ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Утверждена решением
Ученого совета ДГУНХ,
протокол № 13
от 06 июля 2020 г

Кафедра «Информационные технологии и информационная безопасность»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Форма обучения – очная

Махачкала – 2020

УДК 681.518(075.8)
ББК 32.81.73

Составитель – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдуллаев Ших-Саид Омаржанович, доктор технических наук, главный научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской академии наук.

Представитель работодателя - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Рабочая программа дисциплины «Безопасность операционных систем» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г., № 1515, в соответствии с приказом Министерства образования и науки Российской Федерации от 5.04.2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Рабочая программа по дисциплине «Безопасность операционных систем» размещена на официальном сайте www.dgunh.ru

Гасанова З.А. Рабочая программа по дисциплине «Безопасность операционных систем» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2020 г., 15 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 03 июля 2020 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 30 июня 2020 г., протокол № 12

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Цель дисциплины – сформировать компетенции обучающегося в области построения защищенных автоматизированных систем на основе современных операционных систем, а также администрирования подсистем информационной безопасности операционных систем.

Задачи дисциплины:

- Рассмотреть основные принципы устройства и принципов функционирования операционных систем различной архитектуры;
- Раскрыть принципы построения подсистем защиты в операционных системах различной архитектуры;
- Показать особенности средств и методов несанкционированного доступа к различным ресурсам операционных систем.

1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Безопасность операционных систем» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ПСК	**Профессиональные специализированные компетенции**
ПСК-1	способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ПСК-2	способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей
ПСК-3	способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации
ПСК-4	способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности

1.2. Планируемые результаты обучения по дисциплине

код и формулировка компетенции	компонентный состав компетенции		
	знать	уметь	владеть
ПСК-1: Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организа-	З1 - принципы организации и структуру подсистем защиты операционных систем	У1 - определять подлежащие защите информационные ресурсы системы; У2 - выявлять слабости защиты операционной си-	В1 – навыками разработки комплекса мер для управления информационной безопасностью в операционных системах

ции защиты обрабатываемой в них информации		стемы и использовать их для вскрытия защиты	
ПСК-2: Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	З1 – основные приемы настройки подсистем информационной безопасности операционных систем З2 - принципы построения подсистем защиты в операционных системах	У1 - пользоваться средствами защиты, предоставляемыми операционной системой У2 - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	В1 - методами и инструментарием конфигурирования и настройки средств защиты информации в ОС
ПСК-3: Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	З1 - возможности и особенности средств безопасности ОС	У1 – планировать политику безопасности операционной системы; У2 – формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	В1 - методами и средствами выявления угроз безопасности ОС
ПСК-4: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	З1 - наиболее распространенные методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации	У1 - разрабатывать программные средства обеспечения информационной безопасности с учетом и использованием возможностей ОС	

1.3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Код компетенции	Этапы формирования компетенций (темы дисциплин)					
	Тема 1. Понятие защищенной операционной системы	Тема 2. Управление доступом	Тема 3. Аутентификация	Тема 4. Аудит и обнаружение вторжений	Тема 5. Обеспечение целостности данных и систем	Тема 6. Сетевая безопасность ОС
ПСК-1		+	+	+	+	+
ПСК-2		+	+	+	+	+

ПСК-3	+	+	+	+	+	+
ПСК-4			+	+	+	+

Код компетенции	Этапы формирования компетенций (темы дисциплин)					
	Тема 7. Доверенная загрузка ОС	Тема 8. Основные понятия операционных систем специального назначения (ОССН) пом	Тема 9. Управление доступом в ОССН	Тема 10. Управление безопасностью в ОССН	Тема 11. Виртуализация операционных систем	Тема 12. Безопасность операционных систем мобильных устройств
ПСК-1	+	+	+	+	+	+
ПСК-2	+	+	+	+	+	+
ПСК-3	+	+	+	+	+	+
ПСК-4	+	+			+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ОД.2 «Безопасность операционных систем» относится к вариативной части Блока 1 «Дисциплины» учебного плана направления подготовки «Информационная безопасность», профиля «Безопасность автоматизированных систем».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам «Архитектура операционных систем», «Аппаратные средства вычислительной техники», «Основы информационной безопасности», «Криптографические методы защиты информации», «Программно-аппаратные средства защиты информации», «Безопасность вычислительных сетей».

Знания, умения и навыки, полученные студентами в рамках данной дисциплины, пригодятся им при написании выпускной квалификационной работы, а также необходимы при прохождении производственной практики.

Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся, на самостоятельную работу обучающихся и форму промежуточной аттестации

Объем дисциплины в зачетных единицах составляет 5 зачетных.

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 68 часов, в том числе:

на занятия лекционного типа – **34**ч.

на занятия семинарского типа – **34** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **76** ч.

Форма промежуточной аттестации: экзамен, 36 ч.

Отдельные практические занятия по дисциплине реализуются в форме практической подготовки.

Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1	Тема 1. Понятие защищенной операционной системы.	10	2	-	1	1	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
2	Тема 2. Управление доступом	14	4	-	2	2	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
3	Тема 3. Аутентификация*	10	2*	-	1*	1*	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
4	Тема 4. Аудит и обнаружение вторжений*	10	2*	-	1*	1*	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы

5	Тема 5. Обеспечение целостности данных и систем*	10	2*	-	1*	1*	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
6	Тема 6. Сетевая безопасность ОС*	10	2*	-	1*	1*	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
7	Тема 7. Доверенная загрузка ОС*	10	2*	-	1*	1*	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
8	Тема 8. Основные понятия операционных систем специального назначения (ОССН)	14	4	-	2	2	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
9	Тема 9. Управление доступом в ОССН*	14	4*	-	2*	2*	-	-	6	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
10	Тема 10. Управление безопасностью в ОССН*	16	4*	-	3*	3*	-	-	6	Устный опрос Тестирование

										Подготовка реферата Подготовка презентации Выполнение лабораторной работы
11	Тема 11. Виртуализация операционных систем	14	4	-	1	1	-	-	8	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
12	Тема 12. Безопасность операционных систем мобильных устройств	12	2	-	1	1	-	-	8	Устный опрос Тестирование Подготовка реферата Подготовка презентации Выполнение лабораторной работы
	ИТОГО:	**144**	**34**		**17**	**17**			**76**	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								**Контроль**
	ВСЕГО:	**180**								

*Реализуется в форме практической подготовки

Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Выходные данные	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
I. Основная учебная литература				
1.	Гончарук, С.В.	Администрирование ОС Linux	2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 165 с.	http://biblioclub.ru/index.php?page=book&id=429014
2.	Ложников П.С.	Средства безопасности операционной системы ROSA Linux	Омск : Издательство ОмГТУ, 2017. - 94 с. ISBN 978-5-8149-2502-2	https://biblioclub.ru/index.php?page=book_red&id=493349&sr=1
3.	Молочков В. П.	Операционная система ROSA	Омск : Издательство ОмГТУ, 2017. - 226 с.	https://biblioclub.ru/index.php?page=book_red&id=429056&sr=1
II. Дополнительная литература				
А) Дополнительная учебная литература				
1.	Жидков О.М.	Сетевые операционные системы	Москва : Лаборатория книги, 2011. - 114 с. ISBN 978-5-504-00184-5	http://biblioclub.ru/index.php?page=book&id=142238
2.	Карпов В. , Коньков К.	Основы операционных систем : практикум	Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 301 с.	http://biblioclub.ru/index.php?page=book&id=429022
3.	Котельников Е.	Введение во внутреннее устройство Windows	Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 261 с.	https://biblioclub.ru/index.php?page=book_red&id=429084&sr=1
4.	Куль Т.П.	Операционные системы	Минск : РИПО, 2015. - 312 с. ISBN 978-985-503-460-6	https://biblioclub.ru/index.php?page=book_red&id=463629&sr=1
5.	Пахмурин Д.О.	Операционные системы ЭВМ	Министерство образования и науки	https://biblioclub.ru/index.php?page=book_red&id=480573&sr=1

			Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : ТУСУР, 2013. - 255 с.	

Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ	
1.	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).
2.	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. www.standartgost.ru
3.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru
4.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru
5.	ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» www.standartgost.ru
6.	ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. www.standartgost.ru
7.	ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». www.standartgost.ru
В) Периодические издания	
1.	Журнал для пользователей персональных компьютеров «Мир ПК»
2.	Научный журнал «Информатика и ее применение»
3.	Информатика и безопасность
4.	Журнал о компьютерах и цифровой технике «Computer Bild»
5.	Рецензируемый научный журнал «Информатика и система управления»
6.	Рецензируемый научный журнал «Проблемы информационной безопасности»
Г) Справочно-библиографическая литература	

1.	1. Краткий энциклопедический словарь по информационной безопасности : словарь / сост. В.Г. Дождиков, М.И. Салтан. – Москва : Энергия, 2010. – 240 с. http://biblioclub.ru/index.php?page=book&id=58393

Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (http://e-dgunh.ru). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

Для самостоятельного изучения материала и ознакомления с регламентирующими документами и текущей практикой в области защиты операционных систем, рекомендуется использовать следующие Интернет-ресурсы:

1. http://www.fsb.ru/ – официальный сайт ФСБ
2. http://fstec.ru/ – официальный сайт ФСТЭК
3. http://www.consultant.ru/ – онлайн-версия информационно-правовой системы "КонсультантПлюс"
4. http://Standartgost.ru - Открытая база ГОСТов

Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных

7.1. Необходимый комплект лицензионного программного обеспечения:

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip
- VMware Workstation Player
- AstraLinux
- Kali Linux
- РЕД ОС

7.2. Перечень информационных справочных систем:

- информационно справочная система «КонсультантПлюс»
- http://Standartgost.ru - Открытая база ГОСТов

7.3. Перечень профессиональных баз данных:

- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (http://fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi).
- Единый реестр российских программ для электронных вычислительных машин и баз данных (https://reestr.minsvyaz.ru/reestr/).

– Банк данных угроз безопасности информации (bdu.fstec.ru).
– Национальная база данных уязвимостей (www.nvd.nist.gov).

Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для преподавания дисциплины «Безопасность операционных систем» используются следующие специальные помещения и учебные аудитории:

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 4.9 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»**)**

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.urait.ru), интерактивная доска, акустическая система.

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Лаборатория защищенных автоматизированных систем, учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 4.13 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»).

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор.

Персональные компьютеры – 20 ед.

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Помещение для самостоятельной работы № 4.5 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 19 ед.

Помещение для самостоятельной работы № 1-1 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус №

1)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

Раздел 9. Образовательные технологии

Образовательные технологии, используемые при проведении учебных занятий по дисциплине «Безопасность операционных систем», обеспечивают формирование у обучающихся необходимых знаний и развитие навыков.

На занятиях лекционного типа применяются такие методы обучения как Управляемая дискуссия, Проблемная лекции, техники сторителлинга.

На практических занятиях, целью которых является приобретение учащимися определенных практических умений, эффективными будут такие методы как управляемая дискуссия, тестирование, выполнение лабораторных работ.

Лист актуализации рабочей программы дисциплины
«Безопасность операционных систем»

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» сентября 2020 № 2

Зав. кафедрой Гатцев В.С

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» мая 2021 № 10

Зав. кафедрой Гатцев В.С

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___

Зав. кафедрой_____