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

«РАЗРУШАЮЩИЕ ПРОГРАММНЫЕ ВОЗДЕЙСТВИЯ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования - бакалавриат

Форма обучения – очная

Махачкала – 2020

УДК 004 (075.8)
ББК 32.97я73

Составитель–Меджидов ЗаурУруджалиевич, кандидат экономических наук, доцент кафедры«Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент кафедры «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 «Разрушающие программные воздействия» 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 дисциплины «Разрушающие программные воздействия» размещена на официальном сайте www.dgunh.ru

Меджидов З.У. Рабочая программа дисциплины «Разрушающие программные воздействия» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2020 г. - 17 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 организации комплекса мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости программных и аппаратных средств, защиты их от разрушающих программных воздействий.

Задачи дисциплины:

- Рассмотреть концепцию обеспечения информационной безопасности компьютерных систем с применением программно-аппаратных средств, реализующих отдельные функциональные требования по защите;
- Изучить методы и средства реализации программно-аппаратной защиты информации по различным направлениям.

1.1 Компетенции выпускников, формируемые в результате освоения дисциплины «Разрушающие программные воздействия» как часть планируемых результатов освоения образовательной программы высшего образования

код компетенции	формулировка компетенции
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации
ПСК	**ПРОФЕССИОНАЛЬНЫЕ СПЕЦИАЛИЗИРОВАННЫЕ КОМПЕТЕНЦИИ**
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-3: способность планировать и органи-	З1 – алгоритмы работы вредоносного про-	У1 – определять признаки заражения	В1 – навыками установки и использова-

зовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	граммного обеспечения; З2 – алгоритмы работы антивирусного программного обеспечения; З3 – законодательство в области информационной безопасности, касающегося создания и распространения вирусов	компьютерной системы; У2 – использовать средства обеспечения информационной безопасности на персональном компьютере, в том числе при подключении к глобальной сети	ния антивирусного программного обеспечения; В2 – навыками устранения последствий разрушающих программных воздействий
ПСК-4: способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	З1 – алгоритмы работы вредоносного программного обеспечения; З2 – алгоритмы работы антивирусного программного обеспечения	У1 – использовать средства обеспечения информационной безопасности на персональном компьютере, в том числе при подключении к глобальной сети	В1 – навыками установки и использования антивирусного программного обеспечения
ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	З1– программно-аппаратные средства шифрования.	У1 – применять штатные средства защиты и специализированные продукты для решения типовых задач	В1 – навыками использования программно-аппаратных средств, при обеспечении защиты информации.
ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации	З1– основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем	У1 – подбирать и использовать адекватные методы и средства защиты информации	В1 – приемами тестирования уязвимостей корпоративных программно-технических сервисов, типовыми атаками на ИС предприятий

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

код компетенции	Этапы формирования компетенций			
	Тема 1. Основные определения разрушающих программных воздействий. Вредоносные программы и их классификация.	Тема 2. Вредоносные программы, составленные без использования языков программирования.	Тема 3. Угрозы НСД и его разновидности.	Тема 4. Скрытые каналы передачи данных.
ПСК-3	+	+	+	+

ПСК-4				
ПК-1	+	+	+	+
ПК-12				

код компетенции	Этапы формирования компетенций			
	Тема 5. Эксплойты и шелл-код. Скриптовые вирусы.	Тема 6. Особенности руткитов.	Тема7. Перспективные методы противодействия вредоносным программам.	Тема 8. Структура антивирусного программного обеспечения.
ПСК-3	+	+	+	+
ПСК-4	+	+	+	+
ПК-1				
ПК-12	+	+	+	+

код компетенции	Этапы формирования компетенций			
	Тема 9. Структура межсетевых экранов	Тема 10. Системы обнаружения и предотвращения вторжений.	Тема 11. Законодательство РФ в области компьютерных преступлений.	Тема 12. Основы стеганографии.
ПСК-3	+	+		+
ПСК-4			+	+
ПК-1	+	+	+	+
ПК-12	+	+	+	+

код компетенции	Этапы формирования компетенций	
	Тема 13. Рекламное ПО, боты и ботнеты.	Тема 14. Особенности бэкдоров.
ПСК-3	+	+
ПСК-4	+	+
ПК-1		
ПК-12	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ОД.4 «Разрушающие программные воздействия» относится к вариативной части Блока 1 «Дисциплины» учебного плана по направлению подготовки «Информационная безопасность», профиля «Безопасность автоматизированных систем».

Для изучения дисциплины рекомендуется ознакомиться с дисциплинами: «Математическая логика и теория алгоритмов», «Технологии и методы программирования». «Интернет-программирование», «Аппаратные средства вычислительной техники», «Основы информационной безопасности», «Архитектура операционных систем».

Освоение данной дисциплины необходимо обучающемуся для успешного изучения дисциплины «Комплексное обеспечение защиты информации объекта информатизации».

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

Объем дисциплины в зачетных единицах составляет **4** зачетные единицы.

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

на занятия лекционного типа –**34ч.**

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

Количество академических часов, выделенных на самостоятельную работу обучающихся – **40 ч.**

Форма промежуточной аттестации–экзамен, **36** ч.

Отдельные практические занятия по дисциплине реализуются в форме практической подготовки.

Раздел4. 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.	Основные определения разрушающих программных воздействий. Вредоносные программы и их классификация	6	4	-	2	2	-	-	2	Тестирование Выполнение опроса Решение кейс-задачи Подготовка реферата Выполнение лабораторной работы
2.	Вредоносные программы, составленные без использования языков программирования	6	2	-	1	1	-	-	4	Тестирование Выполнение опроса Решение кейс-задачи Подготовка презентации Выполнение лабораторной работы
3.	Угрозы НСД и его разновид-	8	2	-	1	1	-	-	4	Тестирование Выполнение опроса Решение кейс-задачи

	ности									Подготовка реферата Выполнение лабораторной работы
4.	Скрытые каналы передачи данных	4	2	-	1	1	-	-	2	Тестирование Выполнение опроса Решение кейс-задачи Подготовка презентации Выполнение лабораторной работы
5.	Эксплойты и шелл-код. Скриптовые вирусы*	6	2*	-	1*	1*	-	-	2	Тестирование Выполнение опроса Проведение деловой игры Подготовка реферата Выполнение лабораторной работы
6.	Особенности руткитов	6	2	-	1	1	-	-	2	Тестирование Выполнение опроса Проведение деловой игры Выполнение письменной работы Выполнение лабораторной работы
7.	Перспективные методы противодействия вредоносным программам*	4	2*	-	1*	1*	-	-	2	Тестирование Выполнение опроса Выполнение проекта Подготовка реферата Выполнение лабораторной работы
8.	Структура	14	4	-	2	2	-	-	2	Тестирование

	антивирусного программного обеспечения									Выполнение опроса Выполнение проекта Подготовка презентации Выполнение лабораторной работы
9.	Структура межсетевых экранов*	12	2*	-	1*	1*	-	-	2	Тестирование Выполнение опроса Выполнение проекта Проведение круглого стола Выполнение лабораторной работы
10.	Особенности систем обнаружения и предотвращения вторжений*	10	4*	-	2*	2*	-	-	2	Тестирование Выполнение опроса Выполнение проекта Проведение круглого стола Выполнение лабораторной работы
11.	Законодательство РФ в области компьютерных преступлений	8	2	-	1	1	-	-	4	Тестирование Выполнение опроса Решение кейс-задачи Подготовка реферата Выполнение лабораторной работы
12.	Основы стеганографии	8	2	-	1	1	-	-	4	Тестирование Выполнение опроса Решение кейс-задачи Подготовка презентации Выполнение лабора-

										торной работы
13.	Рекламное ПО, боты и ботнеты	8	2	-	1	1	-	-	4	Тестирование Выполнение опроса Решение кейс-задачи Выполнение письменной работы Выполнение лабораторной работы
14.	Особенности бэкдоров	8	2	-	1	1	-	-	4	Тестирование Выполнение опроса Решение кейс-задачи Подготовка презентации Выполнение лабораторной работы
ИТОГО:		**108**	**34**	**-**	**17**	**17**	**-**	**-**	**40**	
Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)		**36**								**Контроль**
ВСЕГО:		**144**								

*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
1.Основная учебная литература				
1.	Ковалев Д.В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов н / Д: Издательство Южного федерального университета, 2016 -74с.	http://biblioclub.ru/index.php?page=book&id=493175
2.	Михайлов А. В.	Компьютерные вирусы и борьба с ними	М.: Диалог-МИФИ, 2012. – 148 с.	http://biblioclub.ru/index.php?page=book&id=136089
2.Дополнительная литература **А) Дополнительная учебная литература**				
1.	Артемов А. В.	Информационная безопасность: курс лекций	Орел: МАБИВ, 2014. – 257 с.	http://biblioclub.ru/index.php?page=book&id=428605
2.	Гошко С.В.	Технологии борьбы с компьютерными вирусами. Практическое пособие	М.: СОЛОН-ПРЕСС, 2009 г. – 351 с.	http://biblioclub.ru/index.php?page=book&id=117855
3.	Спицын В. Г.	Информационная безопасность вычислительной техники: учебное пособие	Томск: Эль Контент, 2011. -148 с.	http://biblioclub.ru/index.php?page=book&id=208694
4.	Щербаков А.	Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учебное пособие	М.: Книжный мир, 2009. – 352 с.	http://biblioclub.ru/index.php?page=book&id=89798
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 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г.www.standartgost.ru			
3.	ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств. 2002 г.www.standartgost.ru			
4.	ГОСТ Р ИСО/МЭК 15288-2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. 2006 г.www.standartgost.ru			
5.	ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г.www.standartgost.ru			

6.	ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. 2009 г.www.standartgost.ru
7	ГОСТ 28195-89. Оценка качества программных средств. Общие положения. 2001 г.www.standartgost.ru
8	ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.www.standartgost.ru
В) Периодические издания	
1.	Рецензируемый научный журнал «Проблемы информационной безопасности»
2.	Научный журнал «Прикладная дискретная математика»
3.	Научный журнал «Информатика и ее применение»
4.	Журнал о компьютерах и цифровой технике «ComputerBild»
5.	Рецензируемый научный журнал «Информатика и система управления»
6.	Рецензируемый научный журнал «Проблемы информационной безопасности»
7.	Рецензируемый научный журнал «Прикладная информатика»
Г) Справочно-библиографическая литература	
1.	Краткий энциклопедический словарь по информационной безопасности https://biblioclub.ru/index.php?page=book_red&id=58393&sr=1
2	Энциклопедия информатики ИНФОПЕДИЯ - http://s-infopedia.com/

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 информационной безопасности, рекомендуется использовать следующие Интернет-ресурсы:

1. Интернет-Университет Информационных Технологий «ИНТУИТ» - www.intuit.ru
2. Русскоязычный сайт, посвящённый разработке программного обеспечения - http://rsdn.ru/
3. Энциклопедия информатики ИНФОПЕДИЯ - http://s-infopedia.com/
4. Электронно-библиотечная система «КнигаФонд» - http://www.knigafund.ru/
5. Университетская библиотека ONLINE - http://biblioclub.ru/
6. "Российское образование" Федеральный портал. - www.edu.ru
7. МультиМедиа Технологии - http://macintoshca.chat.ru/
8. Компьютерная библиотека - http://computerlibrary.info
9. Единое окно доступа к образовательным ресурсам - http://window.edu.ru/
10. http://www.fsb.ru/ – официальный сайт ФСБ
11. http://fstec.ru/ – официальный сайт ФСТЭК

12. http://www.consultant.ru/ – онлайн-версия информационно-правовой системы "КонсультантПлюс"
13. http://Standartgost.ru - Открытая база ГОСТов
14. https://www.anti-malware.ru/
15. http://www.matousec.com
16. http://www.iso27000.ru

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

7.1. Необходимый комплект лицензионного программного обеспечения

1. Windows 10

2. Microsoft Office Professional

3. Adobe Acrobat Reader DC

4. VLC Media player

5. 7-zip

6. VMware Workstation Player

7. Kaspersky Endpoint Security 11

7.2.Перечень информационных справочных систем:

- Справочно-правовая система «КонсультантПлюс».

7.3. Перечень профессиональныхбаз данных:

- Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 (http://fstec.ru/ tekhnicheskayazashchitainformatsii/dokumenty-po-sertifikatsii/153-sistemasertifikatsii/591-gosudarstvennyj-reestr-sszi).
- Государственный реестр сертифицированных средств защиты информации (http://clsz.fsb.ru/certification.htm);
- Научная электронная библиотека «Elibrary» (https://elibrary.ru);

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

Для преподавания дисциплины«Разрушающие программные воздействия»используются следующие специальные помещения **– 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

При освоении дисциплины «Разрушающие программные воздействия» используются следующие образовательные технологии:

–деловые игры для выработки навыков принятия командных решений;

–кейс-задания для экспериментальной работы с аналоговыми моделями реальных объектов, а также закрепления теоретического материала при решении практических задач;

–практическое занятие на основе выполнения проекта для анализа конкретных ситуаций и задач, поиска верного подхода к их решению;

–внеаудиторная работа в форме обязательных консультаций и индивидуальных занятий со студентами (помощь в понимании тех или иных моделей и концепций, подготовка рефератов, а также тезисов для студенческих конференций и т.д.).

Лист актуализации рабочей программы дисциплины

«Разрушающие программные воздействия»

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» сентября 2020 № 2

Зав. кафедрой Татаев В.С.

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» мая 2021 № 10

Зав. кафедрой Татаев 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_____