МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Институт компьютерных наук и технологий

Авторы-составители: **Черников Арсений Викторович**

Рабочая программа дисциплины

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Код УМК 94461

Утверждено
Протокол №6
от «06» мая 2022 г.

Пермь, 2022

1. Наименование дисциплины

Модели безопасности компьютерных систем

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.01** Компьютерная безопасность

специализация Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Модели безопасности компьютерных систем** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

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

Индикаторы

ОПК.11.1 Ориентируется в существующих угрозах безопасности информации и требованиях по защите информации

ОПК.11.2 Ориентируется в политиках управления доступом и информационными потоками в компьютерных системах

ОПК.11.3 Самостоятельно создает политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации

4. Объем и содержание дисциплины

Специальность	10.05.01 Компьютерная безопасность (специализация: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	14
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (3) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (14 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Модели безопасности компьютерных систем

Входное тестирование

Проверяется умение применять аппарат математического анализа, дискретной математики, теории алгоритмов, математической статистики, теоретико-числовых методов

Основные элементы и понятия моделей безопасности компьютерных систем

Изучаются основные элементы и понятия теории компьютерной безопасности. Сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени. Модели ценности информации: порядковая шкала, решетка многоуровневой безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Понятие политики безопасности. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков.

Модели безопасности компьютерных систем

Изучаются основные модели безопасности компьютерных сетей

- Модели компьютерных систем с дискреционным управлением доступом.
- Модели компьютерных систем с мандатным управлением доступом.
- Модели компьютерных систем с ролевым управлением доступом.
- Модель администрирования ролевого управления доступом.

Анализ моделей безопасности компьютерных систем

Приводится сравнительная характеристика моделей и их методов анализа. Рассматриваются алгоритмы проверки безопасности, правила формирования и преобразования графов доступов и информационных потоков, примеры реализации запрещенных информационных потоков по памяти или по времени.

Итоговое контрольное мероприятие

Проводится письменное контрольное мероприятие для проверки полученных в ходе курса знаний.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 c. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/77317.html

2. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 c. — ISBN 978-5-4497-0946-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/102017.html

Дополнительная:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 c. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/97562

2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей:учебное пособие для студентов вузов/В. Ф. Шаньгин.-Москва:ИНФРА-М,2008, ISBN 978-5-8199-0331-5.-416.-Библиогр.: с. 401-408

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Модели безопасности компьютерных систем** предполагает использование следующего программного обеспечения и информационных справочных систем:
Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения практических занятий - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:
система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).
система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.
система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «AdobeAcrobatReader DC»;
- офисный пакет приложений «LibreOffice».

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:
1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными

компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Модели безопасности компьютерных систем

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

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 (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.11.2 Ориентируется в политиках управления доступом и информационными потоками в компьютерных системах	Знает нормативную документацию по информационной безопасности на уровне управления доступом и информационными потоками в компьютерных системах. Умеет ориентироваться в политиках управления доступом и информационными потоками в компьютерных системах.	**Неудовлетворител** Не знает нормативную документацию по информационной безопасности на уровне управления доступом и информационными потоками в компьютерных системах. Не умеет ориентироваться в политиках управления доступом и информационными потоками в компьютерных системах. **Удовлетворительн** Знает часть нормативной документации по информационной безопасности на уровне управления доступом и информационными потоками в компьютерных системах. Не умеет ориентироваться в политиках управления доступом и информационными потоками в компьютерных системах. **Хорошо** Знает нормативную документацию по информационной безопасности на уровне управления доступом и информационными потоками в компьютерных системах. Умеет частично ориентироваться в политиках управления доступом и информационными потоками в компьютерных системах. **Отлично** Знает нормативную документацию по информационной безопасности на уровне управления доступом и информационными потоками в компьютерных системах. Умеет ориентироваться в политиках управления доступом и информационными потоками в компьютерных системах.
ОПК.11.1 Ориентируется в существующих угрозах	Знает основные угрозы безопасности информации и требованиях по защите	**Неудовлетворител** Не знает основные угрозы безопасности информации и требованиях по защите

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
безопасности информации и требованиях по защите информации	информации. Умеет ориентироваться в существующих угрозах безопасности информации и требованиях по защите информации.	**Неудовлетворител** информации. Не умеет ориентироваться в существующих угрозах безопасности информации и требованиях по защите информации. **Удовлетворительн** Знает часть основных угроз безопасности информации и требованиях по защите информации. Не умеет ориентироваться в существующих угрозах безопасности информации и требованиях по защите информации. **Хорошо** Знает основные угрозы безопасности информации и требованиях по защите информации. Частично умеет ориентироваться в существующих угрозах безопасности информации и требованиях по защите информации. **Отлично** Знает основные угрозы безопасности информации и требованиях по защите информации. Умеет ориентироваться в существующих угрозах безопасности информации и требованиях по защите информации.
ОПК.11.3 Самостоятельно создает политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	Знает нормативные документы по разработке политики безопасности, политики управления доступом и информационными потоками в компьютерных системах. Умеет самостоятельно создавать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.	**Неудовлетворител** Не знает нормативные документы по разработке политики безопасности, политики управления доступом и информационными потоками в компьютерных системах. Не умеет самостоятельно создавать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации. **Удовлетворительн** Знает часть нормативные документы по разработке политики безопасности, политики управления доступом и информационными потоками в компьютерных системах. Не умеет самостоятельно создавать политики

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации. **Хорошо** Знает нормативные документы по разработке политики безопасности, политики управления доступом и информационными потоками в компьютерных системах. Частично умеет самостоятельно создавать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации. **Отлично** Знает нормативные документы по разработке политики безопасности, политики управления доступом и информационными потоками в компьютерных системах. Умеет самостоятельно создавать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Экзамен
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 48 до 60
«неудовлетворительно» / «незачтено» менее 48 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль **ОПК.11.1** Ориентируется в существующих угрозах безопасности информации и требованиях по защите информации **ОПК.11.3** Самостоятельно создает политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации **ОПК.11.2** Ориентируется в политиках управления доступом и информационными потоками в компьютерных системах	Входное тестирование **Входное тестирование**	Остаточные знания

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.11.1 Ориентируется в существующих угрозах безопасности информации и требованиях по защите информации **ОПК.11.3** Самостоятельно создает политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации **ОПК.11.2** Ориентируется в политиках управления доступом и информационными потоками в компьютерных системах	Основные элементы и понятия моделей безопасности компьютерных систем **Защищаемое контрольное мероприятие**	Элементы теории защиты информации, математические основы моделей безопасности, Основные виды моделей безопасности
ОПК.11.1 Ориентируется в существующих угрозах безопасности информации и требованиях по защите информации **ОПК.11.3** Самостоятельно создает политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации **ОПК.11.2** Ориентируется в политиках управления доступом и информационными потоками в компьютерных системах	Модели безопасности компьютерных систем **Защищаемое контрольное мероприятие**	-модели систем дискреционного разграничения доступа-модели систем мандатного разграничения доступа -модели безопасности информационных потоков-модели ролевого разграничения доступа

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.11.1 Ориентируется в существующих угрозах безопасности информации и требованиях по защите информации **ОПК.11.3** Самостоятельно создает политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации **ОПК.11.2** Ориентируется в политиках управления доступом и информационными потоками в компьютерных системах	Анализ моделей безопасности компьютерных систем **Защищаемое контрольное мероприятие**	-алгоритмы проверки безопасности -правила формирования и преобразования графов доступов и информационных потоков-примеры реализации запрещенных информационных потоков по памяти или по времени- проблемы применения моделей безопасности при построении защищенных компьютерных систем - проблема адекватности реализации модели безопасности в реальной компьютерной системе- проблемы реализации политики безопасности
ОПК.11.1 Ориентируется в существующих угрозах безопасности информации и требованиях по защите информации **ОПК.11.3** Самостоятельно создает политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации **ОПК.11.2** Ориентируется в политиках управления доступом и информационными потоками в компьютерных системах	Итоговое контрольное мероприятие **Итоговое контрольное мероприятие**	Комплексный тест по всем темам, изученным в ходе данной дисциплины.

Спецификация мероприятий текущего контроля

Входное тестирование

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

Показатели оценивания	Баллы
Прохождение контроля.	1

Основные элементы и понятия моделей безопасности компьютерных систем

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**
Проходной балл: **12**

Показатели оценивания	Баллы
Основные виды моделей безопасности	12
Элементы теории защиты информации	10
Математические основы моделей безопасности	8

Модели безопасности компьютерных систем

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**
Проходной балл: **12**

Показатели оценивания	Баллы
Модели безопасности информационных потоков, автоматная модель безопасности информационных потоков, программная модель контроля информационных потоков	5
Модели ролевого разграничения доступа, понятие ролевого разграничения доступа, базовая модель РРД, модель администрирования РРД	5
Субъектно-ориентированная модель изолированной программной среды, основные понятия. Монитор безопасности объектов, монитор безопасности субъектов	5
Модели систем мандатного разграничения доступа, модель Белла—ЛаПадула, модель систем военных сообщений	5
Модели систем дискреционного разграничения доступа, Модель матрицы доступов ХРУ, Модель распространения прав доступа Take-Grant	5

Анализ моделей безопасности компьютерных систем

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**
Проходной балл: **12**

Показатели оценивания	Баллы
Примеры реализации запрещенных информационных потоков по памяти или по времени.	5
Проблемы применения моделей безопасности при построении защищенных компьютерных систем, примеры реализации запрещенных информационных потоков по памяти или по времени.	5
Правила формирования и преобразования графов доступов и информационных потоков.	5

Проблемы применения моделей безопасности при построении защищенных компьютерных систем.	5
Алгоритмы проверки безопасности.	5

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**
Проходной балл: **12**

Показатели оценивания	Баллы
Знает и умеет использовать модели безопасностей компьютерных систем, может проводить их анализ и строить собственные модели.	10
Знает и умеет использовать модели безопасностей компьютерных систем, может проводить их анализ.	10
Знает и умеет использовать модели безопасностей компьютерных систем.	5