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 ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ»

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 – Газимагомедов Ахмед Абдуллаевич, кандидат экономических наук, главный специалист научно – организационного отдела ДНЦ РАН.

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

Рабочая программа дисциплины «Безопасность вычислительных сетей» 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 вычислительных сетей» размещена на официальном сайте www.dgunh.ru.

Гасанова З.А. Рабочая программа по дисциплине «Безопасность вычислительных сетей» 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

Целью дисциплины является формирование компетенции обучающегося в области построения, эксплуатации и администрирования вычислительных сетей, принципов и методов защиты информации в компьютерных сетях с целью повышения надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации.

Задачами дисциплины являются:

- Рассмотреть архитектуру вычислительных сетей, правила организационной, технической и правовой защиты;
- Раскрыть принципы построения сетей и правления ими, методологии проектирования, развертывания и сопровождения безопасных сетей, обследования и анализа защищенности вычислительных сетей;
- Показать особенности программно-аппаратных и технических средств создания сетей, использования программных и аппаратных технологий защиты сетей;
- Ознакомиться с основными принципами и методами защиты информации в компьютерных сетях.

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

Код компетенции	Формулировка компетенции
ПСК	**ПРОФЕССИОНАЛЬНО-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 организации защиты обрабатываемой в них информации.	З1 – методологические и технические основы обеспечения информационной безопасности сетевых автоматизированных систем.	У1 – проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности.	В1 – навыками комплексного анализа и оценки сетевой безопасности.
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 компьютерных сетей.	У1 – реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения.	В1 – навыками комплексного проектирования, построения, обслуживания и администрирования защищенных вычислительных 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.	З1 – типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения.	У1 – разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства.	В1 – навыками проектирования защищенных сетей с целью обеспечения 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.	З1 – перспективные направления развития технологий обеспечения безопасности в сетях, современных проблемах науки информационной безопасности и роли и месте защиты информации в сетях при решении задач, связанных с обеспечением комплексной информационной безопасности.	У1 – применять защищенные протоколы и межсетевые экраны, необходимые для реализации системы защиты информации в сетях.	В1 – построения и эксплуатации вычислительных сетей; В2 – навыками использовать аппаратные и программные средства обеспечения информационной безопасности.

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

Код компетенции	Этапы формирования компетенций					
	Тема 1. Се-	Тема 2. Осно-	Тема 3.	Тема 4.	Тема 5. За-	Тема 6. Средства

	тевая архитектура.	вы организации и функциони рования сетей.	Типовые угрозы сетевой безопасн	Защита топологии сети.	щита сетевого трафика и компонентов сети.	повышения надежности функционирования сетей
ПСК-1	+	+				
ПСК-2				+	+	
ПСК-3			+	+	+	
ПСК-4						+

Код компетенции	Этапы формирования компетенций					
	Тема 7. Построение защищенных сетей на базе сетевых операционных систем	Тема 8. Политика безопасности и оценка безопасности сетевых операционных систем.	Тема 9. Безопасность глобальной сети Интернет	Тема 10. Защита каналов связи в глобальной сети.	Тема 11. Защита рабочего места пользователя в глобальной сети.	Тема 12. Уязвимость и защита базовых протоколов и служб.
ПСК-1		+	+	+	+	+
ПСК-2	+			+	+	+
ПСК-3	+	+		+	+	+
ПСК-4				+	+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ОД.5 «Безопасность вычислительных сетей» относится к базовой 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 «Информационные технологии», «Аппаратные средства вычислительной техники», «Основы информационной безопасности», «Сети и системы передачи информации», «Интернет-программирование».

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 и форму промежуточной аттестации

Объем дисциплины в зачетных единицах составляет **3** зачетные единицы.

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет **48** часов, в том числе:

на занятия лекционного типа – **16** ч.

на занятия семинарского типа – **32** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **24** ч.

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

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.	Сетевая архитектура	5	1	-	1	1	-	-	2	Проведение опроса Тестирование Выполнение лабораторной работы
2.	Основы организации и функционирования сетей	5	1	-	1	1	-	-	2	Проведение опроса Тестирование Выполнение лабораторной работы
3.	Типовые угрозы сетевой безопасности	5	1	-	1	1	-	-	2	Проведение опроса Выполнение лабораторной работы
4.	Защита топологии сети	5	1	-	1	1	-	-	2	Проведение опроса Тестирование Выполнение лабораторной работы

5.	Защита сетевого трафика и компонентов сети*	5	1*	-	1*	1*	-	-	2	Проведение опроса Тестирование Выполнение лабораторной работы
6.	Средства повышения надежности функционирования сетей*	5	1*	-	1*	1*	-	-	2	Проведение опроса Выполнение лабораторной работы
7.	Построение защищенных сетей на базе сетевых операционных систем*	8	2*	-	2*	2*	-	-	2	Проведение опроса Написание реферата Тестирование Выполнение лабораторной работы
8.	Политика безопасности и оценка безопасности сетевых операционных систем*	8	2*	-	2*	2*	-	-	2	Проведение опроса Выполнение лабораторной работы
9.	Безопасность глобальной сети Интернет	5	1	-	1	1	-	-	2	Проведение опроса Написание реферата Тестирование Выполнение лабораторной работы
10.	Защита каналов связи	5	1	-	1	1	-	-	2	Проведение опроса

	в глобальной сети*									Тестирование Выполнение лабораторной работы
11.	Защита рабочего места пользователя в глобальной сети	8	2	-	2	2	-	-	2	Проведение опроса Тестирование Выполнение лабораторной работы
12.	Уязвимость и защита базовых протоколов и служб*	8	2*	-	2*	2*	-	-	2	Проведение опроса Тестирование Выполнение лабораторной работы
	ИТОГО	**72**	**16**	**-**	**16**	**16**	**-**	**-**	**24**	
	Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)	**36**								**Контроль**
	ВСЕГО:	**108**								

*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.	-	Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов	Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.	http://biblioclub.ru/index.php?page=book&id=428820
2.	Голиков А.М.	Основы проектирования защищенных телекоммуникационных систем	Томск: ТУСУР, 2016. - 396 с.	http://biblioclub.ru/index.php?page=book&id=480796
3.	Голиков А.М.	Защита информации в инфокоммуникационных системах и сетях	Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с.	http://biblioclub.ru/index.php?page=book&id=480637
4.	Мэйволд Э.	Безопасность сетей	Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.	http://biblioclub.ru/index.php?page=book&id=429035
II. Дополнительная литература				
А) Дополнительная учебная литература				
1.	–	Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов	Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с.	http://biblioclub.ru/index.php?page=book&id=429834
2.	Проскуряков А.В.	Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций с.	Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону; Таганрог: Издательство Южного федерального уни-	http://biblioclub.ru/index.php?page=book&id=561238

			верситета, 2018. – 202	
3.	Сысоев Э.В.	Администрирование компьютерных сетей	Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. - 80 с.: ISBN 978-5-8265-1802-1	http://biblioclub.ru/index.php?page=book&id=499414

Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ	
1.	Федеральный закон от 27 июля 2006 г. № 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 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» 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 менеджмента информационной безопасности, рекомендуется использовать следующие Интернет-ресурсы:

1. http://www.fsb.ru/ – официальный сайт ФСБ России;
2. http://fstec.ru/ – официальный сайт ФСТЭК России;
3. http://www.consultant.ru/ – онлайн-версия информационно-правовой системы «КонсультантПлюс»;
4. http://Standartgost.ru–открытая база ГОСТов;
5. http://www.garant.ru/ – онлайн-версия информационно-правовой системы «Гарант».

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;
- Справочно-правовая система «КонсультантПлюс».

7.2. Перечень информационных справочных систем

- Информационно справочная система «КонсультантПлюс».

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);
- Государственный реестр сертифицированных средств защиты информации (http://clsz.fsb.ru/certification.htm);
- Научная электронная библиотека (https://elibrary.ru/).

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

Для преподавания дисциплины «Безопасность вычислительных сетей» используются следующие специальные помещения:

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).

Компьютерный класс, 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, акустическая система.

Персональные компьютеры – 20 ед.

Типовой комплект учебного оборудования «Криптографические системы».

Программно-аппаратные комплексы ViPNet

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 вычислительных сетей», обеспечивают развитие у обучающихся необходимых профессиональных знаний и навыков.

При освоении дисциплины «Организация защиты сведений, составляющих государственную тайну» используются следующие образовательные технологии:

- выполнение лабораторных работ для выработки навыков работы с правовыми и организационными документами, регламентирующими проведение мероприятий по защите сведений, составляющих государственную тайну;
- разбор кейс-задач в целях выработки навыков применения нормативной документации и принятия управленческих решений в различных ситуациях;
- проектная деятельность для выработки умений анализа информационных активов предприятия и разработки документов, регламентирующих деятельность по управлению информационной безопасностью в организации;
- проведение устных опросов в целях развития навыков поиска решений и межличностной коммуникации;
- внеаудиторная работа в форме обязательных консультаций и индивидуальных занятий со студентами (помощь в понимании тех или иных моделей и концепций, подготовка рефератов и эссе, а также тезисов для студенческих конференций и т.д.).

Лист актуализации рабочей программы дисциплины
«Безопасность вычислительных сетей»

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» сентября 2020 № 2

Зав. кафедрой Гатчев В.С.

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» мая 2021 № 10

Зав. кафедрой Гатчев 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_____