

МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Черепанов Иван Николаевич
Лунегов Алексей Игоревич**

Рабочая программа дисциплины
БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ
Код УМК 68659

Утверждено
Протокол №4
от «24» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Безопасность операционных систем

2. Место дисциплины в структуре образовательной программы

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

Специальность: **10.05.03** Информационная безопасность автоматизированных систем
специализация Безопасность открытых информационных систем

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Безопасность операционных систем** у обучающегося должны быть сформированы следующие компетенции:

10.05.03 Информационная безопасность автоматизированных систем (специализация : Безопасность открытых информационных систем)

ОПК.2 Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Индикаторы

ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности

ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы

ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

4. Объем и содержание дисциплины

Направления подготовки	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	9
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (3) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (9 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Безопасность операционных систем.Первый семестр

Архитектура операционных систем

Рассматривается история возникновения информационных систем в целом и операционных систем в частности. Изучается устройство IBM- совместимых компьютеров и требования к архитектуре ОС.

Концептуальные основы операционных систем

Рассматриваются основы операционных систем: основные требования, функции и задачи.

Понятие управления задачами

Рассматриваются проблемы управления задачами в операционной системе, основные принципы мультизадачности. Изучаются методы долгосрочного и краткосрочного планирования

Управление памятью в операционных системах

Рассматриваются вопросы управления оперативной памятью в операционной системе. Вводятся понятия основной и внешней памяти. Изучаются вопросы размещения данных в оперативной памяти: сегментное и страничное представления. Изучается понятие виртуальной памяти.

Управление файлами и вводом-выводом в операционных системах

Изучаются вопросы управления внешними хранилищами. Рассматривается принцип работы устройств внешнего хранения на примере жестких дисков. Рассматриваются вопросы файловой системы. Рассматриваются наиболее распространенные файловые системы fat32, NTFS, ext4.

Основные понятия и положения защиты информации в информационно-вычислительных системах

Рассматриваются основные понятия и положения защиты информации в информационно-вычислительных системах. Изучаются требования информационным системам с точки зрения разных классов безопасности. Изучаются механизмы операционных систем позволяющие управлять информационной безопасностью.

Угрозы безопасности информации в информационно-вычислительных системах

Рассматриваются основные источники угроз информационной безопасности, проводится их классификация. Приводится примерная статистика по актуальности тех или иных угроз.

Программно-технический уровень информационной безопасности

Рассматриваются все уровни информационной безопасности, законодательный, административный, программно-технический. определяются круг задач решаемый на Программно-техническом уровне, показываются границы его зоны ответственности.

Модели безопасности основных операционных систем

Рассматриваются модели безопасности основных операционных систем на примере Windows и GNU/Linux

Системы защиты программного обеспечения

Изучаются проблема защиты программного обеспечения. Рассматриваются вопросы авторского права и пиратства. Приводятся примеры существующих средств защиты ПО, изучаются их стойкости и преимущества разных подходов

Итоговое контрольное мероприятие

Итоговое контрольное мероприятие проводится в виде экзамена

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. Гостев, И. М. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/453469>
2. Курячий, Г. В. Операционная система Linux. Курс лекций : учебное пособие / Г. В. Курячий, К. А. Маслинский. — 2-е изд. — Саратов : Профобразование, 2019. — 348 с. — ISBN 978-5-4488-0110-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт] <http://www.iprbookshop.ru/88000.html>

Дополнительная:

1. Мезенцева, Е. М. Операционные системы : лабораторный практикум / Е. М. Мезенцева, О. С. Коняева, С. В. Малахов. — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2017. — 214 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/75395.html>
2. Технология открытых систем/под общ. ред. А. Я. Олейникова.-М.:Янус-К,2004, ISBN 5-8037-0203-X.- 288.-Библиогр. в конце глав

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<http://www.iso27000.ru/> Безопасность операционных систем. Читальный зал

https://intuit.ru/studies/professional_retraining/962/courses/497/lecture/11268 Безопасность операционных систем курс лекций

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

Образовательный процесс по дисциплине **Безопасность операционных систем** предполагает использование следующего программного обеспечения и информационных справочных систем:

- презентационные материалы (слайды по темам лекционных занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).

Перечень используемого программного обеспечения:

- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель);
- программа просмотра интернет контента (браузер).

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 проведения лекционных занятий:

Аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.

Для проведения лабораторных занятий – Компьютерный класс, оснащенный персональными ЭВМ и соответствующим программным обеспечением. Состав оборудования определен в Паспорте Компьютерного класса.

Аудитории для проведения текущего контроля;

Компьютерный класс, оснащенный персональными ЭВМ и соответствующим программным обеспечением. Состав оборудования определен в Паспорте компьютерного класса.

Аудитории для групповых (индивидуальных) консультаций;

Аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.

Аудитория для самостоятельной работы:

Аудитория оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченная 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
Безопасность операционных систем**

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

ОПК.2

Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности</p>	<p>Знать основные положения и концепции в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности.</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Отсутствие знаний основных положений и концепций в области программирования, архитектуры языков программирования, основных терминологий и базовых алгоритмов, основных требований информационной безопасности Отсутствие умений основных положений и концепций в области программирования, архитектуры языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности Не владение навыками основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности</p> <p style="text-align: center;">Удовлетворительн</p> <p>Общие, но не структурированные знания основных положений и концепций в области программирования, архитектуры языков программирования, основных терминологий и базовых алгоритмов, основных требований информационной безопасности Частично сформированное умение основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности Частичное владение навыками основных положений и концепций в области программирования, архитектуру языков</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Удовлетворительн</p> <p>программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности</p> <p style="text-align: center;">Хорошо</p> <p>Сформированные, но содержащие отдельные пробелы положений и концепций в области программирования, архитектуры языков программирования, основных терминологий и базовых алгоритмов, основных требований информационной безопасности</p> <p>В целом успешные, но содержащие отдельные пробелы основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности</p> <p>В целом успешные, но содержащие отдельные пробелы основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности</p> <p style="text-align: center;">Отлично</p> <p>Сформированные систематические знания основных положений и концепций в области программирования, архитектуры языков программирования, основных терминологий и базовых алгоритмов, основных требований информационной безопасности</p> <p>Сформированное умение разрабатывать основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности</p> <p>Сформированное владение навыками основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично информационной безопасности

ПК.29

способность администрировать подсистему информационной безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы	знать принципы администрирования автоматизированных систем, уметь администрировать подсистему информационной безопасности автоматизированной системы, владеть навыками контроля безопасности автоматизированной системы	<p>Неудовлетворител Отсутствие знаний по администрированию подсистем информационной безопасности автоматизированной системы</p> <p>Удовлетворительн Общие, но не структурированные знания принципов администрирования автоматизированных систем, частично сформированное умение администрировать подсистему информационной безопасности автоматизированной системы, посредственное владение навыками контроля безопасности автоматизированной системы</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания принципов администрирования автоматизированных систем, сформированное, но содержащие отдельные пробелы умение администрировать подсистему информационной безопасности автоматизированной системы, неуверенное владение навыками контроля безопасности автоматизированной системы</p> <p>Отлично Сформированные знания принципов администрирования автоматизированных систем, сформированное умение администрировать подсистему информационной безопасности автоматизированной системы, уверенное владение навыками контроля безопасности автоматизированной системы</p>

ПК.30

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	знать частные политик информационной безопасности автоматизированной системы, уметь проводить мониторинг безопасности автоматизированной системы	Неудовлетворител Отсутствие знаний связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы Удовлетворительн Общие, но не структурированные знания связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы Хорошо Сформированные, но содержащие отдельные пробелы знания связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы Отлично Сформированные систематические знания связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

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	Архитектура операционных систем Входное тестирование	Проверяются знания в области информационной безопасности
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Понятие управления задачами Защищаемое контрольное мероприятие	Подсистема безопасности Windows, права доступ, шифрованная файловая система.
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Основные понятия и положения защиты информации в информационно - вычислительных системах Защищаемое контрольное мероприятие	Настройка резервных копий файлов и восстановление системы

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Модели безопасности основных операционных систем Защищаемое контрольное мероприятие	Проверяется умение провести контроль целостности системы, восстановить систему после сбоя, а также восстановить пароль администратора.
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Итоговое контрольное мероприятие Итоговое контрольное мероприятие	Знание основных концепций построения операционных систем и механизмов обеспечения информационной безопасности.

Спецификация мероприятий текущего контроля

Архитектура операционных систем

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

Показатели оценивания	Баллы
За каждый правильный ответ в тексте	5

Понятие управления задачами

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **25**

Проходной балл: **10.8**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	30
В ходе выполнения задания были допущены незначительные ошибки	17
В ходе выполнения задания были допущены существенные ошибки и понадобилась помощь преподавателя	13
Задание не выполнено	

	0

Основные понятия и положения защиты информации в информационно - вычислительных системах

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	10
В ходе выполнения задания допущены незначительные ошибки	7
В ходе выполнения задания допущены существенные ошибки или понадобилась помощь преподавателя	5
Задание не выполнено	0

Модели безопасности основных операционных систем

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **10**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	20
В ходе выполнения задания были допущены незначительные ошибки	13
В ходе выполнения задания были допущены существенные ошибки и понадобилась помощь преподавателя	10
Задание не выполнено	0

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **45**

Проходной балл: **22.5**

Показатели оценивания	Баллы
Уверенные ответ на каждый из двух вопросов экзаменационный вопрос в билете	25
Уверенные ответы на каждый дополнительный вопрос	20