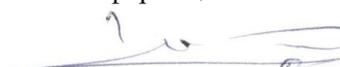




МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП
«Информационная безопасность»



(подпись) Варлатая С.К.
(Ф.И.О. рук. ОП)

« 5 » июля 2018 г.

«УТВЕРЖДАЮ»
Заведующий (ая) кафедрой
информационной безопасности



(подпись) Добржинский Ю.В.
(Ф.И.О. рук. ОП)

« 5 » июля 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (РПУД)

«Защита информации в операционных системах»

Направление –10.03.01 «Информационная безопасность»

Профиль подготовки - «Комплексная защита объектов информатизации»

Форма подготовки – очная

курс 3 семестр 5

лекции 36 час.

практические занятия _____ час.

лабораторные работы 18 час.

в том числе с использованием МАО лек. _____ / пр. _____ / лаб. _____ час.

всего часов аудиторной нагрузки 54 час.

в том числе с использованием МАО _____ час.

самостоятельная работа 54 час.

в том числе на подготовку к экзамену 36 час.

контрольные работы (количество) учебным планом не предусмотрены

курсовая работа / курсовой проект учебным планом не предусмотрены

зачет учебным планом не предусмотрен

экзамен 5 семестр

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 20.07.2017 №12-13-1479.

Рабочая программа обсуждена на заседании кафедры _____ информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

Заведующий (ая) кафедрой: _____ Добржинский Ю.В., к.т.н., с.н.с.

Составитель (ли): _____ Дзенскиевич Е.А., к.т.н.

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от « _____ » _____ 20 г. № _____

Заведующий кафедрой _____ Ю.В. Добржинский
(подпись) (и.о. фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от « _____ » _____ 200 г. № _____

Заведующий кафедрой _____ Ю.В. Добржинский
(подпись) (и.о. фамилия)

Аннотация к рабочей программе дисциплины «Защита информации в операционных системах»

Дисциплина «Защита информации в операционных системах» имеет целью обучить студентов принципам построения современных операционных систем, принципам построения защиты информации в операционных системах (ОС), как с помощью встроенных, так и дополнительных средств защиты, и анализа надежности защиты ОС, а также принципам хранения, обработки и передачи информации в автоматизированных системах, показать им, что концепция баз данных стала определяющим фактором при создании эффективных систем обработки информации.

Общая трудоемкость освоения дисциплины составляет 144 часа (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (18 час.), самостоятельная работа студентов (54 час.), контроль качества обучения студентов (36 час.). Дисциплина реализуется на 3 курсе в 5 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Защита информации в операционных системах» относится к вариативным дисциплинам учебного плана. Изучение дисциплины «Защита информации в операционных системах» базируется на следующих дисциплинах: «Информатика», «Языки программирования».

Дисциплина «Защита информации в операционных системах» обеспечивает изучение следующих дисциплин: «Комплексная защита объектов информатизации», «Вычислительные сети». Знания и практические навыки, полученные из дисциплины «Защита информации в операционных системах», используются студентами при разработке курсовых и дипломных работ.

Цель: дать основы устройства и принципов функционирования ОС различной архитектуры; принципов построения и защиты информации в ОС различной архитектуры.

Задачи:

- дать базовое представление об ОС различных архитектур;
- дать основы средств и методов несанкционированного доступа к ресурсам ОС;
- дать основные принципы построения защиты информации от рассмотренных средств и методов НСД;
- привить системный подход к проблеме защиты информации в ОС.

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные/ общепрофессиональные/ профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-4) способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знает	роль и место информационной безопасности в системе национальной безопасности Российской Федерации
	Умеет	анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	методами формирования требований по защите информации
(ОПК-5) способность использовать нормативные правовые акты в профессиональной деятельности	Знает	основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет	пользоваться нормативными документами по защите информации
	Владеет	навыками работы с нормативными правовыми актами
(ОПК-7) способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта	Знает	информационные ресурсы, подлежащие защите и возможные пути реализации угроз безопасности
	Умеет	определять информационные ресурсы, подлежащие защите
	Владеет	способностью анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

защиты		
(ПК-10) способностью оценивать уязвимости информационных систем, разрабатывать требования и критерии оценки информационной безопасности, согласованных со стратегией развития информационных систем	Знает	структуру баз данных с конфиденциальной информацией

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита информации в операционных системах» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

МОДУЛЬ 1. Современные операционные системы (18 час.)

Раздел I. Архитектура современных ОС (18 час.)

Тема 1. Общая характеристика ОС (2 час.)

Назначение ОС. Задачи, решаемые ОС. Классификация ОС. Общая характеристика ОС MS-DOS, Windows, UNIX.

Тема 2. Интерфейс ОС (2 час.)

Диалоговые и пакетные интерфейсы. Интерфейсы, управляемые сообщениями. Программирование в графическом интерфейсе Windows.

Тема 3. Управление ресурсами ОС (5 час.)

Объектно-ориентированные ОС, понятие объекта, управление объектами. Управление памятью, виртуальная память, защита памяти.

Тема 4. Управление устройствами (4 час.)

Понятие устройства. Драйверы устройств, классификация драйверов, управление драйверами. Синхронные и асинхронные запросы к драйверам. Сетевые протоколы как устройства ОС. Архитектура драйверов WindowsNT.

Тема 5. Управление программами (5 час.)

Понятие процесса и потока. Управление процессами, планирование задач, обработка прерываний. Симметричная и ассиметричная мультипроцессорная архитектура. Синхронизация параллельных задач. Обеспечение корректности совместного доступа к данным, предотвращение тупиковых ситуаций. Разделение кода и данных между процессами. Экспорт и импорт функций.

МОДУЛЬ 2. Реализация защиты информации в ОС (18 час.)

Раздел I. Защита информации в современных ОС (18 час.)

Тема 1. Угрозы безопасности ОС (3 час.)

Классификация угроз безопасности ОС. Наиболее распространенные угрозы.

Тема 2. Требования к защите ОС (7 час.)

Понятие защищенной ОС. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты. Стандарты безопасности ОС.

Тема 3. Разграничение доступа в ОС (6 час.)

Понятие разграничения доступа. Виды разграничений доступа, используемые в современных ОС. Способы реализации разграничения доступа в Windows, Linux, UNIX.

Тема 4. Реализация защиты информации в ОС с помощью дополнительных программных средств (2 час.)

Классификация программных средств защиты информации. Общие рекомендации по использованию дополнительных средств защиты ОС. Целесообразность использования дополнительных средств защиты информации.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (36 час.)

Лабораторная работа №1.

Защищаемые объекты операционных систем. Работа с защищаемыми объектами (8 час)

Лабораторная работа №2.

Извлечь маркер доступа из текущего приложения (процесса или потока).

Из маркера извлечь информацию о текущем пользователе и домене.

Для некоторого файла (имеет смысл запретить текущему пользователю некоторые операции) определить дескриптор безопасности.

Из дескриптора безопасности извлечь и вывести на экран информацию о владельце, группе, списке Dacl (все записи в списке). (8 час)

Лабораторная работа №3.

Привилегии. Получить списки всех привилегий и установленных привилегий. Включение, выключение привилегий. (4 час)

Лабораторная работа №4.

Использование API функций для работы с системным реестром. (4 час)

Лабораторная работа №5.

Основы механизма обработки прерываний и исключений в современных операционных системах. Функции и классы обработки исключений языка C++.

(6 час)

Лабораторная работа №6.

Разработка сценариев Windows Script Host. (6 час)

Практические занятия (18 час.)

Занятие № 1.

Знакомства со встроенными средствами администрирования ОС Windows (Редактор реестра, Редактор локальной групповой политики, Диспетчер задач

Просмотр событий, Планировщик заданий, Монитор стабильности системы,

Системный монитор, Монитор ресурсов, Брандмауэр Windows)

Основные команды системного администратора

Структура реестра Windows (6 час)

Занятие № 2

Защищаемые объекты ядра операционных систем. Типы объектов. Учет пользователей. Таблица описателей объектов ядра. Совместное использование объектов ядра. (2 час)

Занятие №3.

Основы использования командлетов. Администрирование с помощью командлетов. (6 час)

Занятие №4.

Компонент операционной системы Windows – Windows Script Host. , Возможности и преимущества WSH-скриптов. Объект WScript. (4 час)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Электроника и схемотехника» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

- требования к представлению и оформлению результатов самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	МОДУЛЬ 1. Современные операционные системы	ОПК-4, ОПК-5, ОПК-7,	знает	ПР-7	1-21
			умеет	ПР-6	1-21
			владеет	ПР-7	1-21
2	МОДУЛЬ 2. Реализация защиты информации в ОС	ОПК-4, ОПК-5, ОПК-7,	знает	ПР-7	22-36
			умеет	ПР-6	22-36
			владеет	ПР-7	22-36

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Компьютерные науки. Деревья, операционные системы, сети [Электронный ресурс] / И.Ф. Астахова [и др.]. — Электрон. дан. — Москва : Физматлит, 2013. — 88 с. — Режим доступа: <https://e.lanbook.com/book/59757>. — Загл. с экрана

2. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. —

592 с. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/546679>

3. Мельников А.А. Безопасность жизнедеятельности. Топографо-геодезические и землеустроительные работы [Электронный ресурс]: учебное пособие для вузов/ Мельников А.А.— Электрон. текстовые данные.— М.: Академический Проект, Трикста, 2015.— 336 с.— Режим доступа: <http://www.iprbookshop.ru/36844.html>.— ЭБС «IPRbooks»

4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: <http://www.iprbookshop.ru/52209.html>.— ЭБС «IPRbooks»

5. Верещагина Е.А. Операционные системы : учебно-методический комплекс / Владивосток : Изд-во Дальневосточного технического университета, 2008. — 137 с. - <http://lib.dvfu.ru:8080/lib/item?id=chamo:384171&theme=FEFU>

Дополнительная литература

(печатные и электронные издания)

1. IP-телефония в компьютерных сетях [Электронный ресурс]: учебное пособие / И.В. Баскаков [и др.]. — Электрон. дан. — Москва: , 2016. — 226 с. — Режим доступа: <https://e.lanbook.com/book/100611>. — Загл. с экрана.

2. Альпидовский, А.Д. Компьютерные системы и сети [Электронный ресурс] : учебное пособие / А.Д. Альпидовский. — Электрон. дан. — Нижний Новгород : ВГУВТ, 2012. — 156 с. — Режим доступа: <https://e.lanbook.com/book/60800>. — Загл. с экрана

3. Крис Просис, Кевин Мандиа, в переводе Олега Труфанова /Расследование компьютерных преступлений/ Издательство: Лори, 2005, 476с. <http://lib.dvfu.ru:8080/lib/item?id=chamo:233476&theme=FEFU>

Интернет-ресурсы

1. Встраиваемые системы на основе Linux. Издательство "ДМК Пресс". 2017, 360 страниц.

2. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4925

Пушкарев В.В. «Защита информационных процессов в компьютерных системах», Издательство: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), Год: 2012, Объем:131 стр.

3. Кручинин А.Ю. Операционные системы [Электронный ресурс]: учебное пособие/ Кручинин А.Ю.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2009.— 132 с.— <http://www.iprbookshop.ru/30115.html>

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education University Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019
---	--

<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус Д, ауд. Д 546а, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education University Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020</p>
<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус Д, ауд. Д 314, Специализированная лаборатория кафедры ИБ. Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education University Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019</p>

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 547, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education University Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020
---	--

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Защита информации в операционных системах», составляет 90 часов. На самостоятельную работу – 54 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов, 36 часов лабораторных работ и 18 часов практических занятий.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Курс имеет практическую направленность, поэтому основное внимание следует уделять выработке практических навыков и умений по администрированию реальных операционных систем, а также практики использования системных интерфейсов при создании приложений. При этом большое значение имеет практическое выполнение слушателями всех заданий и упражнений в компьютерном классе. Исходя из объема часов, выделяемых на изучение дисциплины, надо обратить особое внимание на

организацию самостоятельной работы. Студентам необходимо прививать умение самостоятельного поиска решений в ходе выполнения заданий. Детальную проработку материала, связанного с разработкой программного обеспечения, следует оставить на самостоятельное изучение.

Подготовка к практическим занятиям и лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии и выполнению лабораторных работ. Основной практической составляющей является выполнение одного практического задания с последующим предоставлением отчета о выполнении. Основными лабораторными работами является выполнение заданий с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям и лабораторным работам.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW330U, 3000 ANSI Lumen, 1280x800 Сетевая видеочка Multipix MP-HD718 Доска аудиторная</p>
--	---

<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 546а, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: Компьютер (твердотельный диск - объемом 128 ГБ; жесткий диск - объем 1000 ГБ; форм-фактор - Tower; комплектуется клавиатурой, мышью, монитором АОС i2757Fm; комплектом шнуров эл. питания) модель - M93p 1 Доска аудиторная</p>
<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Специализированная лаборатория кафедры ИБ. Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: "Компьютер DNS Office (автоматизированное рабочее место), Рабочее место сотрудников в составе: системный блок, клавиатура, мышь, монитор 17" Aser-173 Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW330U, 3000 ANSI Lumen, 1280x800 Сетевая видекамера Multipix MP-HD718" Доска аудиторная</p>
<p>Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 547, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 26) Оборудование: "Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW330U, 3000 ANSI Lumen, 1280x800 Сетевая видекамера Multipix MP-HD718" Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.</p>



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

**УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ
РАБОТЫ ОБУЧАЮЩИХСЯ**
по дисциплине «Защита информации в операционных системах»
Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»
Форма подготовки очная

**Владивосток
2019**

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка практических заданий и лабораторных работ.	18	Отчет о выполнении
2	Сессия	Подготовка к экзамену	36	Экзамен

Подготовка отчетов к практическим заданиям и лабораторным работам предполагает повторение лекционного материала и выполнение практических заданий и лабораторных работ. В результате студент должен представить отчеты о проделанной работе.

Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить

широкий спектр мнений по изучаемой проблеме.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.
2. Самопроверка, взаимопроверка выполненного задания в группе.
3. Обсуждение результатов выполненной работы на занятии.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентами учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности,

варианты действий;

- умение сформировать свою позицию, оценку и аргументировать ее.

Критерии оценки выполнения контрольных заданий для самостоятельной работы

Процент правильных ответов	Оценка
От 95% до 100%	отлично
От 76% до 95%	хорошо
От 61% до 75%	удовлетворительно
Менее 61 %	неудовлетворительно

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников, материалов по практическим занятиям и лабораторным работам.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Защита информации в операционных системах»
Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции	
способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)	Знает	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации
	Умеет	Анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	Методами формирования требований по защите информации
способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	Знает	Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области
	Умеет	Пользоваться нормативными документами по защите информации
	Владеет	Навыками работы с нормативными правовыми актами
способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	Знает	Информационные ресурсы, подлежащие защите и возможные пути реализации угроз безопасности
	Умеет	Определять информационные ресурсы, подлежащие защите
	Владеет	Способностью анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	МОДУЛЬ 1.	ОПК-4,	знает	ПР-7	1-21

	Современные операционные системы	ОПК-5, ОПК-7,	умеет	ПР-6	1-21
			владеет	ПР-7	1-21
2	МОДУЛЬ 2. Реализация защиты информации в ОС	ОПК-4, ОПК-5, ОПК-7,	знает	ПР-7	22-36
			умеет	ПР-6	22-36
			владеет	ПР-7	22-36

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

1. Угрозы безопасности операционной системы
2. Классификации угроз
3. Адекватная политика безопасности
4. "Критерии безопасности компьютерных систем" (Оранжевая книга)
5. Основные документы ФСТЭК по вопросам защиты компьютерных систем.
6. Разграничение доступа в ОС
7. Модели доступа: избирательное(дискреционное) разграничение доступа, изолированная программная среда.
8. Полномочное или мандатное разграничение доступа
9. Идентификация и аутентификация с помощью имени и пароля. Методы подбора паролей.
10. Защита паролей от компрометации
11. Протокол NTLM, алгоритм работы.
12. Версия протокола NTLMv2, алгоритм работы.
13. Диспетчер учетных записей SAM. Назначение, основные объекты.
14. Active Directory. Основные понятия и определения.
15. Протокол Kerberos (версия 5)
16. Компоненты системы защиты ОС Windows.
17. Привилегии. Состояние привилегий. Работа с привилегиями.

18. Схема доступа к объектам ядра ОС Windows (SID, дескриптор безопасности, маркер доступа)
19. Маска доступа. Структура маски доступа. Извлечение информации о правах доступа.
20. Windows Scripting Host. Типы WSH сценариев. Возможности и преимущества
21. ОС в общей структуре программного обеспечения компьютера.
Основные задачи ОС
22. Типы ОС
23. Структура ОС (конструктивные решения)
24. Управление памятью. Способы организации памяти для однопользовательской ОС.
25. Абстракция памяти. Адресные пространства. Алгоритмы управления памятью
26. Виртуальная память. Страничная организация.
27. Буферы быстрого преобразования (TLB).
28. Таблицы страниц для больших объемов памяти
29. Алгоритмы замещения страниц: NRU, FIFO, "Вторая попытка", LRU, "часы", рабочий набор.
30. Процессы: модель процессов, иерархия процессов, создание, завершение процессов, состояние процесса.
31. Реализация процессов. Таблица процессов
32. Модель потока. Преимущества использования потоков.
33. Реализация потоков в пространстве пользователя.
34. Реализация потоков в ядре.
35. Объекты ядра ОС Windows. Таблица описателей объектов ядра в процессе.
36. Основные объекты административных скриптов. Примеры использования.
37. Системный реестр. Назначение. Работа с системным реестром.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по дисциплине «Защита информации в операционных системах»
Направление подготовки 10.03.01 Информационная безопасность
профиль «Комплексная защита объектов информатизации»
Форма подготовки очная

Владивосток
2019

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Защита информации в операционных системах», составляет 90 часов. На самостоятельную работу – 54 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов, 36 часов лабораторных работ и 18 часов практических занятий.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Курс имеет практическую направленность, поэтому основное внимание следует уделять выработке практических навыков и умений по администрированию реальных операционных систем, а также практики использования системных интерфейсов при создании приложений. При этом большое значение имеет практическое выполнение слушателями всех заданий и упражнений в компьютерном классе. Исходя из объема часов, выделяемых на изучение дисциплины, надо обратить особое внимание на организацию самостоятельной работы. Студентам необходимо прививать умение самостоятельного поиска решений в ходе выполнения заданий. Детальную проработку материала, связанного с разработкой программного обеспечения, следует оставить на самостоятельное изучение.

Подготовка к практическим занятиям и лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии и выполнению лабораторных работ. Основной практической составляющей является выполнение одного практического задания с последующим предоставлением отчета о выполнении. Основной лабораторных работ является выполнение заданий с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям и лабораторных работ.