МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета
Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины

Модели безопасности компьютерных систем

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Дисциплина «Модели безопасности компьютерных систем» обеспечивает приобретение фундаментальных и профессиональных знаний и умений в соответствии с Федеральным государственным образовательным стандартом, содействует фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является формирование способностей:

- разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;
- проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;
- строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты систем безопасности с использованием современных математических методов.

2. Место дисциплины в структуре ОП специалитета

Дисциплина «Модели безопасности компьютерных систем» относится к обязательной части образовательной программы. Она играет исключительно важную роль для профессиональной подготовки специалиста. При ее изучении существенно используются знания, полученные при изучении математических дисциплин «Алгебра», «Дискретная математика» и «Математическая логика и теория алгоритмов».

Знания и практические навыки, полученные из этого курса, используются обучаемыми при изучении профессиональных дисциплин, таких как «Основы построения защищенных баз данных», «Основы построения защищенных компьютерных систем», при разработке курсовых и дипломных работ, а также в дальнейшей профессиональной деятельности.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП специалитета

Процесс изучения дисциплины «Модели безопасности компьютерных систем» направлен на формирование следующих профессиональных компетенций в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности «10.05.01-Компьютерная безопасность» (уровень специалитета) и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Профессиональные компетенции		
ПК-2 Способен разрабатывать математические модели систем обеспечения информационной безопасности, математически доказывать их соответствие выбранным	И-ПК-2.1 Знает основные понятия, методы построения и исследования математических моделей систем обеспечения информационной безопасности	**Знать** основные понятия: Сущность, субъект, доступ, информационный поток, угрозы безопасности информации, политики безопасности, дискреционный, мандатный, ролевой принципы разграничения доступа Уметь воспроизводить ключевые математические приемы, используемые при описании основных понятий

политикам безопасности	И-ПК-2.2 Умеет разрабатывать математические модели систем обеспечения информационной безопасности, математически доказывать их соответствие выбранным политикам безопасности	**Умеет** разрабатывать модели дискреционного/мандатного/ролевого разграничения доступа **Владеет навыками** математически доказывать их соответствие выбранным политикам безопасности
ПК-3 Способен анализировать математические модели систем обеспечения информационной безопасности, а также проводить тестирование средств защиты информации на соответствие этим моделям	И-ПК-3.1 Знает способы анализа математических моделей систем обеспечения информационной безопасности	**Знать** способы анализа математических моделей систем обеспечения информационной безопасности
	И-ПК-3.2 Способен проводить тестирование средств защиты информации на соответствие математическим моделям систем обеспечения информационной безопасности	**Уметь** ориентироваться в концепции защиты компьютерных систем и средств вычислительной техники по руководящим документам ФСТЭК России. **Владеть навыками** тестирования средств защиты информации на соответствие моделям систем обеспечения информационной безопасности

4. Объем, структура и содержание дисциплины «Модели безопасности компьютерных систем»

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 акад.часа.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные	самостоятельная работа	
1	**Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем** 1.1. Элементы теории защиты информации 1.2. Математические основы моделей безопасности 1.3. Основные виды моделей безопасности	9	4	4				**4**	Устный опрос
2	**Модели систем дискреционного разграничения доступа** 2.1. Модель матрицы доступов ХРУ 2.2. Модель распространения прав доступа Take-Grant	9	**4**	**4**				4	Задания для самостоятельной (домашней) работы Устный опрос
3	**Модели систем мандатного разграничения доступа** 3.1. Модель Белла—ЛаПадула 3.2. Модель систем военных сообщений	9	4	4				6	Задания для самостоятельной (домашней) работы Устный опрос

4	**Основные критерии защищенности КС. Классы защищенности КС.** 4.1. Основные критерии оценки защищенности КС 4.2. Стандарт оценки безопасности компьютерных систем *TCSEC* («Оранжевая книга») 4.3. Концепция защиты КС и СВТ по руководящим документам ФСТЭК России. 4.4. Общие критерии безопасности информационных технологий (*Common Criteria*)	9	4	4				**4**	Задания для самостоятельной (домашней) работы Устный опрос
5	**Модели безопасности информационных потоков** 5.1. Автоматная модель безопасности информационных потоков 5.2. Программная модель контроля информационных потоков. Контролирующий механизм защиты. 5.3. Вероятностная модель безопасности информационных потоков	9	4	4				**6**	Задания для самостоятельной (домашней) работы Устный опрос
6	**Субъектно-ориентированная модель изолированной программной среды** 6.1. Основные понятия 6.2. Базовая теорема ИПС	9	4	4				**4**	Задания для самостоятельной (домашней) работы Устный опрос
7	**Модели ролевого разграничения доступа** 7.1. Понятие ролевого разграничения доступа 7.2. Базовая модель РРД 7.3. Модель администрирования РРД 7.4. Модель мандатного РРД	9	4	4				4	Задания для самостоятельной (домашней) работы Устный опрос

8	**Проблемы применения моделей безопасности при построении защищенных компьютерных систем** 8.1. Проблема адекватности реализации модели безопасности в реальной компьютерной системе 8.2. Обоснование политики безопасного администрирования ОС семейств Windows	9	4	4				**4**	Задания для самостоятельной (домашней) работы Устный опрос
						2	**0.5**	**33,5**	**Экзамен**
	Всего	**144**	**32**	**32**		**10**	**0.5**	**69,5**	

Содержание разделов программы дисциплины «Модели безопасности компьютерных систем»

Раздел 1. Введение. Основные понятия и определения

1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем

Элементы теории защиты информации.
Математические основы моделей безопасности.
Основные виды моделей безопасности.

Сущность, субъект, доступ, информационный поток

Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени). Основная аксиома компьютерной безопасности. Модель решетки: линейная решетка, решетка многоуровневой безопасности.

Угрозы безопасности информации. Политика безопасности

Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Понятие политики безопасности. Модель угроз. Модель нарушителя. Основные виды политик управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления доступом, управления доступом на основе атрибутов, изолированной программной среды и безопасности информационных потоков.

Раздел 2. Модели компьютерных систем с дискреционным управлением доступом

2. Модели систем дискреционного разграничения доступа

2.1. Модель матрицы доступов ХРУ

Модель матрицы доступов Харрисона-Руззо-Ульмана

Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ.

Модель типизированной матрицы доступов

Модель типизированной матрицы доступов (ТМД). Монотонные системы ТМД и их каноническая форма. Граф создания. Ациклические монотонные ТМД и алгоритм проверки их безопасности.

2.2. Модель распространения прав доступа Take-Grant

Классическая модель распространения прав доступа *Take-Grant*

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 распространения прав доступа Take-Grant

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.

Раздел 3. Модели компьютерных систем с мандатным управлением доступом

3. Модели систем мандатного разграничения доступа

3.1. Модель Белла—ЛаПадулы

Классическая модель Белла-ЛаПадулы

Классическая модель Белла-ЛаПадулы. Свойства безопасности. Безопасный доступ, состояние, система. Базовая теорема безопасности.

Интерпретации модели Белла-ЛаПадулы

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.

3.2. Модель систем военных сообщений

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.

Раздел 4. Критерии защищенности компьютерных систем.

4. Основные критерии защищенности КС. Классы защищенности КС.

4.1. Основные критерии оценки защищенности КС

4.2. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).

4.3. Концепция защиты КС и СВТ по руководящим документам ФСТЭК России.

4.4. Общие критерии безопасности информационных технологий (*Common Criteria*).

Раздел 5. Модели безопасности информационных потоков и изолированной программной среды

5. Модели безопасности информационных потоков

5.1. Автоматная модель безопасности информационных потоков

5.2. Программная модель контроля информационных потоков. Контролирующий механизм защиты.

5.3. Вероятностная модель безопасности информационных потоков.

Раздел 6. Субъектно-ориентированная модель изолированной программной среды

6. Субъектно-ориентированная модель изолированной программной среды

6.1. Основные понятия

6.3. Базовая теорема ИПС

Раздел 7. Модели компьютерных систем с ролевым управлением доступом

7. Модели ролевого разграничения доступа

7.1. Понятие ролевого разграничения доступа

7.2. Базовая модель РРД

7.3. Модель администрирования РРД

7.4. Модель мандатного РРД

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 обладают роли, иерархии ролей.

Модель мандатного ролевого управления 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.

Раздел 8. Проблемы применения моделей безопасности при построении защищенных компьютерных систем

8. Проблемы применения моделей безопасности при построении защищенных компьютерных систем

8.1. Проблема адекватности реализации модели безопасности в реальной компьютерной системе

8.2. Обоснование политики безопасного администрирования ОС семейств Windows

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция — первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. На этой лекции высказываются методические и организационные особенности

работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) — последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие — занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

В процессе обучения используется в том числе **Электронный учебный курс в LMS Электронный университет Moodle ЯрГУ,** в котором представлены список учебной литературы для освоения дисциплины, правила прохождения промежуточной аттестации по дисциплине, задания для самостоятельной работы обучающихся, представлены тексты лекций по отдельным темам дисциплины, ссылки на лекции и практические семинары и консультации, проводимые онлайн.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

- программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов: Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery); Microsoft OfficeSTD; MikTeX (свободно распространяемое ПО);

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, интернет-ресурсов, необходимых для освоения дисциплины

а) основная литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие для вузов / Девянин П. Н. - 2-е изд. , испр. и доп. - Москва : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991203289.html (дата обращения: 24.01.2022). - Режим доступа : по подписке.

б) дополнительная литература

1. Дурнев В. Г. Методы комбинаторной теории групп в современной криптографии [Электронный ресурс]: учеб.-метод. пособие. / В. Г. Дурнев, О. В. Зеткина; Яросл. гос. ун-т. им. П. Г. Демидова - Ярославль: ЯрГУ, 2017. - 49 с. http://www.lib.uniyar.ac.ru/edocs/iuni/20170207.pdf
2. Дурнев, В. Г., Алгоритмические проблемы в комбинаторной теории групп [Электронный ресурс] : учебно-методическое пособие / В. Г. Дурнев, О. В. Зеткина ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2019, 53с http://www.lib.uniyar.ac.ru/edocs/iuni/20190203.pdf
3. Дурнев, В. Г., Дополнительные вопросы теории алгоритмов [Электронный ресурс] : учебно-методическое пособие / В. Г. Дурнев, О. В. Зеткина ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2020, 117с http://www.lib.uniyar.ac.ru/edocs/iuni/20200208.pdf

4. **в) ресурсы сети «Интернет»**

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
2. Электронно-библиотечная система «Юрайт https://www.biblio-online.ru/
3. Электронно-библиотечная система «Лань» http://e.lanbook.com/

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы) :

Доцент каф. КБ и ММОИ Чулкова В.С.

Приложение №1 к рабочей программе дисциплины
«Модели безопасности компьютерных систем»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

Типовые контрольные задания или иные материалы,
необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,
характеризующих этапы формирования компетенций

1. Контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Примеры заданий для самостоятельного решения или устного опроса по темам лекций

Тема **«Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем» (И-ПК-2.1)**

Задания для самостоятельного решения № 1.1 - 1.7 из параграфа 1.5 главы I учебника: Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2012. 320 с.

Тема **«Модели систем дискреционного разграничения доступа» (И-ПК-2.1, И-ПК-3.1)**

Задания для самостоятельного решения № 2.1 - 2.20 из параграфа 2.4 главы II учебника: Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2012. 320 с.

Тема **«Модели систем мандатного разграничения доступа» (И-ПК-2.1, И-ПК-3.1)**
Задания для самостоятельного решения № 4.1 - 4.11 из параграфа 4.4 главы IV учебника: Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2012. 320 с.

Тема **«Модели безопасности информационных потоков» (И-ПК-2.1, И-ПК-3.1)**

Задания для самостоятельного решения № 4.1 - 4.11 из параграфа 4.4 главы IV учебника: Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2012. 320 с.

Тема **«Модели безопасности информационных потоков» (И-ПК-2.1, И-ПК-3.1)**

Задания для самостоятельного решения № 5.1 - 5.12 из параграфа 5.5 главы V учебника: Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2012. 320 с.

Тема **«Модели ролевого разграничения доступа» (И-ПК-2.1, И-ПК-3.1)**

Задания для самостоятельного решения № 6.1 - 6.10 из параграфа 6.6 главы VI учебника: Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2012. 320 с.

Тема **«Субъектно-ориентированная модель изолированной программной среды» (И-ПК-2.1, И-ПК-3.1)**

Задания для самостоятельного решения № 3.1 - 3.14 из параграфа 3.4 главы III учебника: Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2012. 320 с.

Тема **«Критерии защищенности компьютерных систем» (И-ПК-3.2)**
Примеры контрольных вопросов и заданий:

- Описать концепцию Стандарта оценки безопасности компьютерных систем TCSEC («Оранжевая книга»)
- Описать концепцию Стандарта оценки безопасности компьютерных систем TCSEC («Оранжевая книга»)
- Описать концепцию Общих критериев безопасности информационных технологий (*Common Criteria*)
- Описать концепцию защиты КС и СВТ по руководящим документам ФСТЭК России
- Руководствуясь пользовательской документацией на СЗИ НСД Dallas Lock 8.0, описать, для защиты каких компьютерных систем может использоваться средство защиты и каким образом

2. Задания для практических занятий

В рамках обучения студентам могут быть предложены практические задания, которые также необходимы для оценки знаний и приобретения новых навыков. Примеры заданий:

- создать сеть Петри, отображающую принцип дискреционного управления доступом, в среде CPN Tools **(И-ПК-2.2)**;
- создать сеть Петри, отображающую принцип ролевого управления доступом, в среде CPN Tools **(И-ПК-2.2)**;
- создать сеть Петри, отображающую принцип ограничений ролевого управления доступом, в среде CPN Tools **(И-ПК-2.2)**.

3. Список вопросов и (или) заданий для проведения аттестации

Вопросы к экзамену по дисциплине «Модели безопасности компьютерных систем»

1. Модели систем дискреционного разграничения доступа
1.1. Модель матрицы доступов ХРУ
1.2. Модель распространения прав доступа Take-Grant

2. Модели систем мандатного разграничения доступа
2.1. Модель Белла—ЛаПадула
2.2. Модель систем военных сообщений

3. Модели безопасности информационных потоков
3.1. Автоматная модель безопасности информационных потоков

3.2. Программная модель контроля информационных потоков
3.3. Вероятностная модель безопасности информационных потоков

4. Модели ролевого разграничения доступа
4.1. Понятие ролевого разграничения доступа
4.2. Базовая модель РРД
4.3. Модель администрирования РРД
4.4. Модель мандатного РРД

5. Субъектно-ориентированная модель изолированной программной среды
5.1. Основные понятия
5.2 Базовая теорема ИПС

6. Проблемы применения моделей безопасности при построении защищенных компьютерных систем
6.1. Проблема адекватности реализации модели безопасности в реальной компьютерной системе
6.2. Обоснование политики безопасного администрирования ОС семейств Windows

Фонд оценочных средств для проведения текущей и промежуточной аттестации студентов по дисциплине «Модели безопасности компьютерных систем»

1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем
1.1. Элементы теории защиты информации
1.2. Математические основы моделей безопасности
1.3. Основные виды моделей безопасности

2. Модели систем дискреционного разграничения доступа
2.1. Модель матрицы доступов ХРУ
2.2. Модель распространения прав доступа Take-Grant

3. Модели систем мандатного разграничения доступа
3.1. Модель Белла—ЛаПадула
3.2. Модель систем военных сообщений

4. Модели безопасности информационных потоков
4.1. Автоматная модель безопасности информационных потоков
4.2. Программная модель контроля информационных потоков
4.3. Вероятностная модель безопасности информационных потоков

5. Модели ролевого разграничения доступа
5.1. Понятие ролевого разграничения доступа
5.2. Базовая модель РРД
5.3. Модель администрирования РРД
5.4. Модель мандатного РРД

6. Субъектно-ориентированная модель изолированной программной среды
6.1. Основные понятия
6.2 Базовая теорема ИПС

7. Основные критерии защищенности КС. Классы защищенности КС.
7.1. Основные критерии оценки защищенности КС

7.2. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»)
7.3. Концепция защиты КС и СВТ по руководящим документам ФСТЭК России
7.4. Общие критерии безопасности информационных технологий (Common Criteria)

8. Проблемы применения моделей безопасности при построении защищенных компьютерных систем
8.1. Проблема адекватности реализации модели безопасности в реальной компьютерной системе
8.2. Обоснование политики безопасного администрирования ОС семейств Windows

4. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

4.1.Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале.

Пороговый уровень предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень.

Высокий уровень предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень.

5. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

6. Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- полные и систематизированные знания в объеме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;

- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

7. Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка.

Оценка ответа на экзамене

Экзаменационный ответ оценивается по 4-х бальной системе, в соответствие с которой выставляются оценки ***«отлично», «хорошо», «удовлетворительно», «неудовлетворительно»***.

Правила выставления оценки:

оценка ***«отлично»*** выставляется студенту, если он владеет материалом дисциплины, четко отвечает на вопросы, имеет системный взгляд на материал дисциплины, способен разбирать более сложные предлагаемые ему случаи, не испытывает сложностей при решении практических заданий;

оценка ***«хорошо»*** выставляется студенту, если он твердо знает и понимает материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответах, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;

оценка ***«удовлетворительно»*** выставляется студенту, если он имеет знания основного материала, но не усвоил его деталей, знает дисциплину только в том виде, как она была ему преподана, но приходит в замешательство от сопутствующих и/или наводящих вопросов, испытывает затруднения при выполнении практических работ;

оценка ***«неудовлетворительно»*** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями и ошибками выполняет практические задания.

Приложение №2 к рабочей программе дисциплины
«Модели безопасности компьютерных систем»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Модели безопасности компьютерных систем» являются лекции, что связано, прежде всего, с достаточно высоким уровнем абстрактности изучаемых в курсе понятий. По большинству тем предусмотрены практические занятия, целью которых является закрепление лекционного материала путем решения специальным образом подобранных задач и упражнений.

Для успешного освоения дисциплины важно самостоятельное решение достаточно большого набора хорошо подобранных задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и основы математической логики. Для решения задач необходимо не только знать, но и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с конспектами лекций и рекомендованной литературой.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на практических занятиях и контрольной работы. Также проводятся консультации (при необходимости) по лекционному материалу и разбору некоторых заданий для самостоятельной работы.

В конце изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. Билеты формируются на основании списка вопросов к экзамену, который охватывает полностью всю программу дисциплины. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать учебную литературу, указанную в разделе 8.

Для подбора дополнительного материала рекомендуется использовать интернет-ресурсы:

1. Электронная библиотека учебных материалов ЯрГУ http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
2. Электронно-библиотечная система «Юрайт https://www.biblio-online.ru/
3. Электронно-библиотечная система «Лань» http://e.lanbook.com/

Допускается использование ресурсов habr.com, researchgate.net и иных подобных ресурсов.