5
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата (Р);* *- написание эссе (Э);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;*	**59,75**	**46,75**	**106,5**

Вид работы	Трудоемкость, академических часов		
	9 семестр	10 семестр	всего
- подготовка к лабораторным занятиям; *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*			
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	**экзамен**	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в понятийные основы моделирования компьютерных систем и их безопасности	36	8		12	16
2	Моделирование систем защиты информации	46	12		16	18
3	Субъектно-объектная модель КС в механизмах и процессах коллективного доступа к информационным ресурсам	62	14		22	26
	Итого:	144	34		50	60

Разделы дисциплины, изучаемые в 10 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
4	Модели безопасности на основе дискреционной политики		6		6	10
5	Модели распространения прав доступа		6		6	10
6	Модели мандатного управления доступом		8		8	10
7	Модели ролевого управления доступом		6		6	10
8	Информационные модели		4		4	8
	Итого:	108	30		30	48
	Всего:	252	64		80	108

4.2 Содержание разделов дисциплины

Раздел 1. Введение в понятийные основы моделирования компьютерных систем и их безопасности.

Модель и моделирование КС. Цели моделирования, классификация моделей КС. Применение моделей и моделирования в КС.

Раздел 2. Моделирование систем защиты информации.

Общая модель СЗИ, обобщенная модель СЗИ, модель с полным перекрытием. Модели оптимизации затрат на ЗИ. Формальные и неформальные политики безопасности. Формальные методы анализа систем.

Раздел 3. Субъектно-объектная модель КС в механизмах и процессах коллективного доступа к информационным ресурсам

Модели конечных состояний. Понятие политики и моделей безопасности информации в КС. Понятия субъекта и объекта системы, ассоциированных объектов, потоков информации, доступа к объекту. Аксиомы защищенности компьютерных систем. Монитор (ядро) безопасности КС. Гарантирование выполнения политики безопасности, изолированная программная среда. Основная теорема безопасности.

Раздел 4. Модели безопасности на основе дискреционной политики

Модели на основе матрицы доступов. Модель Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Модель типизированной матрицы доступов. Пятимерное пространство Хартсона.

Раздел 5. Модели распространения прав доступа

Теоретико-графовая модель анализа распространения прав доступа в дискреционных системах на основе матрицы доступа. Модель распространения прав доступа Take-Grant. Основные положения классической модели Take-Grant. Предикат Can_Share. Расширенная модель Take-Grant. Де-факто и де-юро правила. Предикат Can_Steal.

Раздел 6. Модели мандатного управления доступом

Классическая модель Белла-ЛаПадула. Политика low-watermark. Безопасность переходов. Модель мандатной политик целостности информации Биба. Модель систем военных сообщений.

Раздел 7. Модели ролевого управления доступом

Разновидности ролевых моделей. Базовая модель ролевого разграничения доступа. Иерархическая система ролей. Агрегация прав при иерархической организации ролей. Строго таксономический листовой подход, нетаксономический листовой подход, иерархически охватный подход. Модели индивидуально-группового доступа.

Раздел 8. Информационные модели

Понятие и общая характеристика скрытых каналов утечки информации. Автоматная модель невлияния Гогена-Месигера (GM-модель). Теоретико-информационные модели невыводимости и невлияния (невмешательства).

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Основы моделирования компьютерных систем и их безопасности.	12
2	2	Моделирование систем защиты информации	16
3	3	Монитор безопасности (пересылок)	22
1	4	Модель разграничения доступа Харрисона-Рузо-Ульмана. Модель типизированной матрицы доступа.	6
2	5	Мандатная классическая модель Белла-Ла Падула	6
3	6	Модель распространения прав доступа Take-Grant	8
4	7	Ролевая модель разграничения доступа	6
5	8	Организация управления доступом в операционной системе Astra Linux Special Edition	4
		Итого:	80

5 Учебно-методическое обеспечение дисциплины

(В личном кабинете преподавателя, в разделе «Начало» размещены «Рекомендации к оформлению раздела 5 рабочих программ учебных дисциплин»)

5.1 Основная литература

1. Девянин, П.Н. Модели безопасности компьютерных систем [Текст] : учеб. пособие для вузов / П. Н. Девянин. - М. : Академия, 2005. - 144 с. - (Высшее профессиональное образование : информационная безопасность). - Библиогр.: с. 139-140. - ISBN 5-7695-2053-1.
2. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев.- 4-е изд., стер. - М. : Академия, 2008. - 256 с. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 251-252. - ISBN 978-5-7695-5118-5.
3. Сергеева Ю. С. Защита информации. Конспект лекций. Учебное пособие [Электронный ресурс] / Сергеева Ю. С. - А-Приор, 2011. – Режим доступа: http://www.biblioclub.ru/index.php?page=book&id=72670

5.2 Дополнительная литература

1. Галатенко В. А. Основы информационной безопасности [Электронный ресурс] / Галатенко В. А. - Интернет-Университет Информационных Технологий, 2006. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=233063
2. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] : учеб. пособие для вузов / А. А. Малюк. - М. : Горячая линия-Телеком, 2004. - 280 с. : ил. - Библиогр.: с. 276-278. - ISBN 5-93517-197-X.
3. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для вузов / П. Н. Девянин [и др.]. - М. : Радио и связь, 2000. - 192 с. : ил. - Авт. указаны на обороте тит. л.. - Библиогр. в конце гл. - ISBN 5-256-01413-7.

5.3 Периодические издания

1. Информационная безопасность : журнал. - М. : Агентство "Роспечать".
2. Информация и безопасность : журнал. - М. : Агентство "Роспечать".
3. Вестник информационной безопасности : журнал. - М. : Агенство "Роспечать".

5.4 Интернет-ресурсы

1. Погонышева Д.А. Безопасность информационных систем. Глава 4.2. Модели безопасности и их применение // ВикиЧтение, 2012. – Режим доступа: https://it.wikireading.ru/4308.
2. Ниссенбаум О.В. Общие материалы. Все документы. – Режим доступа: http://www.imkn.ru/KIB/Nissenbaum/Shared%20Documents/Forms/AllItems.aspx
3. Введение в безопасность на основе мандатных ссылок (англ. Capability-based security). –Режим доступа: https://habrahabr.ru/post/148743/

https://universarium.org/catalog - «Универсариум», Курсы, МООК: «Общие вопросы философии науки»;

https://www.lektorium.tv/mooc - «Лекториум», МООК: «Дискретная математика»

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Microsoft Windows.
2. Операционная система Astra Linux Special Edition
3. Open Office/LibreOffice - свободный офисный пакет программ, включающий в себя

текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
4. Среда разработки Microsoft Visual Studio.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется лаборатория «*Наименование*» (при наличии), (компьютерный класс) оснащенная/ оснащенный (указывается конкретное оборудование и т.п.)

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

Каждый вид помещения может быть дополнен средствами обучения, реально используемыми при проведении учебных занятий соответствующего типа (например, - лабораторные стенды, макеты, имитационные модели, компьютерные тренажеры, симуляторы, муляжи, учебно-наглядные пособия, плакаты и т.п.)

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.