МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **09.03.01 Информатика и вычислительная техника**
Направленность (профиль) / специализация: **Программное обеспечение средств вычислительной техники и автоматизированных систем**
Форма обучения: **заочная (в том числе с применением дистанционных образовательных технологий)**
Факультет: **ФДО, Факультет дистанционного обучения**
Кафедра: **АСУ, Кафедра автоматизированных систем управления**
Курс: **4**
Семестр: **8**
Учебный план набора 2018 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Самостоятельная работа под руководством преподавателя	10	10	часов
2	Лабораторные работы	16	16	часов
3	Контроль самостоятельной работы	2	2	часов
4	Всего контактной работы	28	28	часов
5	Самостоятельная работа	107	107	часов
6	Всего (без экзамена)	135	135	часов
7	Подготовка и сдача экзамена	9	9	часов
8	Общая трудоемкость	144	144	часов
			4.0	З.Е.

Контрольные работы: 8 семестр - 1
Экзамен: 8 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 28.02.2018
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 46515

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «17» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 09.03.01 Информатика и вычислительная техника, утвержденного 12.01.2016 года, рассмотрена и одобрена на заседании кафедры АСУ «___» _____ 20__ года, протокол №_____.

Разработчик:

профессор каф. АСУ	_____	А. Н. Горитов
Заведующий обеспечивающей каф. АСУ	_____	А. М. Кориков

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФДО	_____	И. П. Черкашина
Заведующий выпускающей каф. АСУ	_____	А. М. Кориков

Эксперты:

Доцент кафедры технологий электронного обучения (ТЭО)	_____	Ю. В. Морозова
Доцент кафедры автоматизированных систем управления (АСУ)	_____	А. И. Исакова

Согласована на портале № 46515

1. Цели и задачи дисциплины

1.1. Цели дисциплины

дать студентам необходимые знания, умения и навыки в области современных информационных технологий, применяемых в настоящее время, а также защиты информации.

1.2. Задачи дисциплины

– овладение теоретическими знаниями в области информационных технологий и обеспечения их безопасности, а также управления информационными ресурсами;

– приобретение прикладных знаний в области создания систем защиты информации, а также оптимизации моделей сложных процессов бизнеса;

– овладение навыками самостоятельного использования соответствующих инструментальных программных систем.

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации» (Б1.Б.15) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Математика, Математическая логика и теория алгоритмов, Программирование.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Практика по получению профессиональных умений и опыта профессиональной деятельности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

В результате изучения дисциплины обучающийся должен:

– **знать** основные понятия и принципы защиты информации; современные подходы к защите продуктов и систем информационных технологий; основные методы обеспечения многоуровневой безопасности в информационных системах.

– **уметь** выявлять угрозы информационной безопасности; использовать средства защиты данных для организации безопасной работы компьютеров.

– **владеть** навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Контактная работа (всего)	28	28
Самостоятельная работа под руководством преподавателя (СРП)	10	10
Лабораторные работы	16	16
Контроль самостоятельной работы (КСР)	2	2
Самостоятельная работа (всего)	107	107
Подготовка к контрольным работам	16	16
Оформление отчетов по лабораторным работам	8	8
Подготовка к лабораторным работам	8	8
Самостоятельное изучение тем (вопросов)	75	75

Согласована на портале № 46515

теоретической части курса		
Всего (без экзамена)	135	135
Подготовка и сдача экзамена	9	9
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	СРП, ч	Лаб. раб., ч	КСР, ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр						
1 Проблемы и методы защиты компьютерной информации.	1	0	2	7	8	ОПК-5
2 Исторические шифры.	1	0		12	13	ОПК-5
3 Основные понятия криптографии.	1	4		16	21	ОПК-5
4 Математические основы криптографических методов.	2	0		12	14	ОПК-5
5 Компьютерные алгоритмы шифрования.	2	4		16	22	ОПК-5
6 Компьютерная безопасность и практическое применение криптографии.	1	4		16	21	ОПК-5
7 Вирусы и угрозы, связанные с вирусами.	1	0		12	13	ОПК-5
8 Брандмауэры.	1	4		16	21	ОПК-5
Итого за семестр	10	16	2	107	135	
Итого	10	16	2	107	135	

5.2. Содержание разделов дисциплины (самостоятельная работа под руководством преподавателя)

Содержание разделов дисциплин (самостоятельная работа под руководством преподавателя) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (самостоятельная работа под руководством преподавателя)

Названия разделов	Содержание разделов дисциплины (самостоятельная работа под руководством преподавателя)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Проблемы и методы защиты компьютерной информации.	Информационная безопасность. Проблемы защиты информации в компьютерных системах. Традиционные вопросы криптографии. Современные приложения криптографии.	1	ОПК-5

Согласована на портале № 46515

	Итого	1	
2 Исторические шифры.	Подстановочные и перестановочные шифры. Статистические свойства языка шифрования. Критерий статистической оценки происхождения шифротекста.	1	ОПК-5
	Итого	1	
3 Основные понятия криптографии.	Криптографическая терминология. Однонаправленные функции. Однонаправленная хэш-функция. Передача информации с использованием криптографии с открытыми ключами. Смешанные криптосистемы.	1	ОПК-5
	Итого	1	
4 Математические основы криптографических методов.	Теория информации. Теория сложности. Теория чисел. Генерация простого числа. Дискретные логарифмы в конечном поле.	2	ОПК-5
	Итого	2	
5 Компьютерные алгоритмы шифрования.	Симметричные шифры. Поточные шифры. Блочные шифры. Шифр Фейстеля. Шифр DES. Режимы работы DES. Шифр Rijndael. Алгоритм ГОСТ 28147-89. Алгоритм IDEA. Однонаправленная хэш-функция MD5. Алгоритм шифрования данных RSA.	2	ОПК-5
	Итого	2	
6 Компьютерная безопасность и практическое применение криптографии.	Обзор стандартов в области защиты информации. Подсистема информационной безопасности. Методы и средства обеспечения информационной безопасности локальных рабочих станций.	1	ОПК-5
	Итого	1	
7 Вирусы и угрозы, связанные с вирусами.	Вредоносные программы. Типы вирусов. Природа вирусов. Структура вируса. Макровирусы. Антивирусная защита. Перспективные методы антивирусной защиты.	1	ОПК-5
	Итого	1	
8 Брандмауэры.	Принципы разработки брандмауэров. Характеристики брандмауэров. Типы брандмауэров. Конфигурации брандмауэров.	1	ОПК-5
	Итого	1	
Итого за семестр		10	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Согласована на портале № 46515

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин							
	1	2	3	4	5	6	7	8
Предшествующие дисциплины								
1 Математика	+	+	+	+	+	+		
2 Математическая логика и теория алгоритмов	+	+	+	+	+	+	+	+
3 Программирование	+	+	+		+	+	+	+
Последующие дисциплины								
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+		+	+	+	+	+	+
2 Практика по получению профессиональных умений и опыта профессиональной деятельности			+	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий				Формы контроля
	СРП	Лаб. раб.	КСР	Сам. раб.	
ОПК-5	+	+	+	+	Контрольная работа, Экзамен, Проверка контрольных работ, Отчет по лабораторной работе, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
3 Основные понятия криптографии.	Администрирование учетных записей пользователей.	4	ОПК-5
	Итого	4	
5 Компьютерные алгоритмы шифрования.	Управление параметрами операционной системы.	4	ОПК-5
	Итого	4	
6 Компьютерная безопасность и	Дискреционный механизм разграничения доступа.	4	ОПК-5

Согласована на портале № 46515

практическое применение криптографии.	Итого	4	
8 Брандмауэры.	Политика ограниченного использования программ.	4	ОПК-5
	Итого	4	
Итого за семестр		16	

8. Контроль самостоятельной работы

Виды контроля самостоятельной работы приведены в таблице 8.1.

Таблица 8.1 – Виды контроля самостоятельной работы

№	Вид контроля самостоятельной работы	Трудоемкость (час.)	Формируемые компетенции
8 семестр			
1	Контрольная работа с автоматизированной проверкой	2	ОПК-5
Итого		2	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Проблемы и методы защиты компьютерной информации.	Самостоятельное изучение тем (вопросов) теоретической части курса	5	ОПК-5	Контрольная работа, Тест, Экзамен
	Подготовка к контрольным работам	2		
	Итого	7		
2 Исторические шифры.	Самостоятельное изучение тем (вопросов) теоретической части курса	10	ОПК-5	Контрольная работа, Тест, Экзамен
	Подготовка к контрольным работам	2		
	Итого	12		
3 Основные понятия криптографии.	Самостоятельное изучение тем (вопросов) теоретической части курса	10	ОПК-5	Контрольная работа, Отчет по лабораторной работе, Тест, Экзамен
	Подготовка к лабораторным работам	2		
	Оформление отчетов по лабораторным работам	2		
	Подготовка к контрольным работам	2		
	Итого	16		

Согласована на портале № 46515

4 Математические основы криптографических методов.	Самостоятельное изучение тем (вопросов) теоретической части курса	10	ОПК-5	Контрольная работа, Тест, Экзамен
	Подготовка к контрольным работам	2		
	Итого	12		
5 Компьютерные алгоритмы шифрования.	Самостоятельное изучение тем (вопросов) теоретической части курса	10	ОПК-5	Контрольная работа, Отчет по лабораторной работе, Тест, Экзамен
	Подготовка к лабораторным работам	2		
	Оформление отчетов по лабораторным работам	2		
	Подготовка к контрольным работам	2		
	Итого	16		
6 Компьютерная безопасность и практическое применение криптографии.	Самостоятельное изучение тем (вопросов) теоретической части курса	10	ОПК-5	Контрольная работа, Отчет по лабораторной работе, Тест, Экзамен
	Подготовка к лабораторным работам	2		
	Оформление отчетов по лабораторным работам	2		
	Подготовка к контрольным работам	2		
	Итого	16		
7 Вирусы и угрозы, связанные с вирусами.	Самостоятельное изучение тем (вопросов) теоретической части курса	10	ОПК-5	Контрольная работа, Тест, Экзамен
	Подготовка к контрольным работам	2		
	Итого	12		
8 Брандмауэры.	Самостоятельное изучение тем (вопросов) теоретической части курса	10	ОПК-5	Контрольная работа, Отчет по лабораторной работе, Тест, Экзамен
	Подготовка к лабораторным работам	2		
	Оформление отчетов по лабораторным работам	2		
	Подготовка к контрольным работам	2		
	Итого	16		
	Выполнение контрольной работы	2	ОПК-5	Контрольная работа
Итого за семестр		107		

Согласована на портале № 46515

	Подготовка и сдача экзамена	9		Экзамен
Итого		116		

10. Контроль самостоятельной работы (курсовой проект / курсовая работа)

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Спицин В.Г. Информационная безопасность вычислительной техники [Электронный ресурс] [Электронный ресурс]: учебное пособие /В.Г. Спицин. - Томск: Эль Контент, 2011. - 148 с. Доступ из личного кабинета студента. — Режим доступа: https://study.tusur.ru/study/library/ (дата обращения: 18.09.2018).

12.2. Дополнительная литература

1. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 616 с. — Доступ из личного кабинета студента. — Режим доступа: https://e.lanbook.com/book/5154 (дата обращения: 18.09.2018).
2. Шаньгин, В.Ф. Защита компьютерной информации [Электронный ресурс] [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2010. — 544 с. — Доступ из личного кабинета студента. — Режим доступа: https://e.lanbook.com/book/1122 (дата обращения: 18.09.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Спицин В.Г. Информационная безопасность вычислительной техники : Электронный курс /В.Г. Спицин. - Томск: ТУСУР ФДО, 2018. Доступ из личного кабинета студента.
2. Горитов А. Н. Защита информации [Электронный ресурс] [Электронный ресурс]: методические указания по организации самостоятельной работы для студентов заочной формы обучения технических направлений, обучающихся с применением дистанционных образовательных технологий / А. Н. Горитов, А. М. Кориков. – Томск : ФДО, ТУСУР, 2018. Доступ из личного кабинета студента. — Режим доступа: https://study.tusur.ru/study/library/ (дата обращения: 18.09.2018).
3. Якимук А. Ю. Защита информации [Электронный ресурс]: методические указания по выполнению лабораторной работы для студентов заочной формы обучения с применением дистанционных образовательных технологий / А. Ю. Якимук. – Томск : ФДО, ТУСУР, 2017. Доступ из личного кабинета студента. — Режим доступа: https://study.tusur.ru/study/library/ (дата обращения: 18.09.2018).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;

Согласована на портале № 46515

– в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. American Mathematical Society: www.ams.org
2. Copyright for Librarians: cyber.law.harvard.edu
3. eLIBRARY.RU: www.elibrary.ru
4. IEEE Xplore: www.ieeexplore.ieee.org
5. Nature: www.nature.com

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение дисциплины

Кабинет для самостоятельной работы студентов

учебная аудитория для проведения занятий лабораторного типа, помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации, помещение для самостоятельной работы

634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- Коммутатор MicroTeak;
- Компьютер PENTIUM D 945 (3 шт.);
- Компьютер GELERON D 331 (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– 7-zip (с возможностью удаленного доступа)
– FAR Manager (с возможностью удаленного доступа)
– Free Pascal (с возможностью удаленного доступа)
– Google Chrome
– Kaspersky Endpoint Security 10 для Windows (с возможностью удаленного доступа)
– MS Office версий 2010 (с возможностью удаленного доступа)
– Microsoft Windows
– OpenOffice (с возможностью удаленного доступа)
– PascalABC (с возможностью удаленного доступа)
– Visual Studio 2015 (с возможностью удаленного доступа)

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

Кабинет для самостоятельной работы студентов

учебная аудитория для проведения занятий лабораторного типа, помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации, помещение для самостоятельной работы

634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- Коммутатор MicroTeak;
- Компьютер PENTIUM D 945 (3 шт.);
- Компьютер GELERON D 331 (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– 7-zip (с возможностью удаленного доступа)
– DEV C++ (с возможностью удаленного доступа)
– FAR Manager (с возможностью удаленного доступа)

Согласована на портале № 46515

– Free Pascal (с возможностью удаленного доступа)
– Google Chrome
– Kaspersky Endpoint Security 10 для Windows (с возможностью удаленного доступа)
– MS Office версий 2010 (с возможностью удаленного доступа)
– Microsoft Windows
– OpenOffice (с возможностью удаленного доступа)
– PascalABC (с возможностью удаленного доступа)
– Visual Studio 2015 (с возможностью удаленного доступа)

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

Согласована на портале № 46515

14.1.1. Тестовые задания

1) Количество знаков в шифротексте и в исходном тексте в общем случае:
1. не может различаться.
2. может различаться.
3. должно быть равно сумме знаков открытого текста и ключа.
4. должно быть равно разности знаков открытого текста и ключа.
5. должно быть равно длине алфавита.

2) Стойкость современных криптосистем основывается на:
1. секретности долговременных элементов криптозащиты.
2. применении стеганографических алгоритмов.
3. секретности алгоритма шифрования.
4. секретности информации сравнительно малого размера, называемой ключом.
5. секретности алгоритма шифрования и ключа.

3) Подстановочным шифром называется шифр, в котором:
1. используется матрица чисел размерностью 5x5.
2. используется открытый ключ.
3. используется фрагмент текста.
4. используется фрагмент текста и открытый ключ.
5. каждый символ открытого текста в шифротексте заменяется другим символом.

4) В однозвучном подстановочном шифре:
1. один символ открытого текста отображается на несколько символов шифротекста.
2. два символа открытого текста отображаются на один символ шифротекста.
3. три символа открытого текста отображаются на один символ шифротекста.
4. четыре символа открытого текста отображаются на один символ шифротекста.
5. пять символов открытого текста отображаются на один символ шифротекста.

5)Открытый текст M (message) для компьютера – это
1. двоичные данные.
2. набор символов.
3. текстовый файл.
4. оцифрованный звук.
5. цифровое видеоизображение.

6) Энтропия сообщения в теории информации определяет:
1. число символов в сообщении.
2. норму языка.
3. количество возможных значений сообщения.
4. размер ключа.
5. вероятность появления тех или иных символов.

7) Работа симметричных шифров включает в себя два преобразования:
C = Ek(m) и m = Dk(C), где m – открытый текст, E – шифрующая функция, D – расшифровывающая функция, C – шифротекст, k–
1. пространство ключей.
2. секретный ключ.
3. число символов в алфавите.
4. порядковый номер шифрующей и дешифрующей функций.
5. длина открытого текста.

8) Для обеспечения безопасной передачи данных по сети на физическом и канальном уровнях применяются следующие подходы:

Согласована на портале № 46515

1. аутентификация рабочей станции, являющейся источником сообщений.
2. административная защита на маршрутизаторах.
3. шифрование соединения.
4. выборочное или полное шифрование трафика.
5. фильтрация трафика между внутренней сетью и внешней коммуникационной средой.
6. защита при помощи межсетевых экранов.

9) К вредоносным программам, требующим программу-носитель, относятся:
1. бактерии.
2. логические бомбы.
3. «троянские кони».
4. черви.
5. вирусы.

10) Брандмауэры могут быть:
1. эффективным средством защиты только локальной рабочей станции, но не компьютерной сети, от угроз, имеющих сетевую природу, в то же время не ограничивающим связь с внешним миром через глобальные сети и Internet.
2. неэффективным средством защиты локальной системы или компьютерной сети от угроз, имеющих сетевую природу, в то же время не ограничивающим связь с внешним миром через глобальные сети и Internet.
3. эффективным средством защиты локальной системы или компьютерной сети от угроз, имеющих сетевую природу, в то же время ограничивающим связь с внешним миром через глобальные сети и Internet.
4. эффективным средством защиты локальной системы или компьютерной сети от угроз, не имеющих сетевую природу, в то же время не ограничивающим связь с внешним миром через глобальные сети и Internet.
5. эффективным средством защиты локальной системы или компьютерной сети от угроз, имеющих сетевую природу, в то же время не ограничивающим связь с внешним миром через глобальные сети и Internet.

14.1.2. Экзаменационные тесты

1) Все элементы систем защиты подразделяются на две категории – долговременные и легкозаменяемые. К долговременным элементам относятся:
1. секретный ключ.
2. алгоритм шифрования.
3. открытый ключ.
4. пароль.
5. идентификатор данных.

2) Шифротекст и исходный текст могут иметь в общем случае:
1. одинаковое количество знаков.
2. знаки ключа шифрования.
3. одинаковое количество знаков и повторяющиеся знаки.
4. разное количество знаков и повторяющиеся знаки.
5. ни одного повторяющегося знака.

3) Основным условием стойкости современных криптосистем является секретность:
1. всех долговременных элементов криптозащиты.
2. всех легкозаменяемых элементов криптозащиты.
3. алгоритма шифрования.
4. информации сравнительно малого размера, называемой ключом.
5. алгоритма шифрования и ключа.

4) Перестановочный шифр в отличие от подстановочного:

Согласована на портале № 46515

1. является более стойким.
2. использует открытый ключ.
3. имеет больший период.
4. использует множественные ключи.
5. меняет не открытый текст, а порядок символов.

5) Подстановочный шифр, в котором один символ открытого текста отображается на несколько символов шифротекста, называется:
1. однозвучным.
2. моноалфавитным.
3. полиграмным.
4. полиалфавитным.
5. книжным.

6) Подстановочный шифр, который блоки символов шифрует по группам, называется:
1. однозвучным.
2. моноалфавитным.
3. полиграмным.
4. полиалфавитным.
5. книжным.

7) Функция шифрования E(M) = C открытого текста M в шифротекст C создает на выходе для компьютера:
1. закодированный набор символов.
2. текстовый файл того же размера, что и M.
3. текстовый файл большего размера, чем M.
4. текстовый файл меньшего размера, чем M.
5. двоичные данные.

8) Идентичность понятий “криптографический алгоритм” и “шифр” позволяют определить криптосистему, как совокупность:
1. математических функций, используемых для шифрования и дешифрования.
2. шифра, открытого текста и шифротекста.
3. шифра и пространства ключей.
4. математических функций, используемых для шифрования и дешифрования, пространства ключей и открытого текста.
5. шифра, всевозможных открытых текстов, шифротекстов и ключей.

9) В большинстве симметричных алгоритмов ключ шифрования:
1. совпадает с ключом дешифрования.
2. не может быть рассчитан по ключу дешифрования.
3. применяется в совокупности с несколькими ключами.
4. является открытым.
5. чаще всего хранится в некоторой базе данных.

10) В общем случае энтропия сообщения – это:
1. число символов в сообщении.
2. количество символов, необходимых для кодирования сообщения.
3. минимальное количество бит, необходимых для кодирования всех возможных значений сообщения.
4. длина сообщения в битах.
5. вероятность появления тех или иных символов.

11) Соотношение H (M)=log2 n, где n – количество возможных значений, определяет:

Согласована на портале № 46515

1. меру избыточности сообщения.
2. информативность сообщения.
3. максимум энтропии отдельного символа
4. энтропию криптосистемы.
5. энтропию сообщения.

12) Абсолютная норма языка является функцией:
1. нормы языка.
2. числа символов в алфавите.
3. избыточности языка.
4. длины сообщения.
5. энтропии криптосистемы.

13) Криптостойкость симметричных шифров зависит только от секретности используемого ключа. Ключ, исключающий взлом простым перебором, содержит не менее чем:
1. 64 бита.
2. 80 бит.
3. 48 бит.
4. 32 бита.
5. 16 бит.

14) Для простейшего поточного шифра, использующего в качестве функций шифрования и дешифрования операцию исключающего ИЛИ, при значении открытого текста = 1110101110, потоке ключей = 1010010001, шифротекст =

1. 1110011001.
2. 0100111111.
3. 0111001110.
4. 0101010001.
5. 1010101111.

15) Подходы, которые применяются для обеспечения безопасной передачи данных по сети на двух нижних уровнях модели сетевого взаимодействия:
1. административная защита на маршрутизаторах.
2. фильтрация трафика между внутренней сетью и внешней коммуникационной средой.
3. защита при помощи межсетевых экранов.
4. шифрование соединения.
5. выборочное или полное шифрование трафика.

16) Какие угрозы можно выделить на двух нижних уровнях модели сетевого взаимодействия?
1. физическое уничтожение канала связи.
2. ошибочная коммутация.
3. атаки на систему маршрутизации.
4. разведка имен и паролей пользователей.
5. атаки на систему разграничения прав доступа пользователей.

17) Вредосносные программы, требующие наличия программы-носителя:
1. бактерии.
2. логические бомбы.
3. троянские кони.
4. черви.
5. вирусы.

Согласована на портале № 46515

18) Укажите высказывания, которые верны по отношению к лазейкам:

1. лазейки относятся к вредоносным программам, не требующим программы-носителя.

2. лазейка — это секретная точка входа в программу, позволяющая

тому, кто знает о ее существовании, получить доступ в обход стандартных процедур защиты.

3. контроль возможных лазеек легко реализуется стандартными средствами операционной системы.

4. лазейки незаконно используются в программистской практике для ускорения отладки и тестирования программ.

5. меры защиты от лазеек должны быть сфокусированы на контроле процесса разработки программного обеспечения и его обновления.

19) Брандмауэр:

1. может защитить от внутренних угроз безопасности.

2. не может защитить от внутренних угроз безопасности, например со стороны сотрудника, вступившего в сговор с внешним нарушителем.

3. не может фильтровать электронную почту, отсеивая «спам».

4. может разрешить доступ извне только к определенной части информации, находящейся на локальном Web-сервере.

5. не может защитить от угрозы передачи инфицированных вирусами программ или файлов.

20) Укажите верные утверждения о фильтрующих маршрутизаторах:

1. Фильтрующий маршрутизатор принимает решение о том, передавать по сети поступивший пакет IP дальше или отвергнуть его, на основе определенного набора правил.

2. Правила фильтрования основываются на значениях полей заголовка IP, заголовка транспортного уровня, а также номера порта, определяющего приложение.

3. Фильтрующий маршрутизатор работает как ретранслятор данных уровня приложений.

4. Вне зависимости от настроек фильтрующего маршрутизатора, используемая по умолчанию политика – “Все, что не разрешено, запрещено”.

5. Вне зависимости от настроек фильтрующего маршрутизатора, используемая по умолчанию политика – “Все, что не запрещено, разрешено”.

14.1.3. Темы контрольных работ

защита информации

1) Целостность:

1. свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.

2. способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.

3. свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.

4. способность совершать некоторые действия в информационной системе незаметно для других объектов.

5. свойство информации быть доступной ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.

2) Достоверность:

1. свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.

2. способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.

3. свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.

4. способность совершать некоторые действия в информационной системе незаметно для

Согласована на портале № 46515

других объектов.

5. свойство информации быть доступной ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.

3) Полиграмный подстановочный шифр:

1. один символ открытого текста отображается на один символ шифротекста.
2. один символ открытого текста отображает на несколько символов шифротекста.
3. блоки символов шифрует по группам.
4. применяет псевдослучайный ключ.
5. применяет открытый ключ.

4) В полиалфавитном подстановочном шифре:

1. применяется псевдослучайный ключ.
2. применяется имитовставка.
3. применяется открытый ключ.
4. длина ключа равна длине сообщения.
5. применяются несколько простых подстановочных шифров.

5) Безопасность симметричного алгоритма определяется:

1. ключом.
2. функцией шифрования.
3. функцией дешифрования.
4. применением двух ключей.
5. применением разных ключей для шифрования и дешифрования.

6) Расстояние уникальности измеряет:

1. количество криптотекста нужного для криптоанализа.
2. минимальное количество криптотекста, необходимое для единственности результата криптоанализа.
3. сумму энтропии киптосистемы и энтропии ключа шифрования.
4. избыточность криптосиситемы.
5. точную длину шифротекста.

7) Основные отличия блочного шифра от поточного:

1. за один прием обрабатывается блок открытого текста.
2. при шифровании необходимо постоянно помнить, какое место в строке в данный момент обрабатывается.
3. более общий – легко трансформируется в поточный.
4. использует более математизированную структуру.
5. более быстрый, чем поточный.

8) Защиту информации на физическом и канальном уровне обеспечивают такие устройства как:

1. шифрующие модемы.
2. специализированные канальные адаптеры.
3. криптосерверы.
4. шифрующие маршрутизаторы.
5. proxy-серверы.

9) Какие могут быть заданы действия или события, по наступлению которых активизируется лазейка:

1. введение с клавиатуры специальной последовательности.
2. введение определенного идентификатора пользователя.
3. наступление определенного дня недели.

Согласована на портале № 46515

4. последовательность каких-то маловероятных событий.

5. наступление определенной даты.

10) Брандмауэр представляет собой:

1. единственную точку входа, в которой предотвращается санкционированный доступ внешних пользователей к защищаемой сети, запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.

2. одну из точек входа, в которой предотвращается несанкционированный доступ внешних пользователей к защищаемой сети, запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.

3. единственную точку входа, в которой возможен несанкционированный доступ внешних пользователей к защищаемой сети, запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.

4. единственную точку входа, в которой предотвращается несанкционированный доступ внешних пользователей к защищаемой сети, однако не запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.

5. единственную точку входа, в которой предотвращается несанкционированный доступ внешних пользователей к защищаемой сети, запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.

14.1.4. Темы лабораторных работ

Администрирование учетных записей пользователей.

Управление параметрами операционной системы.

Дискреционный механизм разграничения доступа.

Политика ограниченного использования программ.

14.1.5. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

- чтение или просмотр материала необходимо осуществлять медленно, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

- если в тексте встречаются термины, следует выяснить их значение для понимания дальнейшего материала;

- необходимо осмысливать прочитанное и изученное, отвечать на предложенные вопросы.

Студенты могут получать индивидуальные консультации с использованием средств теле-

Согласована на портале № 46515

коммуникации.

По дисциплине могут проводиться дополнительные занятия в форме вебинаров. Расписание вебинаров публикуется в кабинете студента на сайте Университета. Запись вебинара публикуется в электронном курсе по дисциплине.

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

Согласована на портале № 46515

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 46515