Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт дополнительного образования

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ (ДПП ПК)

Информационная безопасность систем и компьютерных сетей

наименование программы повышения квалификации

Объем: 72 часа

Махачкала
2022

Дополнительная профессионального программа повышения квалификации «**Информационная безопасность систем и компьютерных сетей**» разработана 2022г. в соответствии с Порядком организации и осуществления образовательной деятельности по дополнительным профессиональным программам (Утвержден приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. N 499).

Разработчик(и): __каф.ИТиБКС__к.ф-м.н, доцент Ахмедова З.Х._____

Дополнительная профессионального программа повышения квалификации утверждена на заседании методической комиссии факультета ИиИТ от «__3__» ___марта___2022г., протокол №__7__

Председатель _____ Ахмедова З.Х.

Согласовано:

Директор ИДО _____ Быкова В.И.

Начальник УМУ _____ Гасангаджиева А.Г.

Оглавление

I. ОБЩАЯ ХАРАКТЕРИСТИКА

1.1. Нормативно-правовые основания разработки программы

Нормативную правовую основу разработки программы составляют:

- Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Федеральный государственный образовательный стандарт высшего образования по направлению подготовки Информационная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. №1515;
- Устав федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Дагестанский государственный университет»
- Локальные нормативные акты ДГУ

1.2. Цель реализации ДПП ПК.

Цель обучения программы ДПК ПК «Информационная безопасность систем и компьютерных сетей», является подготовка высококвалифицированных специалистов для науки, производства на основе фундаментального образования, инфраструктур малого и среднего бизнеса, позволяющего выпускникам курсов быстро адаптироваться к потребностям общества.
Дополнительное образование по настоящей программе направлено на удовлетворение образовательных и профессиональных потребностей, профессиональное развитие человека, обеспечение соответствия его квалификации меняющимся условиям профессиональной деятельности и социальной среды.
Слушателями по программе «Информационная безопасность систем и компьютерных сетей» могут быть:
- преподаватели и научные работники сферы высшего образования регионов РФ.
- руководители и сотрудники в сфере государственного и муниципального управления, бизнеса

1.3 Требования к слушателю.

На курс повышения квалификации принимаются слушатели, имеющие законченное среднее профессиональное или высшее образование, связанные в своей профессиональной деятельности;
- с базовыми понятиями управления информационной безопасности малого и среднего бизнеса;
- с применением современных технических и аппаратных средств обеспечения информационной безопасностью;
- с технологией использования современных механизмов обеспечения сетевой безопасности;
- с криптографией и инфраструктурой открытых ключей.

Возрастных ограничений нет.

Требования к результатам освоения программы
Слушатель, освоивший программу должен обладать профессиональными компетенциями, включающими в себя способность:

Знать:

- основы теории информации и основные угрозы в области информационной безопасности предприятия; об умышленном и непреднамеренном разрушении системы передачи информации в целях управления

- основные положения сбора информации и проведения анализа при организации защиты операционных систем.

- основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования;

Уметь:

- использовать признаки несанкционированного доступа к информации в местах ее хранения, в процессе ее передачи от одного пользователя к другому путем перехвата каналов связи и компрометации шифров для построения системы защиты;

- анализировать сложившуюся ситуацию при организации защиты операционных систем;

- использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки; применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

Владеть:

- методами выявления рисков и угроз в области информационной безопасности предприятия

- способами и методами анализа защищенности операционных систем

- криптографической терминологией; навыками использования типовых криптографических алгоритмов

1.4. Объем и срок получения образования ДПП ПК.

Объем: 72 часа

Срок реализации программы: 2 недели

1.5. Виды и задачи профессиональной деятельности.

По дополнительной профессиональной программе в соответствии профессиональным стандартом «Информационная безопасность систем и безопасность компьютерных систем», слушатели будут подготовлены к следующим видам профессиональной деятельности**:** организационно-управленческая эксплуатационная деятельность.

Слушатель, освоивший дополнительную профессиональную программу готов решать следующие профессиональные задачи:

Организационно-управленческая:

− способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

− способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

− способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

Эксплуатационная деятельность:

− способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ;

− способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ;

− способностью администрировать подсистемы информационной безопасности объекта защиты;

− способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

− способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

− способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ;

1.6. Планируемые результаты освоения ДПП ПК

Слушатель, освоивший дополнительную профессиональную программу, должен обладать следующими профессиональными компетенциями, на которые ориентирована программа повышения квалификации:

Код компетенции	Наименование профессиональных компетенций
Организационно-управленческая деятельность:	
ПК 1.1	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК 1.2	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК 1.3.	Способностью организации взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия
Эксплуатационная деятельность:	
ПК 2.1	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК 2.2	способностью выполнять организацию работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации
ПК 2.3.	способностью администрировать подсистемы информационной безопасности объекта защиты

II. ДОКУМЕНТЫ, РЕГЛАМЕНТИРУЮЩИЕ СОДЕРЖАНИЕ И ОРГАНИЗАЦИЮ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПРИ РЕАЛИЗАЦИИ ДПП ПК

2.1. Учебный план.

Объем обязательной части образовательной программы ДПП ПК определяется с учетом требований ДПП ПК.

контактная работа - 36ч
лекции – 10часов
практические занятия и семинары – 10 часов
Лабораторные работы – 16 часов
самостоятельная работа – 34 часов
итоговая аттестация – 2 ч

Срок реализации программы: 2 недели

2.2. Календарный учебный график.

В календарный учебный график (Приложение 2) включены:

- даты начала и окончания обучения;
- продолжительность обучения
- сроки проведения промежуточных аттестаций.

2.3. Матрица компетенций, формируемых в результате освоения программы.

Результаты освоения ДПП ПК определяются приобретаемыми слушателями компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности. (Приложение 3)

2.4. Рабочие программы дисциплин/модулей.

Рабочие программы дисциплин/модулей определяет объем, содержание, порядок изучения и преподавания дисциплин/модулей, а также способы контроля результатов ее усвоения, соответствующий требованиям по данной программе и формирующие одну или несколько определенных профессиональных компетенций, сопровождаемая контролем знаний и умений обучаемых на выходе.

2.5. Итоговая аттестация.

Демонстрация слушателями сформированных профессиональных компетенций будет проводиться в рамках круглого стола.

III. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Организационно-педагогические условия реализации программы.

Качество повышения квалификации будет обеспечено высококвалифицированным профессорско-преподавательским составом ДГУ, других ведущих вузов РФ, а также специалистами-практиками.

3.2. Материально-технические условия реализации программы.

Материально-техническая база обучения с использованием ДОТ включает следующие составляющие:

- каналы связи;
- компьютерное оборудование;
- периферийное оборудование;
- программное обеспечение;
- систему электронного дистанционного обучения, обеспечивающую формирование информационной образовательной среды

Помещения для осуществления образовательного процесса	Перечень основного оборудования (с указанием кол-ва посадочных мест)	Адрес (местоположение)
Аудитории для проведения лекционных занятий		
Лекционные аудитории	Интерактивная доска, ноутбук; проектор. Количество посадочных мест – 30.	Ауд. 3-14, 4-16, 2-10, учебный корпус № 8, г. Махачкала, ул. Джержинского, 12.
Аудитории для проведения практических занятий, контроля успеваемости		

Сетевая лаборатория Cisco	Компьютеры с выходом в Интернет и доступом в электронную информационно- образовательную среду вуза. Количество посадочных мест – 15.	Компьютерный зал № 2 учебный корпус № 3, г.Махачкала, ул. Джержинского, 12.
Помещения для самостоятельной работы		
Компьютерные классы	Компьютеры с выходом в Интернет и доступом в электронную информационно- образовательную среду вуза. Количество посадочных мест – 15	Компьютерный зал № 1, учебный корпус № 3, г. Махачкала, ул. Джержинского, 12.
Читальный зал библиотеки ДГУ	Компьютеры с выходом в Интернет и доступом в электронную информационно- образовательную среду вуза. Количество посадочных мест – 30.	Электронный читальный зал научной библиотеки ДГУ, г. Махачкала, ул. Батырая, 4

Приложение 1

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт дополнительного образования

УЧЕБНЫЙ ПЛАН
дополнительной профессионального повышения квалификации

Информационная безопасность систем и компьютерных сетей

(наименование программы повышения квалификации)

Форма обучения - очная

Махачкала
2022

Программа повышения квалификации

«Информационная безопасность систем и компьютерных сетей»

№ п/п	Наименование модуля/темы	Всего, час	В т.ч. контактных часов	по видам учебных занятий:				Самост. работа	Форма контроля (экзамен, дифференцированный зачет, зачет)
				Лекции	Практические занятия и семинары	Лабораторные	консультации		
	Модуль 1.	36	24	6	6	12		12	
1.	Основы управления информационной безопасностью	12	8	2	2	4		4	Собеседование
2.	Интернет- безопасность	12	8	2	2	4		4	Собеседование
3.	Организация технической защиты информации	12	8	2	2	4		4	Собеседование
	Модуль 2.	34	12	4	4	4		22	
1	Безопасность операционных систем	18	6	2	2	2		12	Собеседование
2	Безопасность компьютерных сетей	16	6	2	2	2		10	Собеседование
	ИТОГОВАЯ АТТЕСТАЦИЯ	36					2		Круглый стол
	ИТОГО:	**72**	**36**	**10**	**10**	**16**	**2**	**34**	

Приложение 2

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт дополнительного образования

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК
дополнительной профессиональной программы повышения квалификации «Информационная безопасность систем и компьютерных сетей»

Форма обучения – очная

Месяц									

Условные обозначения:

- теоретическое обучение	**ИА**- итоговая аттестация	= -нет день недели

Приложение 3

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт дополнительного образования

МАТРИЦА

компетенций при подготовке дополнительной профессиональной программы повышения квалификации
«Информационная безопасность систем и компьютерных сетей»

Форма обучения – очная

Махачкала 2022

Реализуемые виды профессиональной деятельности:

1. Организационно-управленческая деятельность (ПК1.1., ПК-1.2., ПК-1.3.)
2. Эксплуатационная деятельность (ПК-2.1., ПК-2.2)

Наименование модулей в соответствии с учебным планом	Профессиональные компетенции					
	Организационно-управленческая деятельность			Эксплуатационная деятельность		
	ПК 1.1	ПК 1.2	ПК 1.3	ПК 2.1	ПК 2.2	ПК 2.3
Основы управления информационной безопасностью		+		+	+	
Информационная безопасность и интернет	+		+			
Криптографическая защита информации				+	+	
Информационная безопасность компьютерных сетей					+	+
Итоговая аттестация	+	+	+	+	+	+

Код дополнительной профессиональной компетенции	**Наименование профессиональных компетенций**
Организационно-управленческая деятельность:	
ПК 1.1	Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК 1.2	Способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК 1.3.	Способностью организации взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия
Эксплуатационная деятельность:	
ПК 2.1	Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК 2.2	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК 2.3.	способностью администрировать подсистемы информационной безопасности объекта защиты

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт дополнительного образования

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Основы управления информационной безопасностью

Кафедра Информационных технологий и безопасности компьютерных систем
факультета Информатики и информационных технологий

Дополнительная профессиональная программы
повышения квалификации

Информационная безопасность систем и компьютерных сетей

Форма обучения – очная

Махачкала

2022

1. Цели освоения модуля

Целями изучения модуля «Основы управления информационной безопасностью» является:

формирование навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ;

создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ;

развитие способностей по использованию существующей системы управления информационной безопасности.

2. Компетенции обучающегося, формируемые в результате освоения модуля (перечень планируемых результатов обучения).

Код компетенции	Наименование компетенции	Планируемые результаты обучения	Процедура оценивания результатов освоения
ПК 1.1	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**Знает:** основы теории информации и основные угрозы в области информационной безопасности предприятия; об умышленном и непреднамеренном разрушении системы передачи информации в целях управления; **Умеет:** использовать признаки несанкционированного доступа к информации в местах ее хранения, в процессе ее передачи от одного пользователя к другому путем перехвата каналов связи и компрометации шифров для построения системы защиты; **Владеет:** методами выявления рисков и угроз в области информационной безопасности предприятия	Собеседование
ПК 1.2	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**Знает:** основы теории информации и основные угрозы в области информационной безопасности предприятия; **Умеет:**	Реферат

		осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты; **Владеет**: профессиональной терминологией	
ПК 1.3.	способностью 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	Знать периоды развития информационной безопасности, этапы развития вычислительной техники, критерии периодизации, развитие элементной базы, ведущих ученых в этой области, развитие отечественной вычислительной техники и информационной безопасности в России. Умеет: осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе мораль нонравственных и правовых норм, соблюдать принципы профессиональной этики. Владеет: навыками: проводить поиск информации по требуемой тематике, аргументировано и последовательно излагать свое мнение, проводить сравнительный анализ состояния общества и вычислительной техники. Обладать способностью к логически правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, про-	Собеседование

		гнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания.	

3. Объем, структура и содержание модуля.

3.1. Объем модуля составляет 36 академических часов.

3.2. Структура модуля.

№ п/п	Разделы и темы модуля	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа	
1.	Угрозы информационной безопасности в информационных системах	2	2	4	4	
2.	Методы оценки рисков информационной безопасности компании		2	4	4	
3.	Правовые меры обеспечения безопасности компьютерных информационных систем	2		4		
4.	Базовые вопросы управления ИБ. Процессный подход	2	2		4	собеседование
	ИТОГО:	6	6	12	12	

3.3. Содержание модуля, структурированное по темам (разделам).

3.3.1. Содержание лекционных занятий по модулю.

Тема 1: "Угрозы информационной безопасности в информационных системах"

Содержание темы.

1. Основные определения и критерии классификации угроз.
2. Основные угрозы доступности.

3. Основные угрозы целостности.
4. Основные угрозы конфиденциальности.
5. Вредительские программы

Тема 2. Методы оценки рисков информационной безопасности компании

Содержание темы.

1. Управление рисками. Основные понятия.
2. Метод оценки рисков на основе модели угроз и уязвимостей

Тема 3. Правовые меры обеспечения безопасности компьютерных информационных систем

Содержание темы.

1. Обзор российского законодательства в области информационной безопасности
2. Закон "Об информации, информатизации и защите информации"
3. Другие законы и нормативные акты
4. О текущем состоянии российского законодательства в области информационной безопасности
5. Обзор зарубежного законодательства в области информационной безопасности

3.3.2. Содержание практических занятий по модулю.

Тема 1: "Угрозы информационной безопасности в информационных системах"

Содержание темы.

- Анализ модели угроз ИБ и уязвимостей
- Анализ модели информационных потоков

Тема 2. Базовые вопросы управления ИБ. Процессный подход

Содержание темы.

Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, ISO/IEC 25999 и др.).

Тема 3. Правовые меры обеспечения безопасности компьютерных информационных систем

Содержание темы.

Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

4. Образовательные технологии

В процессе преподавания модуля применяются следующие образовательные технологии: развивающее обучение, проблемное обучение, коллективная система обучения, лекционно-зачетная система обучения, технология развития критического мышления. При чтении данного курса применяются такие виды лекций, как вводная, лекция-информация, обзорная, проблемная, лекция-визуализация.

Для реализации компетентностного подхода предусматривается использование в учебном процессе активных и интерактивных форм проведения аудиторных и внеаудиторных занятий интерактивного, разбор конкретных ситуаций с целью формирования и развития профессиональных навыков обучающихся.

Владение навыками работы с интернет-ресурсами в области ИБ. Практические занятия проходят в сетевой лаборатории 2.1.2

5.Учебно-методическое обеспечение самостоятельной работы студентов.

При изучении модуля обязательными являются следующие виды самостоятельной работы:

- разбор теоретического материала по учебным пособиям и конспектам лекций;
- самостоятельное изучение указанных теоретических вопросов; подготовка к проведению ситуационных моделей в интерактивной форме;

	Наименование	**Содержание**
1	Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ	Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ.Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации.
2.	Основные процессы СУИБ. Обязательная документация СУИБ	Риск. Вероятность реализации. Уязвимость
3.	Эксплуатация и независимый аудит СУИБ.	Информационная безопасность - сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность.

Виды и порядок выполнения самостоятельной работы:

1. Изучение рекомендованной основной и дополнительной литературы
2. Информационный поиск и работа с интернет-ресурсами.
3. Выполнение практических работ, их анализ, составление резюме и выводов
4. Подготовка к итоговой аттестации.

6. Учебно-методическое обеспечение модуля.

Основная литература:

1. Правовое обеспечение информационной безопасности : [учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность", 075500 "Комплекс. обеспечение информ. безопасности и автоматизир. систем", 075600 "Информ. безопасность телекоммуникац. систем" / С.Я.Казанцев и др.]; под ред. С.Я.Казанцева. - М. : Academia, 2005. - 239 с. : ил. ; 22 см. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 235-237. - Допущено УМО. - ISBN 5-7695-1209-1 : 129-47

2. Филин С. А. Информационная безопасность : учеб. пособие / Филин, Сергей Александрович. - М. : Альфа-Пресс, 2006. - 411 с. - ISBN 5-94280-163-0 : 129-03.

3. Галатенко В. А. Стандарты информационной безопасности : курс лекций: учеб. пособие / Галатенко, Владимир Антонович ; под ред. В.Б.Бетелина; Интернет-ун-т информ. технологий. - 2-е изд. - М. : ИНТУИТ.ру, 2006. - 263 с. - (Основы информационных технологий). - ISBN 5-9556-0053-1 : 176-00.

4. Уколов В. Ф. Теория управления : учеб. для вузов / Уколов, Владимир Фёдорович, А. М. Масс, И. К. Быстряков. - 3-е изд., доп. - М. : Экономика, 2007. - 696 с. - Допущено МО РФ. - ISBN 978-5-282-02698-6 : 260-00

5. Галатенко В. А. Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.

6. Петров С. В. Информационная безопасность : учеб. пособие /. - Новосибирск: М.: АРТА,

2012. - 439-77.

Дополнительная литература:

1. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.Международный стандарт. ISO/IEC 27000:2005 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы./ http://www.27000.org/
2. Аудит информационной безопасности. Под ред. А.П.Курило. – М: БДЦ-Пресс, 2014.
3. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005)./ http://www.27000.org/
4. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью./ http://www.27000.org/Международный стандарт. ISO/IEC 27003:2005 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью./ http://www.27000.org/
5. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью./ http://www.27000.org/
6. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности./ http://www.27000.org/
7. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью./ http://www.27000.org/

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения модуля.

1. ЭБС IPRbooks: http://www.iprbookshop/ru/
2. Электронно-библиотечная система «Университетская библиотека онлайн» (архив):www.biblioclub.ru
3. Единое окно доступа к образовательным ресурсам. http://window.edu.ru/
4. http://www.microsoft.com/msf
5. http://www.uml.org
6. http://www.wikipedia.org

8. Методические указания для обучающихся по освоению модуля.

Перечень учебно-методических изданий, рекомендуемых слушателям, для подготовки к занятиям представлен в разделе «Учебно-методическое обеспечение. Литература». Дополнительно для выполнения практических заданий каждый слушатель обеспечивается компьютерами, программными продуктами.

Лекционный курс. Лекция является основной формой обучения в высшем учебном заведении. В ходе лекционного курса проводится систематическое изложение современных научных материалов.

Практические занятия. В ходе практических занятий слушатель под руководством преподавателя выполняет комплекс практических заданий, позволяющих закрепить лекционный материал по изучаемой теме, научиться выполнять наблюдения, их камеральную обработку, статистическую обработку полученных данных, научиться работать с методиками, руководящими документами, информацией различного уровня.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Образовательный процесс осуществляется с применением локальных и распределенных информационных технологий (таблица 1, 2).

Таблица 1.

Группа программных средств	Наименование программного продукта
Офисные программы	Microsoft Office
	Libre Office
Распознавание текста и речи	ABBYY FineReader 2010
Средства разработки	MicroSoft Visual Studio 2015 MicroSoft SQL Server 2012 VipNet Client 4 Dallas Lock 8.0 КриптоПро CSP

Таблица 2 – Распределенные информационные технологии

Группа	Наименование
Система тестирования	Система сетевого компьютерного тестирования ДГУ www.ts.icc.dgu.ru
Библиотеки и образовательные ресурсы	Электронная библиотека ДГУ http://www.elib.dgu.ru
	Кафедральные сайты ДГУ http://cafedra.dgu.ru
	Сайте электронных образовательных ресурсов ДГУ http://eor.dgu.ru
Система электронного обучения	Сервер электронного обучения moodle http://moodle.dgu.ru

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

1. Учебная аудитория на 50 мест с мультимедийным проектором, ноутбуком и экраном для проведения лекционных занятий
2. Учебные аудитории (компьютерные классы) для проведения практических занятий (с установленным программным обеспечением).
3. Методическое пособие с изложением технологии выполнения практических работ.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет информатики и информационных технологий

Кафедра информатики и информационных технологий

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Безопасность компьютерных сетей

Кафедра ИТиБКС факультета ИиИТ

Дополнительная профессиональная программа

повышения квалификации

Информационная безопасность систем и компьютерных сетей

наименование программы повышения квалификации

Форма обучения – очная

Махачкала
2022 год

1. Цели освоения модуля

Целью модуля является базовые принципы обеспечения сетевой и системной безопасности инфраструктур малого и среднего бизнеса систематизация и расширение знаний приемов и методов работы с защищенными инфраструктурами с использованием аппаратных и программных компонентов обеспечения информационной безопасности.

Задачи освоения модуля – формирование у обучающихся необходимых теоретических знаний и навыков для организации базовой информационной безопасности ИТ- инфраструктуры.

2. Компетенции обучающегося, формируемые в результате освоения модуля (перечень планируемых результатов обучения).

Код компетенции	Наименование компетенции	Планируемые результаты обучения	Процедура оценивания результатов освоения
ПК-2.1	− способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать: основные принципы и способы кодирования и декодирования; характеристики кодов разного типа, понятие оптимального и помехоустойчивого кодирования; методы исследования кодов и их применений в ЭВМ и системах защиты информации. основные классы кодов, их параметры и алгоритмы кодирования/декодирования. Уметь кодировать и декодировать сообщения источника одним из изученных кодов, оценивать его оптимальность и помехоустойчивость; оценивать количество информации, вероятность ошибки на выходе канала связи и вероятность ошибочного декодирования; выбирать, реализовывать и применять кодирующие и декодирующие алгоритмы для различных классов задач. Владеть: основными методами кодирования и декодирования информации для различных задач.	Собеседование
ПК-2.2.	Способность выполнять работы по установке, настройке и обслуживанию программных, про-	**знать:** основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; модели шифров и	Собеседование

	граммно-аппаратных (в том числе криптографических и технических средств защиты информации).	математические методы их исследования; принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах; **уметь:** использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки; применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; уметь пользоваться научно-технической литературой в области криптографии; **владеть:** криптографической терминологией; навыками использования типовых криптографических алгоритмов; навыками использования ПЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии.	
ПК-2.3	способность администрировать подсистемы информационной безопасности объекта защиты	Знает: основные положения сбора информации и проведения анализа при организации защиты операционных систем. Умеет: анализировать сложившуюся ситуацию при организации защиты операционных систем Владеет: способами и методами анализа защищенности операционных систем	Собеседование

3. Объем, структура и содержание модуля.

3.1. Объем модуля составляет 34 академических часов.

3.2. Структура модуля.

№ п/п	Темы модуля	Виды учебной работы и трудоемкость			Самостоятельная работа	Формы текущего контроля успеваемости Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторная работа		
1	Методы статистического кодирования	2			6	
2.	Серверные операционные системы как средство защиты информационной безопасности		2	4	6	
3.	Сетевые протоколы и службы		2		4	
4	Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ. Композиционный шифр.	2		4	6	
	ИТОГО:	4	4	4	22	Собеседование

3.3. Содержание модуля, структурированное по темам (разделам).

3.3.1 Лекционные занятия

Тема 1. Методы статистического кодирования. Простейшие алгоритмы сжатия информации.

Тема 2. Серверные операционные системы как средство защиты информационной безопасности.

- Серверные ОС семейства UNIX
- Серверные ОС семейства Windows

Файловые системы. Управление доступом

Тема 3. Сетевые протоколы и службы.

- Стек протоколов TCP/IP
- Списки контроля доступа, NAT-PAT

Тема 4.
Классификация шифров перестановки. Композиционный шифр.
Классификация шифров перестановки. Примеры шифров перестановки и их крипто-

анализ. Композиционный шифр.

3.3.2 Практические занятия

Тема 1. Адаптивные алгоритмы сжатия. Адаптивный код Хаффмана. Адаптивное арифметическое кодирования. Код «Стопка книг». Интервальный код. Частотный код

Тема 2.

Серверные операционные системы как средство защиты информационной безопасности.

- Серверные ОС семейства UNIX
- Серверные ОС семейства Windows
- Файловые системы. Управление доступом

Тема 3.

Сетевые протоколы и службы.

- Стек протоколов TCP/IP
- Списки контроля доступа, NAT-PAT

Тема 4.

Шифр простой замены. Шифр Виженера.

- Простейшие методы шифрования с закрытым ключом. Шифр простой замены. Шифр Виженера. Частотный анализ.

4.Образовательные технологии

Предусмотрено сочетание традиционных видов учебной активности, таких как конспектирование лекций и контроль усвоения теоретического материала в виде коллоквиумов, так и интерактивных технологий, таких как собеседования, ситуационные игры на выбор методов защиты информации на практических занятиях.

5. Учебно-методическое обеспечение самостоятельной работы студентов.

Наименование темы	Содержание
Алгоритмы шифрования данных	Изучение и конспектирование основной и дополнительной литературы Работа со справочными материалами (словарями, энциклопедиями) Работа с учебно-методическими материалами Изучение образовательных ресурсов интернет
Аппаратные средства обеспечения ИБ	Изучение и конспектирование основной и дополнительной литературы Работа со справочными материалами (словарями, энциклопедиями) Работа с учебно-

	методическими материалами Изучение образовательных ресурсов интернет

Виды и порядок выполнения самостоятельной работы:
1. Изучение рекомендованной основной и дополнительной литературы
2. Информационный поиск и работа с интернет-ресурсами.
3. Выполнение практических работ, их анализ, составление резюме и выводов
4.Подготовка к итоговой аттестации.

6. Учебно-методическое обеспечение модуля.

Методические материалы для обеспечения СРС готовятся преподавателем и могут размещаться на персональном сайте преподавателя, либо на платформе электронного обучения. Кроме того, на основе рабочей программы модуля может составляться план-график, где преподаватель устанавливает рекомендуемые сроки предоставления на проверку результатов самостоятельной работы студента: контрольных работ, отчетов по лабораторным практикумам, индивидуальных домашних заданий, рефератов, курсовых работ и др., советует использование основных и дополнительных источников литературы. http://eor.dgu.ru/Default/NProfileUMK/?code=13.03.02&profileId=43

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения модуля.

1.eLIBRARY.RU [Электронный ресурс]: научная электронная библиотека. – Доступ зарегистрированным пользователям по паролю. – Режим доступа: http://elibrary.ru/defaultx.asp (дата обращения: 10.09.2019).

2. RUNNet [Электронный ресурс]: федеральная университетская компьютерная сеть. – Режим доступа: http://www.runnet.ru/, свободный (дата обращения: 25.09.2019).

3. БИНОМ. Лаборатория знаний [Электронный ресурс]: [официальный сайт]. – Режим доступа: http://lbz.ru/, свободный (дата обращения: 25.09.2019).

4. Википедия [Электронный ресурс]: свободная энцикл. – Режим доступа: http://ru.wikipedia.org/wiki, свободный (дата обращения: 15.09.2019).

5. Высшая аттестационная комиссия [Электронный ресурс]: [официальный сайт]. – Режим доступа: http://vak.ed.gov.ru/, свободный (дата обращения: 25.09.2019).

6. Государственный НИИ информационных технологий и телекоммуникаций «Информика» [Электронный ресурс]: [официальный сайт]. – Режим доступа: http://www.informika.ru/, свободный (дата обращения: 10.09.2019).

7. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс]: федеральный портал. – Режим доступа: http://school-collection.edu.ru, свободный (дата обращения: 15.09.2019).

8. Единое окно доступа к образовательным ресурсам [Электронный ресурс]: федеральный портал. – Режим доступа: http://window.edu.ru, свободный (дата обращения: 15.09.2019).

9.Инновационные решения и технологии для сферы образования [Электронный ресурс]: автоматизированные системы управления сферой образования. – Режим доступа: http://www.ir-tech.ru/, свободный (дата обращения: 25.09.2019).

10.Информатика и информационно-коммуникационные технологии в школе [Электронный ресурс]: информационно-образовательный портал. – Режим доступа: http://klyaksa.net/, свободный (дата обращения: 25.09.2019).

13. Информационно-коммуникационные технологии в образовании [Электронный ресурс]: система федеральных образовательных порталов. – Режим доступа: http://www.ict.edu.ru, свободный (дата обращения: 15.09.2019).

14. Министерство образования и науки Российской Федерации [Электронный ресурс]: [официальный сайт]. – Режим доступа: http://минобрнауки.рф/, свободный (дата обращения: 10.08.2019).

15. Педсовет [Электронный ресурс]: персональный помощник педагога. – Режим доступа: https://pedsovet.org/beta, свободный (дата обращения: 25.08.2019).

16. Российская государственная библиотека [Электронный ресурс]: [официальный сайт]. – Режим доступа: http://www.rsl.ru/, свободный (дата обращения 25.08.2019).

17. Российский общеобразовательный портал [Электронный ресурс]: [образовательный портал]. – Режим доступа: http://www.school.edu.ru, свободный (дата обращения: 15.09.2019).

18. Федеральный институт развития образования [Электронный ресурс]: [официальный сайт]. – Режим доступа: http://www.firo.ru/, свободный (дата обращения: 25.08.2019).

19. Федеральный интернет-экзамен в сфере профессионального образования (ФЭПО) [Электронный ресурс]: [сайт]. – Режим доступа: http://fepo.iexam.ru/, свободный (дата обращения: 25.09.2019).

20.Федеральный центр информационно-образовательных ресурсов [Электронный ресурс] // Единое окно доступа к образовательным ресурсам. – Режим доступа: http://fcior.edu.ru, свободный (дата обращения: 15.09.2019).

21.Электронный каталог НБ ДГУ[Электронный ресурс]: база данных содержит сведения овсех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: http://elib.dgu.ru, свободный (дата обращения: 21.08.2019).

8. Методические указания для обучающихся по освоению модуля.

Перечень учебно-методических изданий, рекомендуемых слушателям, для подготовки к занятиям представлен в разделе «Учебно-методическое обеспечение. Литература». Дополнительно для выполнения практических заданий каждый слушатель обеспечивается компьютерами, программными продуктами.

Лекционный курс. Лекция является основной формой обучения в высшем учебном заведении. В ходе лекционного курса проводится систематическое изложение современных научных материалов.

Практические занятия. В ходе практических занятий слушатель под руководством преподавателя выполняет комплекс практических заданий, позволяющих закрепить лекционный материал по изучаемой теме, научиться выполнять наблюдения, их камеральную обработку, статистическую обработку полученных данных, научиться работать с методиками, руководящими документами, информацией различного уровня.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Программные продукты

- Операционная система: Windows Server 2019, Ubuntu server.
- Программные средства сжатия данных. WinRAR. WinArj. WinZip.
- Языки программирования
- На лабораторных занятиях используются программные продукты PowerPoint, Flash.
- Лабораторные занятие проводятся в классах персональных ЭВМ; операционная система WINDOWS 10.

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

Технические средства

- Компьютерный класс;
- Глобальная и локальная вычислительная сеть; - 11 компьютеров
- Сетевое оборудование CISCO и DLINK;

а) Мультимедийная аудитория - для лекций;

б) Компьютерный класс, оборудованный для проведения практических работ

средствами оргтехники, персональными компьютерами, объединенными в сеть с выходом в Интернет – для практических занятий.

Для проведения лекционных занятий требуется аудитория на курс, оборудованная интерактивной доской, мультимедийным проектором с экраном. Для проведения практических занятий требуется аудитория на группу студентов, оборудованная интерактивной доской, мультимедийным проектором с экраном. Для проведения практических занятий на ПЭВМ требуется компьютерный класс с установленной на ПЭВМ MSOffice 2017. В частности, MSWord, MSExcel, MSPowerpoint.

Для проведения практических и лабораторных занятий на требуется компьютерный класс с серверным и коммуникационным оборудованием на базе серверных ОС Windows Server 2012.