**МИНОБРНАУКИ РОССИИ**

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

**Кафедра информационной безопасности и систем связи**

Авторы-составители: **Шкарапута Александр Петрович**
**Лобков Армандо Львович**
**Черников Арсений Викторович**
**Мустакимова Яна Романовна**

Рабочая программа дисциплины

# МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Код УМК 93162

Утверждено
Протокол №6
от «26» июня 2020 г.

Пермь, 2020

## 1. Наименование дисциплины

Модели безопасности компьютерных систем

## 2. Место дисциплины в структуре образовательной программы

Дисциплина входит в вариативную 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)

**ПК.14** способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения

**ПК.5** Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

**ПК.9** Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем

## 4. Объем и содержание дисциплины

| | |
|---|---|
| **Направления подготовки** | 10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения) |
| **форма обучения** | очная |
| **№№ триместров, выделенных для изучения дисциплины** | 11 |
| **Объем дисциплины (з.е.)** | 3 |
| **Объем дисциплины (ак.час.)** | 108 |
| **Контактная работа с преподавателем (ак.час.), в том числе:** | 42 |
| **Проведение лекционных занятий** | 28 |
| **Проведение практических занятий, семинаров** | 14 |
| **Самостоятельная работа (ак.час.)** | 66 |
| **Формы текущего контроля** | Защищаемое контрольное мероприятие (2)<br>Итоговое контрольное мероприятие (1) |
| **Формы промежуточной аттестации** | Зачет (11 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 // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/97562

2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей:учеб. пособие для студентов вузов/В. Ф. Шаньгин.-М.:ИНФРА-М,2008, ISBN 978-5-8199-0331-5.-416.-Библиогр.: с. 401408

## 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:
- 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».

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

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.

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 и критерии их оценивания**

| Компетенция | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| **ПК.5**<br>Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций | Знать основы информационной безопасности. Уметь осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем. Владеть навыками обработки результатов проведенных исследований. | **Неудовлетворител**<br>Не знает основные элементы и понятия теории компьютерной безопасности.<br>**Удовлетворительн**<br>Знает основные элементы и понятия теории компьютерной безопасности.<br>**Хорошо**<br>Знает основные элементы и понятия теории компьютерной безопасности. Модели ценности информации.<br>Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков.<br>При ответах допускает несущественные ошибки.<br>**Отлично**<br>Знает основные элементы и понятия теории компьютерной безопасности. Модели ценности информации.<br>Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков.<br>Хорошо ориентируется в изученном материале и показывает его понимание. |
| **ПК.14**<br>способность обосновывать правильность выбранной модели решения профессиональной | Знать типовые модели решения профессиональной задачи. Уметь обосновывать правильность выбранной модели решения профессиональной задачи. Владеть навыками анализа | **Неудовлетворител**<br>не знает даже двух типов модели безопасности компьютерных систем из представленных<br>- Модели компьютерных систем с дискреционным управлением доступом.<br>- Модели компьютерных систем с |

| Компетенция | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| задачи, сопоставлять экспериментальные данные и теоретические решения | экспериментальных и теоретических данных. | **Неудовлетворител**<br>мандатным управлением доступом.<br>- Модели компьютерных систем с ролевым управлением доступом.<br>- Модель администрирования ролевого управления доступом.<br><br>Допускает существенные ошибки в ответах.<br>**Удовлетворительн**<br>Знает не менее двух типов моделей:<br>- Модели компьютерных систем с дискреционным управлением доступом.<br>- Модели компьютерных систем с мандатным управлением доступом.<br>- Модели компьютерных систем с ролевым управлением доступом.<br>- Модель администрирования ролевого управления доступом.<br>Допускает существенные ошибки в ответах.<br>**Хорошо**<br>Знает<br>- Модели компьютерных систем с дискреционным управлением доступом.<br>- Модели компьютерных систем с мандатным управлением доступом.<br>- Модели компьютерных систем с ролевым управлением доступом.<br>- Модель администрирования ролевого управления доступом.<br>Делает несущественные ошибки в ответах.<br>**Отлично**<br>Знает<br>- Модели компьютерных систем с дискреционным управлением доступом.<br>- Модели компьютерных систем с мандатным управлением доступом.<br>- Модели компьютерных систем с ролевым управлением доступом.<br>- Модель администрирования ролевого управления доступом.<br>Хорошо понимает материал и ориентируется в нем |
| **ПК.9**<br>Способность проводить анализ проектных | Знать основы информационной безопасности компьютерных систем. Уметь проводить | **Неудовлетворител**<br>Не умеет анализировать модели систем компьютерной безопасности |

| Компетенция | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| решений по обеспечению информационной безопасности компьютерных систем | анализ проектных решений по обеспечению информационной безопасности компьютерных систем. Владеть навыками анализа проектных решений по обеспечению информационной безопасности компьютерных систем. | **Удовлетворительн**<br>Умеет анализировать модели систем компьютерной безопасности. Знает<br>- Алгоритмы проверки безопасности.<br>- Правила формирования и преобразования графов доступов и информационных потоков.<br>- Примеры реализации запрещенных информационных потоков по памяти или по времени.<br>Может делать ошибки в ответах.<br>**Хорошо**<br>Умеет анализировать модели систем компьютерной безопасности. Знает<br>- Алгоритмы проверки безопасности.<br>- Правила формирования и преобразования графов доступов и информационных потоков.<br>- Примеры реализации запрещенных информационных потоков по памяти или по времени.<br>Делает несущественные ошибки в ответах<br>**Отлично**<br>Умеет анализировать модели систем компьютерной безопасности. Знает<br>- Алгоритмы проверки безопасности.<br>- Правила формирования и преобразования графов доступов и информационных потоков.<br>- Примеры реализации запрещенных информационных потоков по памяти или по времени.<br>Хорошо понимает материал и ориентируется в нем. |

## Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

**Вид мероприятия промежуточной аттестации :** Зачет
**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 46 до 60
**«неудовлетворительно» / «незачтено»** менее 46 балла

| Компетенция | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|---|---|
| **ПК.5** Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций | Основные элементы и понятия моделей безопасности компьютерных систем **Защищаемое контрольное мероприятие** | Элементы теории защиты информации, математические основы моделей безопасности, Основные виды моделей безопасности |
| **ПК.9** Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем | 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 |

| Компетенция | Мероприятие текущего контроля | Контролируемые элементы результатов обучения |
|---|---|---|
| **ПК.14** способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения | итоговое контрольное мероприятие **Итоговое контрольное мероприятие** | Комплексный тест по всем темам, изученным в ходе данной дисциплины |

## Спецификация мероприятий текущего контроля

### 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: **30**
Проходной балл: **15**

| Показатели оценивания | Баллы |
|---|---|
| Основные виды моделей безопасности | 12 |
| Математические основы моделей безопасности | 8 |
| Элементы теории защиты информации | 5 |

### Анализ 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: **30**
Проходной балл: **13**

| Показатели оценивания | Баллы |
|---|---|
| - проблемы применения моделей безопасности при построении защищенных компьютерных систем-примеры реализации запрещенных информационных потоков по памяти или по времени | 10 |
| -правила формирования и преобразования графов доступов и информационных потоков | 5 |
| - проблемы применения моделей безопасности при построении защищенных компьютерных систем | 5 |
| -алгоритмы проверки безопасности | 5 |
| -примеры реализации запрещенных информационных потоков по памяти или по времени | 5 |

### итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **18**

| **Показатели оценивания** | **Баллы** |
|---|---|
| знает и умеет использовать модели безопасностей компьютерных систем, может проводить их анализ и строить собственные модели | 20 |
| знает и умеет использовать модели безопасностей компьютерных систем, может проводить их анализ | 15 |
| знает и умеет использовать модели безопасностей компьютерных систем | 9 |