МИНИСТЕРСТВО ОБРАЗОВАНИЯ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ
Дербентский филиал Общества с ограниченной ответственностью
«Азербайджанский Государственный Экономический Университет»

Утверждаю
Ректор, профессор
_____Мурадов А.Д.
«___»_____2017 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.17 Информационная безопасность

Специальность
09.02.04 Информационные системы (по отраслям)

Квалификация
техник по информационным системам

Программа подготовки
базовая

Форма обучения
очная

Рецензент: Гюльмагомедов Т.Х. – кандидат технических наук, доцент

Рабочая программа предназначена для преподавания общепрофессиональной дисциплины вариативной части профессионального учебного цикла студентам очной формы обучения по специальности 09.02.04 Информационные системы (по отраслям.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.04 Информационные системы (по отраслям, утвержденного приказом Министерства образования и науки Российской Федерации от 14 мая 2014 г. № 525.

Составитель _____ Вурдиханов В.Р. – кандидат технических наук, доцент

Содержание

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины: иметь представление и владеть методами и средствами защиты информации.

Задачи:

- иметь представление об основных понятиях и моделях; о стандартах безопасности; о криптографических методах; о средствах и методах защиты информации в сети;
- изучить понятия криптография, стеганография, аутентификация, невозможность отказа от авторства; политика безопасности в мировых законах и законах РФ; криптографические методы и алгоритмы; алгоритмы криптоанализа; алгоритмы идентификации пользователя на биометрических принципах; средства защиты сетей и нормативные требования к системам защиты информации;
- уметь составлять криптосистемы; манипулировать с данными; выбирать наиболее подходящий из методов защиты информации.

2. Место дисциплины в структуре ППССЗ

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности (специальностям) СПО 09.02.04 Информационные системы (по отраслям) на профильном уровне в пределах программы подготовки специалистов среднего звена.

Дисциплина «Информационная безопасность» является вариативной частью профессионального цикла очной формы обучения по специальности 09.02.04 Информационные системы (по отраслям).

3. Требования к результатам освоения содержания дисциплины

В процесс изучения дисциплины «Информационная безопасность» обучаемый должен обладать компетенциями:

В ходе изучения дисциплины ставиться задача формирования следующих компетенций:

а) общие:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности

б) профессиональные:

ПК 1.2. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

ПК 1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

ПК 2.1. Участвовать в разработке технического задания.

ПК 2.2. Программировать в соответствии с требованиями технического задания.

ПК 2.6. Использовать критерии оценки качества и надежности функционирования информационной системы.

В результате освоения дисциплины обучающийся должен **уметь:**

- применять правовые, организационные, технические и программные средства защиты информации;
- создавать программные средства защиты информации.

В результате освоения дисциплины обучающийся должен **знать**:

- источники возникновения информационных угроз;
- модели и принципы защиты информации от несанкционированного доступа;
- методы антивирусной защиты информации;
- состав и методы организационно-правовой защиты информации.

4. Содержание и структура дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	**81**
Обязательная аудиторная учебная нагрузка (всего)	**54**
в том числе:	
лекции (Л)	40
практические занятия (ПЗ)	14
Самостоятельная работа обучающегося (СР) (всего) **в том числе:**	**23**
написание рефератов, сообщений, составление презентаций	23
Консультации (К)	**4**
Итоговая аттестация в форме ***дифференцированного зачета***	

4.2. Тематический план изучения дисциплины

№ занятия	Наименование разделов и тем дисциплины	Количество часов				
		Всего	Аудиторная работа			Внеауд. работа СР
			Л	ПЗ	К	
	Раздел 1. Основы информационной безопасности	**7**	**4**		**1**	**2**
1	Вводное занятие. Основные понятия защиты информации	1	1			
2	Общие проблемы защиты информации. Безопасность в информационной среде. Классификация средств защиты	1	1			
3	Угрозы информационной безопасности и каналы утечки информации	2	1			1
4	Инженерно-технические средства защиты информации. Программно-аппаратные средства защиты	3	1		1	1
	Раздел 2. Криптографические методы информационной безопасности	**27**	**14**	**4**	**1**	**8**
5	История криптографической деятельности. Основные понятия, определения, композиции и синтез шифров	1	1			
6	Простейшие шифры с симметричными ключами: замены	2	1			1
7	Простейшие шифры с симметричными ключами: перестановки	2	1			1
8	Простейшие шифры с симметричными ключами: гаммирование	2	1			1
9	Шифрование с симметричными ключами при помощи аналитических преобразований	4	2	2		
10	Смешанные методы шифрования. Криптографические системы DES и ГОСТ 28147-89	3	2			1
11	Асимметричные шифры. Системы с открытыми ключами	3	2			1
12	Системы с открытыми ключами. Электронно-цифровая подпись	3	2			1
13	Криптографические протоколы: аутентификации, обмена ключами. Специфические протоколы	2	1	-		1
14	Оценка криптостойкости шифров. Элементы криптоанализа	5	1	2	1	1
	Раздел 3. Методы и средства защиты информации	**17**	**8**	**4**	**1**	**4**

15	Стеганография. Становление как науки. Компьютерная стеганография и её применение	2	2			
16	Туннелирование. Управление. Обеспечение отказоустойчивости и обслуживаемости	3	2			1
17	Методы идентификации и аутентификации пользователей на основе паролей	2	1			1
18	Аутентификация пользователя по биометрическим характеристикам	4	1	2		1
19	Парольная защита. Способы атаки на пароль. Обеспечение безопасности пароля	6	2	2	1	1
	Раздел 4. Аппаратные и программные средства защиты компьютерной информации	**30**	**14**	**6**	**1**	**9**
20	Компьютерные вирусы и средства защиты от них. Характер проявления компьютерных вирусов	1	1			
21	Компьютерная преступность. Разновидности компьютерного пиратства	2	1			1
22	Угрозы информационной безопасности при подключении к Интернет. Методы взлома интрасетей	3	1	2		
23	Обзор технических и программных средств обеспечения безопасности компьютерных сетей	2	1			1
24	Средства защиты сети: межсетевые экраны, виртуальные частные сети, системы обнаружения вторжений	2	1			1
25	Средства защиты информации от несанкционированного доступа	2	1			1
26	Защита от несанкционированного доступа в операционной системе Windows	5	2	2		1
27	Защита документов в Microsoft Office. Защита баз данных	3	2			1
28	Организационно-правовое обеспече-ние информационной безопасности	3	2			1
29	Актуальные проблемы уголовно-правовой борьбы с посягательствами на компьютерную информацию	2	1			1
30	Зачетное занятие. Подведение итогов	5	1	2	1	1
	Итого	**81**	**40**	**14**	**4**	**23**

4.3. Содержание разделов дисциплины

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Основы информационной безопасности	Введение. Цель и задачи дисциплины. Предмет и объект защиты информации. Предмет и объект защиты информации. Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности. Основные определения и критерии класссификации угроз. Анализ возможных каналов утечки информации.	реферат, собеседование
2	Криптографические методы информационной безопасности	Основные этапы развития криптологии. Основные понятия и определения. Одноключевые (симметричные, с секретным ключом) системы шифрования. Двухключевые (асимметричные, с открытым ключом) системы шифрования. Криптостойкость. Методы криптографического преобразования данных. Кодирование. Асимметричные системы шиф-рования RSA. Схемы и стандарты цифровой подписи. Аппаратное шифрование и программные пакеты для шифрования. Надежность использования криптосистем.	Лабораторная работа, проверочная работа, индивидуальные творческие задания, собеседование
3	Методы и средства защиты информации	Методы парольной защиты. Использование простого пароля. Использование динамически изменяющегося пароля. Методы идентификации и аутентификации пользователей. Идентификация, аутентификация с помощью биометрических данных. Компьютерная стеганография. Туннелирование. Управление. Обеспечение отказоустойчивости и обслуживаемости.	Лабораторная работа, собеседование
4	Аппаратные и программные средства защиты компьютерной информации	Компьютерные вирусы и средства борьбы с ними. Экранирование, анализ защищенности. Комплексная система защиты информации. Основы современных сетевых технологий. Угрозы информационной безопасности при подключении к Интернет. Методы взлома интрасетей. Обзор технических и программных средств обеспечения безопасности компьютерных сетей. Противодействие несанкционированному межсетевому доступу. Защита электронной почты	Лабораторная работа, реферат, собеседование, деловая игра

4.4. Практические занятия

№ ПЗ	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Шифрование с симметричными ключами при помощи аналитических преобразований	2
2	2	Оценка криптостойкости шифров. Элементы криптоанализа	2
3	3	Аутентификация пользователя по биометрическим характеристикам	2
4	3	Парольная защита. Способы атаки на пароль. Обеспечение безопасности пароля	2
5	4	Угрозы информационной безопасности при подключении к Интернет. Методы взлома интрасетей	2
6	4	Защита от несанкционированного доступа в операционной системе Windows	2
7	4	Зачетное занятие. Подведение итогов	2
		Итого:	**14**

4.5. Самостоятельное изучение разделов дисциплины

№ п/п	Вопросы, выносимые на самостоятельное изучение	Кол-во часов
1.	Угрозы информационной безопасности и каналы утечки информации	1
2.	Инженерно-технические средства защиты информации. Программно-аппаратные средства защиты	1
3.	Простейшие шифры с симметричными ключами: замены	1
4.	Простейшие шифры с симметричными ключами: перестановки	1
5.	Простейшие шифры с симметричными ключами: гаммирование	1
6.	Смешанные методы шифрования. Криптографические системы DES и ГОСТ 28147-89	1
7.	Асимметричные шифры. Системы с открытыми ключами	1
8.	Системы с открытыми ключами. Электронно-цифровая подпись	1
9.	Криптографические протоколы: аутентификации, обмена ключами. Специфические протоколы	1
10.	Оценка криптостойкости шифров. Элементы криптоанализа	1
11.	Туннелирование. Управление. Обеспечение отказоустойчивости и обслуживаемости	1
12.	Методы идентификации и аутентификации пользователей на основе паролей	1
13.	Аутентификация пользователя по биометрическим характеристикам	1
14.	Парольная защита. Способы атаки на пароль. Обеспечение безопасности	1
15.	Компьютерная преступность. Разновидности компьютерного пиратства	1

16.	Обзор технических и программных средств обеспечения безопасности	1
17.	Средства защиты сети: межсетевые экраны, виртуальные частные сети,	1
18.	Средства защиты информации от несанкционированного доступа	1
19.	Защита от несанкционированного доступа в операционной системе	1
20.	Защита документов в Microsoft Office. Защита баз данных	1
21.	Организационно-правовое обеспече-ние информационной безопасности	1
22.	Актуальные проблемы уголовно-правовой борьбы с посягательствами	1
23.	Зачетное занятие. Подведение итогов	1
	Итого:	**23**

5. Образовательные технологии

Выбор организационной формы работы, соответствующей типу выполняемого задания, а также эффективное руководство и управление деятельностью студентов, ее регулирование на занятии способствует интенсификации процесса обучения.

В процессе преподавания данной дисциплины используются как классические методы обучения (лекции, традиционные лабораторные работы), так и различные виды самостоятельной работы студентов по заданию преподавателя, которые направлены на развитие творческих качеств студентов и на поощрение их интеллектуальных инициатив.

При изучении дисциплины «Информационная безопасность» применяются следующие образовательные технологии:

- технология программированного обучения;
- игровые технологии;
- творческие технологии;
- технологии мультимедия с применением интерактивных форм обучения.

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Итоговой формой контроля знаний по дисциплине «Информационная безопасность» в шестом семестре является экзамен. Экзамен проводится по билетам, которые включают два теоретических вопроса и разработку ПС по специальному заданию.

6.1. Образец тестового задания

1. Субъект, обладающий полномочиями владения, пользования и распоряжения информационными ресурсами, систем и технологий:

а) владелец;

б) собственник;

в) пользователь;

г) администратор.

2. Поставьте в соответствие характеристикам информации их свойства:

а) качество;	1) неизменность информации в условиях ее случайного
б) конфиденциальность;	и (или) преднамеренного искажения или разрушения;
в) целостность;	2) способность обеспечения беспрепятственного
г) доступность.	доступа субъектов к интересующей их информации;
	3) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации;
	4) известность содержания информации только имеющим соответствующие полномочия субъектам.

3. Укажите уровни мер защиты информации:

а) правовой;
б) рядовой;
в) программно-аппаратный;
г) криптографический;
д) безопасный.

4. Зашифруйте исходное сообщение «Замена» методом Юлия Цезаря, если алфавит пронумерован следующим образом:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**	**Ю**	**Я**

а) ибнжоб;
б) лгпирв;
в) крнагт;
г) мдрксд.

5. Установите правильную последовательность действий при шифровании методом DES:

а) выходной массив шифруется перестановкой с заменой;

б) формируется выходной массив так, что его левая часть L" представлена правой частью R' входного, правая R" формируется как сумма L’ и R’ операцией XOR;

в) входной массив делится пополам на левую L' и правую R' части;

г) на вход подается массив данных.

6.2. Контрольные вопросы для самопроверки

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Понятия "Безопасная система", "Надежная система".
4. Основные определения и критерии классификации угроз безопасности информации.
5. Случайные угрозы безопасности информации.

6. Преднамеренные умышленные угрозы безопасности информации.
7. Неформальная модель нарушителя.
8. Компьютерные преступления.
9. Компьютерное пиратство. Хакеры.
10. Руководящие документы Гостехкомиссии России в области информационной безопасности.
11. Особенности современных информационных систем, существенные с точки зрения безопасности.
12. Законодательный уровень информационной безопасности.
13. Административный уровень информационной безопасности.
14. Процедурный уровень информационной безопасности.
15. Программно-технический уровень информационной безопасности.
16. Сервисы информационной безопасности.
17. Методы парольной защиты.
18. Использование простого пароля для защиты информационных систем.
19. Использование динамически изменяющегося пароля для защиты информационных систем.
20. Идентификация/аутентификация с помощью биометрических данных. Основные понятия.

6.3. Темы рефератов для самостоятельной работы

1. Важность и сложность проблемы информационной безопасности.
2. Обзор российского законодательства в области информационной безопасности.
3. Обзор зарубежного законодательства в области информационной безопасности.
4. Стандарты и спецификации в области информационной безопасности.
5. Административный уровень информационной безопасности.
6. Процедурный уровень информационной безопасности.
7. Особенности современных информационных систем, существенных с точки зрения безопасности.
8. Основные направления обеспечения безопасности информационных систем.
9. Схемы и стандарты цифровой подписи.
10. Аппаратное шифрование и программные пакеты для шифрования.
11. Основные концепции безопасности в операционных системах.
12. Защита данных при передаче по каналам связи.
13. Защита электронной почты.
14. Проблемы безопасности программного обеспечения.
15. Способы разграничения доступа и средства их реализации.
16. Обзор средств защиты информации в компьютерных сетях.
17. Безопасность электронной коммерции.
18. Защита личности как носителя информации.

7. Учебно-методическое обеспечение дисциплины

7.1. Основная литература

1. Мельников, В.П. Информационная безопасность: учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 4-е изд. – М: Академия, 2011. – 336 с.

2. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов /П.Б. Хореев. – М.: Академия, 2010. – 256 с.

3. Парытка, Т.Л. Информационная безопасность: учебное пособие для спо / Т.Л. Парытка. – М.: ФОРУМ: ИНФРА-М, 2010. – 368 с.

7.2. Дополнительная литература

1. Домарев, В.В. Безопасность информационных технологий: Методология создания систем защиты /В.В. Домарев. – М.; СПб; Киев: «ТИД «ДИС»», 2001. – 688 с.

2. Мельников, В.П. Информационная безопасность: учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – М: Академия, 2005. – 336 с.

7.3. Интернет-ресурсы

1. Интернет-Университет Информационных Технологий: сайт. Басалова, Г.В. Основы криптографии: курс лекций [Электронный ресурс] / Басалова Г.В., 2011. – **Режим доступа: http://www.intuit.ru/**

2. Электронно-библиотечная система «КнигаФонд»

7.4. Программное обеспечение современных информационно-коммуникационных технологий

Для изучения данной дисциплины необходим целый комплекс технических средств, использующийся как основной элемент для усвоения практического материала, умения использовать технические средства в работе. Необходимым и обязательным средством является персональный компьютер современной конфигурации при наличии современного программного компьютерного обеспечения – Windows XP, Microsoft Word – версии не ниже 2003 года, Borland Pascal, PascalABC, Borland Delphi 7.0, WinRar.

8. Материально-техническое обеспечение дисциплины

Для изучения дисциплины имеется следующее материально-техническое обеспечение:

- лекционная аудитория;
- библиотечный фонд;
- научный фонд;
- компьютерная аудитория

9. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения дисциплины «Информационная безопасность» осуществляются преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Уметь:	
- применять правовые, организационные, технические и программные средства защиты информации; - создавать программные средства защиты информации.	Практическая работа Ситуационные задачи
Знать:	
- источники возникновения информационных угроз; - модели и принципы защиты информации от несанкционированного доступа; - методы антивирусной защиты информации; - состав и методы организационно-правовой защиты информации.	Тестирование Ситуационные задачи