МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
функционального анализа
и операторных уравнений

Каменский М.И.
подпись, расшифровка подписи

26.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.29 Безопасность операционных систем

1. Шифр и наименование направления подготовки / специальности: 10.05.04 Информационно-аналитические системы безопасности
2. Профиль подготовки / специализации:
3. Квалификация (степень) выпускника: специалист
4. Форма обучения: очная
5. Кафедра, отвечающая за реализацию дисциплины:
функционального анализа и операторных уравнений
6. Составители программы:
Завгородний Михаил Григорьевич, канд. физ-мат. наук, доцент.

7. **Рекомендована:** НМС математического факультета, протокол №0500-07 от 03.07.2018

8. Учебный год: 2018-2019 **Семестр(-ы): 5**

9. Цели и задачи учебной дисциплины:

Цель курса – освоение студентами принципов построения систем защиты информации в рамках операционной системы (ОС), изучение методов анализа надежности операционных систем и получения практических умений и навыков администрирования операционной системы, приводящего к надежной и безопасной работе пользователей с операционной системой и с приложениями под ее управлением.

Основными задачами изучения дисциплины являются:

- изучение принципов построения подсистем защиты в ОС различной архитектуры;
- изучение возможных средств и методов несанкционированного доступа к ресурсам ОС и получение навыков предотвращения подобных попыток;
- применение системного подхода к проблеме защиты информации в ОС;
- освоение механизмов защиты информации в ОС и потенциальных возможностей по их преодолению.

10. Место учебной дисциплины в структуре ООП: (цикл, к которому относится дисциплина, требования к входным знаниям, умениям и компетенциям, дисциплины, для которых данная дисциплина является предшествующей)

Дисциплина входит в базовую (общепрофессиональную) часть профессионального цикла. Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Правоведение, Дискретная математика, Информатика, Математическая логика и теория алгоритмов, Языки программирования, Технология и методы программирования, Основы информационной безопасности. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при изучении курсов: Безопасность электронного документооборота, Криптографические методы защиты информации, Безопасность информационных и аналитических систем, Моделирование автоматизированных информационных систем, Принципы построения, проектирования и эксплуатации автоматизированных информационных систем, Безопасность сетей ЭВМ, Безопасность программного обеспечения, а также при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области информационной безопасности и защиты информации.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОК-8	способность к самоорганизации и самообразованию	знать: Принципы работы с инструментами для поиска и обработки больших объёмов информации уметь: Уметь писать доклады и делать презентации на заданную тему с использованием современных информационных технологий для поиска и обработки; владеть (иметь навык(и)): Основными инструментами для поиска и обработки больших объёмов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации
ОПК-7	способностью применять методы и средства обеспечения информационной безопасности специальных ИАС	знать: основные типы современных операционных систем и оболочек, их возможности и принципы построения; основные понятий по безопасности операционных систем; требования, предъявляемые к системе защиты современных ОС; организацию управления доступом и защиты ресурсов ОС; применяемые на практике критерии и методы оценивания эффективности и надежности средств защиты используемых ОС; основные механизмы безопасности; уметь: оценивать эффективность и надежность встроенной защиты в ОС; выявлять имеющие место проблемные места в защите ОС и использовать комплекс мероприятий для обеспечения защиты; администрировать встроенный функционал ОС, направленный на встроенную политику безопасности; пользоваться встроенными инструментами и средствами защиты, предоставляемыми ОС;

		проводить анализ и оценивание встроенных в ОС механизмов защиты; владеть навыками: установки и настройки современных ОС; построения системной защиты современной ОС; организации управления доступом и защитой ресурсов ОС; применения действующую законодательную базу в области информационной безопасности; применения методов обеспечения безопасности ОС.

12 Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 5/180

Форма промежуточной аттестации *экзамен.*

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		сем. № 5
Аудиторные занятия	*68*	*68*
в том числе: лекции	*34*	*34*
практические	-	-
лабораторные	*34*	*34*
Самостоятельная работа	*76*	*76*
Контроль	*36*	*36*
Форма промежуточной аттестации		*2 контрольные работы, экзамен*
Итого:	*180*	*180*

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины

1. Лекции		
1	Теоретические основы защиты ОС	Понятие безопасности информационных систем в нормативных документах. Классификация защищенности (международные стандарты). Обзор свойств основных классов. Политика безопасности, формальное представление политик безопасности.
2	Методы защиты ОС	Нарушения безопасности. Изъяны защиты. Классификация изъянов защиты по размещению в вычислительной системе. ОС как среда нарушений безопасности. Категории изъянов защиты в ОС. Понятие доверенного ПО операционных систем, TCB. Свойство безопасности ОС, гарантированность безопасности. Принципы разработки доверенного ПО. Структура безопасной ОС. Общие принципы построения защищенных ОС.
3	Модель безопасности	Модель безопасности ОС семейства Windows. Контроль доступа к объектам Windows. Типы субъектов и объектов защиты. Атрибутивная природа контроля доступа к объектам защиты. Списки и записи контроля доступа. Проверка доступа. Эффективные права доступа.
4	Контроль безопасности в ОС	Организация контроля безопасности в ОС Windows. Шаблоны безопасности. Анализ безопасности с помощью шаблонов. Подсистема аудита. Защита данных при хранении в ОС, EFS. Защита данных при передаче, поддержка VPN. Контроль целостности в ОС. Целостность ядра ОС. Обеспечение целостности кода. Управление учетными записями. Мандатный контроль целостности. Изоляция привилегий пользовательского интерфейса. Защищенные процессы. Изоляция нулевой сессии.
5	Безопасность серверных приложений	Обеспечение безопасности серверных приложений ОС. Сервер IIS, его механизмы защиты. Защита DNS. Защита RDS (протокола удалённого рабочего стола).
6	Безопасность UNIX-систем	Обеспечение безопасности UNIX-систем. Защита ОС на этапе загрузки. Шифрование файловых систем в ОС UNIX. Защищенные терминалы. Аутентификация в ОС, реализация в ОС UNIX. Управление учетными записями и домашними каталогами. Дискреционный контроль доступа в UNIX-системах. Биты защиты. Усиление базовой безопасности ОС UNIX. Механизмы SELinux, RSBAC, GRSecurity. Применение подключаемых модулей аутентификации PAM. Аудит и журналировние событий в UNIX-системах. Анализ журналов, управление ими и защита.
7	Безопасность сетевых взаимодействий	Защита сетевого взаимодействия в ОС UNIX. Фильтрация трафика. Использование прокси-серверов. Криптографическая защита сетевого взаимодействия. Технологии Open SSL, SSH.
8	Безопасность приложений	Обеспечение безопасности на уровне приложений. Задание конфигурации безопасности. Файлы конфигурации.

		Настройка безопасности сервера, модули, создание замкнутой среды выполнения. Анализ уязвимостей на примере ОС UNIX.
3. Лабораторные работы		
1	Теоретические основы защиты ОС	Понятие безопасности информационных систем в нормативных документах. Классификация защищенности (международные стандарты). Обзор свойств основных классов. Политика безопасности, формальное представление политик безопасности.
2	Методы защиты ОС	Нарушения безопасности. Изъяны защиты. Классификация изъянов защиты по размещению в вычислительной системе. ОС как среда нарушений безопасности. Категории изъянов защиты в ОС. Понятие доверенного ПО операционных систем, ТСВ. Свойство безопасности ОС, гарантированность безопасности. Принципы разработки доверенного ПО. Структура безопасной ОС. Общие принципы построения защищенных ОС.
3	Модель безопасности	Модель безопасности ОС семейства Windows. Контроль доступа к объектам Windows. Типы субъектов и объектов защиты. Атрибутивная природа контроля доступа к объектам защиты. Списки и записи контроля доступа. Проверка доступа. Эффективные права доступа.
4	Контроль безопасности в ОС	Организация контроля безопасности в ОС Windows. Шаблоны безопасности. Анализ безопасности с помощью шаблонов. Подсистема аудита. Защита данных при хранении в ОС, EFS. Защита данных при передаче, поддержка VPN. Контроль целостности в ОС. Целостность ядра ОС. Обеспечение целостности кода. Управление учетными записями. Мандатный контроль целостности. Изоляция привилегий пользовательского интерфейса. Защищенные процессы. Изоляция нулевой сессии.
5	Безопасность серверных приложений	Обеспечение безопасности серверных приложений ОС. Сервер IIS, его механизмы защиты. Защита DNS. Защита RDS (протокола удалённого рабочего стола).
6	Безопасность UNIX-систем	Обеспечение безопасности UNIX-систем. Защита ОС на этапе загрузки. Шифрование файловых систем в ОС UNIX. Защищенные терминалы. Аутентификация в ОС, реализация в ОС UNIX. Управление учетными записями и домашними каталогами. Дискреционный контроль доступа в UNIX-системах. Биты защиты. Усиление базовой безопасности ОС UNIX. Механизмы SELinux, RSBAC, GRSecurity. Применение подключаемых модулей аутентификации PAM. Аудит и журналировние событий в UNIX-системах. Анализ журналов, управление ими и защита.
7	Безопасность сетевых	Защита сетевого взаимодействия в ОС UNIX. Фильтрация трафика. Использование прокси-серверов.

	взаимодействий	Криптографическая защита сетевого взаимодействия. Технологии Open SSL, SSH.
8	Безопасность приложений	Обеспечение безопасности на уровне приложений. Задание конфигурации безопасности. Файлы конфигурации. Настройка безопасности сервера, модули, создание замкнутой среды выполнения. Анализ уязвимостей на примере ОС UNIX.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Лабораторные	Самостоятельная работа	Контроль	Всего
1	Теоретические основы защиты ОС	4	2	4	2	12
2	Методы защиты ОС	4	4	6	3	17
3	Модель безопасности	4	4	8	4	20
4	Контроль безопасности в ОС	4	6	10	5	25
5	Безопасность серверных приложений	4	4	10	4	22
6	Безопасность UNIX-систем	4	4	18	8	34
7	Безопасность сетевых взаимодействий	4	4	8	4	20
8	Безопасность приложений	6	6	12	6	30
	Итого	34	34	76	36	180

14. Методические указания для обучающихся по освоению дисциплины

Аудиторные занятия, лекции и лабораторные занятия, предполагают самостоятельную работу студентов по данному курсу. Ряд тем выносятся для самостоятельного изучения, предлагаются темы для создания докладов с презентациями. Предусмотрены домашние задания и оформление отчетов выполнения лабораторных заданий, а также дополнительные задания для сильных студентов

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	*Таненбаум, Эндрю. Современные операционные системы = Modern Operating Systems / Э. Таненбаум ; [пер. с англ. Н. Вильчинского, А. Лашкевича] .— 3-е изд. — СПб. [и др.] : Питер, 2010 .— 1115 с. : ил., табл. — (Классика Computer Science) .— Библиогр.: с.1108-1115 .— ISBN 978-5-49807-306-4.*

б) дополнительная литература:

№ п/п	Источник
2	*Хоглунд, Г. Руткиты. Внедрение в ядро Windows = Rootkits. Subverting the Windovs Kernel : пер. с англ. / Г. Хоглунд, Дж. Батлер .— СПб [и др.] : Питер, 2007 .— 284 с. — Алф. указ.: с.277-284 .— ISBN 978-5-469-01409-6.*
3	*Безбогов, Александр Александрович. Безопасность операционных систем : [учебное пособие для студ. вузов, обуч. по специальности 090105 "Комплекс. обеспечение информ. безопасности автоматизир. систем"] / А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов .— М. : Гелеос АРВ, 2008 .— 319 с. : ил., табл. — Библиогр.: с.308-310 .— ISBN 978-5-85438-181-9.*
4	*Таненбаум, Эндрю. Современные операционные системы / Э. Таненбаум ; Пер. с англ. А. Леонтьева .— 2-е изд. — СПб. : Питер, 2002 .— 1037 с. : ил., табл. — (Классика Computer Science) .— ISBN 5-318-00299-4.*
5	*Проскурин, Вадим Геннадьевич. Защита в операционных системах : Программ.-аппарат. средства обеспечения информ. безопасности :Учеб. пособие для студ. вузов по специальностям "Защищ. телекоммуникац. системы", "Орг. и технология защиты информ.", "Комплекс. обеспечение информ. безопасности автоматизир. / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич .— М. : Радио и связь, 2000 .— 164,[2] с. : ил., табл. — ISBN 5-256-01414-5 : 48.60.*
6	*Боmm, Эд. Безопасность Windows : Windows XP и Windows 2000 / Э. Боmm, К. Зихерт ; Пер. с англ. Д. Жукова и др. — СПб. : Питер, 2003 .— 681 с. : ил. — (Эффективная работа) .— Парал. тит. л. англ. — ISBN 5-8046-0116-4.*

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

№ п/п	Источник
1	*Таненбаум, Эндрю. Современные операционные системы = Modern Operating Systems / Э. Таненбаум ; [пер. с англ. Н. Вильчинского, А. Лашкевича] .— 3-е изд. — СПб. [и др.] : Питер, 2010 .— 1115 с. : ил., табл. — (Классика Computer Science) .— Библиогр.: с.1108-1115 .— ISBN 978-5-49807-306-4.*

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория (доска, мел, маркеры); для проведения лабораторных работ компьютерные классы с набором базового программного обеспечения, с возможностью многопользовательской работы, централизованного администрирования и доступа к информационным ресурсам; мультимедийный проектор.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОК-8 способностью к самоорганизации и самообразованию,	знать: основные типы современных операционных систем и оболочек, их возможности и принципы построения; основные понятий по безопасности операционных систем; требования, предъявляемые к системе защиты современных ОС; организацию управления доступом и защиты ресурсов ОС; применяемые на практике критерии и методы оценивания эффективности и надежности средств защиты используемых ОС; основные механизмы безопасности; уметь: оценивать эффективность и надежность встроенной защиты в ОС;	Разделы 1-4: 1. Теоретические основы защиты ОС 2. Методы защиты ОС 3. Модель безопасности 4. Контроль безопасности в ОС	Лабораторные работы и контрольная работа
		Разделы 5-6: 5. Безопасность серверных приложений 6. Безопасность UNIX-систем	Лабораторные работы и контрольная работа

	выявлять имеющие место проблемные места в защите ОС и использовать комплекс мероприятий для обеспечения защиты; администрировать встроенный функционал ОС, направленный на встроенную политику безопасности; пользоваться встроенными инструментами и средствами защиты, предоставляемыми ОС; проводить анализ и оценивание встроенных в ОС механизмов защиты; владеть навыками: установки и настройки современных ОС; построения системной защиты современной ОС; организации управления доступом и защитой ресурсов ОС; применения действующую законодательную базу в области информационной безопасности; применения методов обеспечения безопасности ОС.		
ОПК-7 способность применять методы и средства обеспечения информационной безопасности	знать: методы и средства обеспечения информационной безопасности специальных ИАС.	Разделы 7-8: 7. Безопасность сетевых взаимодействий	Лабораторные работы и контрольная работа

специальных ИАС.	Уметь: применять методы и средства обеспечения информационной безопасности	8. Безопасность приложений	
	Владеть: способностью применять методы и средства обеспечения информационной безопасности		
Промежуточная аттестация			Комплект КИМ

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

владение понятийным аппаратом данной области науки (теоретическими основами дисциплины), способность иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач в области информатики

Для оценивания результатов обучения на экзамене (зачете с оценкой) используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами применять теоретические знания для решения практических задач	*Повышенный уровень*	*Отлично*
Обучающийся владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами, допускает ошибки при решении практических задачи или способен применять теоретические знания для решения	*Базовый уровень*	*Хорошо*

практических задач в области информатики, но допускает неточности при применении понятийного аппарата данной области науки, но отвечает на дополнительные вопросы		
Обучающийся владеет частично теоретическими основами дисциплины, фрагментарно способен иллюстрировать ответ примерами, фактами, не отвечает на дополнительные вопросы *Не умеет применять теоретические знания для решения практических задач*	*Пороговый уровень*	*Удовлетвори-тельно*
Ответ на контрольно-измерительный материал не соответствует любым трем(четырем) из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	*Неудовлетвор и-тельно*

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Перечень вопросов к экзамену:

1. Понятие защищенной информационной системы.
2. Свойства защищенной ОС.
3. Безопасность информационных систем в нормативных документах.
4. Классификация защищенности ОС по международным стандартам.
5. Политика безопасности, формальное представление политик.
6. Классификация изъянов защиты.
7. Категории изъянов защиты в ОС.
8. Понятие доверенного ПО.
9. Свойство безопасности ОС.
10. Модель безопасности ОС семейства Windows.
11. Контроль доступа к объектам Windows.
12. Проверка доступа. Эффективные права доступа.
13. Шаблоны безопасности.
14. Подсистема аудита ОС Windows.
15. Шифрованная файловая система EFS.
16. Защита данных при передаче. VPN.
17. Контроль целостности в ОС Windows Vista.
18. Механизмы защиты уровня ядра в ОС Windows Vista.
19. Обеспечение безопасности серверных приложений ОС.
20. Сервер IIS. Механизмы защиты.
21. Защита службы DNS.
22. Защита службы RDS.
23. Защита ОС UNIX на этапе загрузки.
24. Шифрование файловых систем в ОС UNIX.
25. Защищенные терминалы.
26. Аутентификация в ОС, реализация в ОС UNIX.
27. Дискреционный контроль доступа в UNIX-системах.
28. Усиление базовой безопасности ОС UNIX.
29. Применение подключаемых модулей аутентификации PAM.

30. Аудит и журналировние событий в UNIX-системах.
31. Фильтрация трафика.
32. Криптографическая защита сетевого взаимодействия.
33. Обеспечение безопасности на уровне приложений.
34. Настройка безопасности сервера Apache.
35. Создание замкнутой среды выполнения.
36. Анализ уязвимостей на примере ОС UNIX.

Пример контрольно-измерительного материала

Контрольно-измерительный материал №___

1. Безопасность информационных систем в нормативных документах.

2. Обеспечение безопасности на уровне приложений.

19.3.2 Перечень практических заданий

Тема: «**Угрозы безопасности клиентским операционным системам**»

Задание. По представленному описанию компании определить угрозы безопасности клиентским ОС, выбрать клиентские ОС, отвечающие интересам компании и описать процесс организации их защиты. По результатам выполнения задания подготовьте отчет.

Вопросы

1. Какие существуют основные типы угроз безопасности ОС? Обоснуйте ответ.
2. Какие механизмы защиты ОС Вы знаете?
3. В чем заключается разница защитных механизмов клиентских ОС семейства Windows и Linux? Обоснуйте ответ.

19.3.4 Перечень заданий для контрольных работ

Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Безопасность операционных систем»
Вариант №___

Составьте алгоритм и напишите программу, обеспечивающую взаимоисключения с помощью семафора.

19.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса (индивидуальный опрос на коллоквиуме); письменных работ (контрольные работы). Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний, или практические задания, позволяющие оценить степень сформированности умений, навыков и опыт деятельности.

При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.