

**МИНОБРНАУКИ РОССИИ**

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

**Кафедра информационной безопасности и систем связи**

Авторы-составители: **Черников Арсений Викторович**

Рабочая программа дисциплины

**МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ**

Код УМК 94461

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 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)

**ПК.10** Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

**ПК.11** способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

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

**ПК.15** Способность оценивать эффективность системы защиты информации в компьютерных системах

**ПК.3** Способность к анализу и формализации поставленных задач в области информационной безопасности

**ПК.6** Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

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

#### 4. Объем и содержание дисциплины

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

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 выполнении 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-образовательную 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**

**ПК.3**

**Способность к анализу и формализации поставленных задач в области информационной безопасности**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ПК.3</b> Способность к анализу и формализации поставленных задач в области информационной безопасности	Знает методики формализации и анализа задач различного уровня в области информационной безопасности. Умеет анализировать и формализовать поставленные задачи в области информационной безопасности. Владеет навыками формализации исходной задачи в области информационной безопасности.	<p align="center"><b>Неудовлетворител</b></p> <p>Не умеет анализировать и формализовать поставленные задачи в области информационной безопасности.</p> <p align="center"><b>Удовлетворительн</b></p> <p>Умеет с большими затруднениями анализировать и формализовать поставленные задачи в области информационной безопасности.</p> <p align="center"><b>Хорошо</b></p> <p>Умеет с небольшими затруднениями анализировать и формализовать поставленные задачи в области информационной безопасности.</p> <p align="center"><b>Отлично</b></p> <p>Умеет без затруднений анализировать и формализовать поставленные задачи в области информационной безопасности.</p>

**ПК.14**

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

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ПК.14</b> способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения	Знает основы информационной безопасности. Умеет обосновывать правильность выбранной модели решения профессиональной задачи. Владеет навыками анализа экспериментальных данных и теоретических решений.	<p align="center"><b>Неудовлетворител</b></p> <p>Не умеет обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения.</p> <p align="center"><b>Удовлетворительн</b></p> <p>Умеет с большими затруднениями обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения.</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;"><b>Хорошо</b></p> <p>Умеет с небольшими затруднениями обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Умеет без затруднений обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения.</p>

**ПК.11**

**способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПК.11</b> способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p>	<p>Знает основы информационной безопасности. Знает методики оценки степени надежности информационных систем. Умеет оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи. Владеет навыками эксплуатации механизмов обеспечения информационной безопасности.</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не умеет оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи.</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Умеет с большими затруднениями оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Умеет с небольшими затруднениями оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Умеет без затруднений оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи.</p>

**ПК.15**

**Способность оценивать эффективность системы защиты информации в компьютерных системах**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПК.15</b></p>	<p>Знает основы информационной</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
Способность оценивать эффективность системы защиты информации в компьютерных системах	безопасности. Знает методики оценки эффективности систем защиты информации. Умеет оценивать эффективность системы защиты информации в компьютерных системах.	<p><b>Неудовлетворител</b> Не умеет оценивать эффективность системы защиты информации в компьютерных системах.</p> <p><b>Удовлетворительн</b> Умеет с большими затруднениями оценивать эффективность системы защиты информации в компьютерных системах.</p> <p><b>Хорошо</b> Умеет с небольшими затруднениями оценивать эффективность системы защиты информации в компьютерных системах.</p> <p><b>Отлично</b> Умеет без затруднений оценивать эффективность системы защиты информации в компьютерных системах.</p>

### ПК.9

#### Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПК.9</b> Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем</p>	Знает основы информационной безопасности. Знает методики разработки проектных решений и их анализа. Умеет проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем.	<p><b>Неудовлетворител</b> Не умеет проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем.</p> <p><b>Удовлетворительн</b> Умеет с большими затруднениями проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем.</p> <p><b>Хорошо</b> Умеет с небольшими затруднениями проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем.</p> <p><b>Отлично</b> Умеет без затруднений проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем.</p>

## ПК.6

### Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<b>ПК.6</b> Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем	Знает основы информационной безопасности. Знает математические модели, на которых построены и рассчитываются системы безопасности. Умеет применять математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем.	<b>Неудовлетворител</b> Не умеет разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. <b>Удовлетворительн</b> Умеет с большими затруднениями разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. <b>Хорошо</b> Умеет с небольшими затруднениями разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. <b>Отлично</b> Умеет без затруднений разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем.

## ПК.10

### Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<b>ПК.10</b> Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели	Знает основы информационной безопасности организаций. Умеет разрабатывать системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы. Владеет навыками разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в	<b>Неудовлетворител</b> Не умеет участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах. <b>Удовлетворительн</b> Умеет с большими затруднениями участвовать в разработке системы защиты

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	компьютерных системах.	<p style="text-align: center;"><b>Удовлетворительн</b></p> <p>информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Умеет с небольшими затруднениями участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Умеет без затруднений участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.</p>

## 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
<b>Входной контроль</b>	Входное тестирование <b>Входное тестирование</b>	Остаточные знания
<b>ПК.3</b> Способность к анализу и формализации поставленных задач в области информационной безопасности	Основные элементы и понятия моделей безопасности компьютерных систем <b>Защищаемое контрольное мероприятие</b>	Элементы теории защиты информации, математические основы моделей безопасности, Основные виды моделей безопасности
<b>ПК.6</b> Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем <b>ПК.9</b> Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем <b>ПК.14</b> способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения	Модели безопасности компьютерных систем <b>Защищаемое контрольное мероприятие</b>	-модели систем дискреционного разграничения доступа-модели систем мандатного разграничения доступа -модели безопасности информационных потоков-модели ролевого разграничения доступа

<b>Компетенция (индикатор)</b>	<b>Мероприятие текущего контроля</b>	<b>Контролируемые элементы результатов обучения</b>
<p><b>ПК.10</b> Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p><b>ПК.11</b> способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p> <p><b>ПК.15</b> Способность оценивать эффективность системы защиты информации в компьютерных системах</p>	<p>Анализ моделей безопасности компьютерных систем</p> <p><b>Защищаемое контрольное мероприятие</b></p>	<p>-алгоритмы проверки безопасности</p> <p>-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 -</p> <p>проблема адекватности реализации модели безопасности в реальной компьютерной системе- проблемы реализации политики безопасности</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.3</b> Способность к анализу и формализации поставленных задач в области информационной безопасности</p> <p><b>ПК.6</b> Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем</p> <p><b>ПК.9</b> Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем</p> <p><b>ПК.10</b> Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p><b>ПК.11</b> способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p> <p><b>ПК.14</b> способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения</p> <p><b>ПК.15</b> Способность оценивать</p>	<p>Итоговое контрольное мероприятие</p> <p><b>Итоговое контрольное мероприятие</b></p>	<p>Комплексный тест по всем темам, изученным в ходе данной дисциплины.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
эффективность системы защиты информации в компьютерных системах		

### 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**

<b>Показатели оценивания</b>	<b>Баллы</b>
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**

<b>Показатели оценивания</b>	<b>Баллы</b>
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