

МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

**Авторы-составители: Лунегов Игорь Владимирович
Черепанов Иван Николаевич**

Рабочая программа дисциплины
БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ
Код УМК 81651

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 базовую часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.03** Информационная безопасность автоматизированных систем
направленность 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 (направленность : Безопасность открытых информационных систем)

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	7
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 практических занятий, семинаров	0
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (5) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (7 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Безопасность операционных систем. Первый семестр

Введение

Предмет и задачи курса. Осваиваются первичные навыки администрирования операционных систем.

Основы безопасности информационных систем

Предмет и задачи курса. Осваиваются первичные навыки администрирования операционных систем.

Безопасность файловых систем

Рассматриваются вопросы разграничения доступа к объектам файловой системы в NTFS и EXT2,

Безопасность NTFS

Рассматриваются вопросы разграничения доступа к объектам файловой системы в NTFS.

Безопасность EXT2

Рассматриваются вопросы разграничения доступа к объектам файловой системы в EXT2.

Повышение надежности информационных систем

Рассматриваются некоторые методы обеспечения требуемого уровня отказоустойчивости автоматизированных систем реализуемые средствами современных операционных систем. Резервное копирование данных. Резервное копирование системного ПО. Автоматизированная установка и первичная настройка. Восстановления работоспособности.

Отказоустойчивость системного ПО

Рассматриваются некоторые методы обеспечения требуемого уровня отказоустойчивости автоматизированных систем реализуемые средствами современных операционных систем. Резервное копирование данных. Резервное копирование системного ПО. Автоматизированная установка и первичная настройка. Восстановления работоспособности.

Безопасность операционных систем

Рассматриваются механизмы обеспечивающие безопасность как самих операционных систем Windows и Linux, так и выполняемых в их среде процессов. Основной функционал. Порядок организации администрирования. Организация мониторинга их функционирования. Систематизируются знания и умения полученные в ходе курса. Формируются навыки регламентирования настроек механизмов обеспечивающих безопасность в современных операционных системах.

Механизмы безопасности операционных систем семейства Windows

Рассматриваются механизмы обеспечивающие безопасность как самих операционных систем Windows так и выполняемых в их среде процессов. Основной функционал. Порядок организации администрирования. Организация мониторинга их функционирования.

Механизмы безопасности операционных систем семейства Linux

Рассматриваются механизмы обеспечивающие безопасность как самих операционных систем Linux, так и выполняемых в их среде процессов. Основной функционал. Порядок организации администрирования. Организация мониторинга их функционирования.

Регламентирование настроек безопасности операционных систем

Систематизируются знания и умения полученные в ходе курса. Формируются навыки регламентирования настроек механизмов обеспечивающих безопасность в современных операционных системах.

Системы защиты программного обеспечения

Механизмы защиты программного обеспечения в автоматизированных системах. Администрирование.
Контроль доступа.

Итоговое контрольное мероприятие

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. Курячий, Г. В. Операционная система UNIX : учебное пособие / Г. В. Курячий. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 258 с. — ISBN 978-5-4497-0670-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/97557>
2. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/451231>

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. Староверова, Н. А. Операционные системы : учебное пособие / Н. А. Староверова, Э. П. Ибрагимова. — Казань : Казанский национальный исследовательский технологический университет, 2016. — 312 с. — ISBN 978-5-7882-2046-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/79444.html>

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

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:

1. Проигрыватели виртуальных машин VirtualBox и VMWare Player (VMware Workstation).
2. Доступ к сети Интернет на всех компьютерах.
3. Доступ к подписке Microsoft Imagine Premium, либо любого иной легальной возможности устанавливать экземпляры операционной системы Windows в виртуальной среде.

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

1. Персональные компьютеры студентов по количеству студентов в обучаемой группе с:
 - производительностью процессора не хуже чем производительность старшего процессора семейства Intel i5 последнего или предпоследнего поколения;
 - объемом оперативной памяти не менее чем 8 ГБ;
 - не менее чем 500 ГБ доступного пространства на жестком диске;
 - установленной операционной системой Windows 8.1 или Windows 10 версии Pro.
2. Компьютер преподавателя с характеристиками аналогичными характеристикам компьютеров студентов подключенный к проекционному оборудованию. Желательно наличие интерактивной доски.

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 и
критерии их оценивания**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p>	<p>знать частные политики информационной безопасности автоматизированной системы; уметь осуществлять мониторинг безопасности автоматизированной системы</p>	<p align="center">Неудовлетворител Отсутствие знаний связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p> <p align="center">Удовлетворительн Общие, но не структурированные знания связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p> <p align="center">Хорошо Сформированные, но содержащие отдельные пробелы знания связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p> <p align="center">Отлично Сформированные систематические знания связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p>
<p>ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы</p>	<p>знать принципы администрирования автоматизированных систем, уметь администрировать подсистему информационной безопасности автоматизированной системы, владеть навыками контроля безопасности автоматизированной системы</p>	<p align="center">Неудовлетворител Отсутствие знаний по администрированию подсистем информационной безопасности автоматизированной системы</p> <p align="center">Удовлетворительн Общие, но не структурированные знания принципов администрирования автоматизированных систем, частично сформированное умение администрировать подсистему информационной безопасности</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Удовлетворительн</p> <p>автоматизированной системы, посредственное владение навыками контроля безопасности автоматизированной системы</p> <p style="text-align: center;">Хорошо</p> <p>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 style="text-align: center;">Отлично</p> <p>Сформированные знания принципов администрирования автоматизированных систем, сформированное умение администрировать подсистему информационной безопасности автоматизированной системы, уверенное владение навыками контроля безопасности автоматизированной системы</p>

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 44 до 60

«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Основы безопасности информационных систем Входное тестирование	Знания и умения контролируемые входным контролем
ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	Безопасность NTFS Защищаемое контрольное мероприятие	Умение решать практически задачи обеспечения безопасности автоматизированных систем используя механизмы разграничения доступа файловой системы NTFS
ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	Безопасность EXT2 Защищаемое контрольное мероприятие	Умение решать практически задачи обеспечения безопасности автоматизированных систем используя механизмы разграничения доступа файловой системы EXT2

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p>	<p>Отказоустойчивость системного ПО Защищаемое контрольное мероприятие</p>	<p>Умение обеспечивать отказоустойчивость автоматизированных систем</p>
<p>ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p>	<p>Механизмы безопасности операционных систем семейства Windows Защищаемое контрольное мероприятие</p>	<p>Умение решать практически задачи обеспечения безопасности автоматизированных систем используя механизмы групповых политик и политик безопасности Windows</p>
<p>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</p>	<p>Механизмы безопасности операционных систем семейства Linux Защищаемое контрольное мероприятие</p>	<p>знать основные механизмы безопасности современных операционных систем; знать основные принципы функционирования этих механизмов; уметь администрировать и осуществлять мониторинг основных механизмов безопасности современных операционных систем</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы</p> <p>ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p>	<p>Регламентирование настроек безопасности операционных систем</p> <p>Итоговое контрольное мероприятие</p>	<p>умение регламентировать настройку механизмов безопасности операционных систем, порядок мониторинга их функционирования</p>

Спецификация мероприятий текущего контроля

Основы безопасности информационных систем

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
Верность и полнота ответов на предложенные вопросы, максимально до	10

Безопасность NTFS

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**

Проходной балл: **6.3**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	15

Безопасность EXT2

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**

Проходной балл: **6.3**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	15

Отказоустойчивость системного ПО

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

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**

Проходной балл: **6.3**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	15

Механизмы безопасности операционных систем семейства Windows

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**

Проходной балл: **6.3**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	15

Механизмы безопасности операционных систем семейства Linux

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

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

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

Проходной балл: **12**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	25

Регламентирование настроек безопасности операционных систем

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

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

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**

Проходной балл: **6.3**

Показатели оценивания	Баллы
Верное выполнение контрольного задания (верность и полнота выполнения определяется успешным прохождением всех предложенных преподавателем проверочных тестов)	15