МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВПО «ВГТУ», ВГТУ)

«УТВЕРЖДАЮ»
Председатель Ученого совета
Факультета информационных
технологий и компьютерной безопасности
проф. Пасмурнов С.М. _____
(подпись)
23 09 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации

(наименование дисциплины (модуля) по УП)

Закреплена за кафедрой: компьютерных интеллектуальных технологий проектирования

Направление подготовки (специальности):

09.03.02 Информатика и вычислительная техника

(код, наименование)

Профиль: Системы автоматизированного проектирования в машиностроении

(название профиля по УП)

Часов по УП: 144; **Часов по РПД:** 144;

Часов по УП (без учета часов на экзамены): 144; **Часов по РПД:** 144;

Часов на интерактивные формы (ИФ) обучения по УП: 32

Часов на интерактивные формы (ИФ) обучения по РПД: 32

Часов на самостоятельную работу по УП: 72(50%);

Часов на самостоятельную работу по РПД: 72 (50%)

Общая трудоемкость в ЗЕТ: 4;

Виды контроля в семестрах (на курсах): Экзамены - 4; Зачеты - 0; Курсовые проекты - 0; Курсовые работы - 0.

Форма обучения: очная;

Срок обучения: нормативный.

Распределение часов дисциплины по семестрам

Вид занятий	№ семестров, число учебных недель в семестрах																	
			2 / 18		3 / 18		4 / 18		5 / 18		6 / 18		7 / 18		8 / 12		Итого	
		РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции											36	36					36	36
Лабораторные											36	36					36	36
Практические											0	0					0	0
Ауд. занятия											72	22					72	72
Сам. работа											72	72					72	72
Итого											144	144					144	14

Сведения о ФГОС, в соответствии с которым разработана рабочая программа дисциплины (модуля) – 09.03.01 «Информатика и вычислительная техника», утвержден приказом Министерства образования и науки Российской Федерации от 12 марта 2015 № 219

Программу составил: _____ к.т.н., Паринов М.В.
(подпись, ученая степень, ФИО)

Рецензент (ы): _____ Тюгаев Н.А.

Рабочая программа дисциплины составлена на основании учебного плана подготовки специалистов по направлению 09.03.01 Информатика и вычислительная техника, профиль Системы автоматизированного проектирования в машиностроении

Рабочая программа обсуждена на заседании кафедры компьютерных интеллектуальных технологий проектирования

протокол № 1 от 30.05 2017 г.

Зав. кафедрой КИТП _____ д.т.н., проф. М.И. Чижов

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями изучения дисциплины являются:

- понимание моделей и стандартов информационной безопасности;
- усвоение методов защиты информационных систем;
- приобретение теоретических знаний и практических навыков по использованию современных программных средств для обеспечения информационной безопасности и защиты информации от несанкционированного использования.
- формирование у студентов мотивации к самообразованию за счет активизации самостоятельной познавательной деятельности.

Задачами для достижения поставленных целей являются:

- изучение и классификация причин нарушений безопасности;
- проектирование мониторов безопасности субъектов и объектов;
- приобретение практических навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации.

Поставленные цели полностью соответствуют целям ООП. Решение поставленных задач достигается в процессе изучения лекционного материала, самостоятельного изучения отдельных разделов дисциплины и выполнения цикла лабораторных работ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина «Защита информации» является базовой профессионального цикла. Для её успешного усвоения необходимы **знания** базовых понятий информатики и вычислительной техники, роли и значения информатики в современном обществе, форм представления и преобразования информации в компьютере; **умения** программировать для решения практических задач, оперировать программными компонентами операционных систем. **Владеть** навыками работы с интегрированными средами программирования.

Пререквизитами данной дисциплины являются следующие дисциплины: «Дискретная математика», «Информатика», «Сети и телекоммуникации» .

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен:

Знать:

- классификацию причин нарушений безопасности;
- Проектирование мониторов безопасности субъектов и объектов;
- Приобретение практических навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации;
- современное состояние и тенденции развития методов информационной безопасности;

уметь:

- выбирать и тестировать программные средства зашиты информации;
- проводить анализ всего многообразия средств защиты ЭВМ с целью выбора наиболее приемлемого варианта для конкретного использования;
- проводить сравнительный анализ параметров систем защиты информации;
- использовать информационные сервисы глобальных телекммуникаций для работы с Web-серверами ведущих фирм производителей систем компьютерной безопасности;
- использовать образовательные ресурсы по дисциплине, представленные в среде WebCT;

владеть практическими навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации;

В процессе освоения дисциплины у студентов развиваются следующие **компетенции:**

1. Универсальные (общекультурные):

- владение основными методами, способами и средствами получения, хранения, переработки информации (ОК-11);
- владение навыками работы с компьютером как средством управления информацией (ОК-12);
- способность работать с информацией в глобальных компьютерных сетях (ОК-13).

2. Профессиональные:

- способность разрабатывать технические задания на оснащение отделов, лабораторий, офисов компьютерным оборудованием (ПК-1);
- инсталлировать программное обеспечение и подключать аппаратные средства информационных и автоматизированных систем (ПК-11).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Лекционные занятия

4.1.1. Концептуальная модель информационной безопасности.

4.1.2. Обзор и сравнительный анализ стандартов информационной безопасности.

4.1.3 Исследование причин нарушений безопасности

4.1.4. Понятие политики безопасности. Реализация и гарантирование политики безопасности.

4.1.5. Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов.

4.1.6. Архитектура защищенных операционных систем.

4.1.7. Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе.

4.1.8. Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей

4.1.9. Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись.

4.2 Лабораторные работы

4.2.1. Исследование и изучение структуры средств безопасности операционных систем и использование их для конфиденциального доступа к информации.

4.2.2. Разработка и реализация алгоритма функционирования системы безопасности объектов.

4.2.3 Разработка и реализация алгоритма функционирования системы безопасности субъектов.

4.2.4. Разработка и реализация алгоритма сетевого фильтра.

4.2.5. Разработка и реализация алгоритма криптографического преобразования.

4.3 Структура дисциплины по разделам и формам организации обучения

Название раздела/темы	Аудиторная работа (час)			СРС (час)	Колл, Контр.Р.	Итого
	Лекции	Практ./сем. занятия	Лаб. зан.			
1. Концептуальная модель информационной безопасности	4		4	8	Отчет	16
2. Обзор и сравнительный анализ стандартов информационной безопасности	4		4	8	Отчет	16
3. Исследование причин нарушений безопасности	4		4	8	Отчет	16
4. Понятие политики безопасности. Реализация и гарантирование политики безопасности	4		4	8	Отчет	16
5. Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов	4		4	8	Отчет	16
6. Архитектура защищенных операционных систем	4		4	8	Отчет	16
7. Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе	4		4	8	Отчет	16
8. Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей	4		4	8	Отчет	16
9. Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись.	4		4	8	Отчет	16
Итого	36		36	72		144

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

5.1 Методы и формы организации обучения (ФОО)

Образовательные технологии, используемые в дисциплине:

ФОО / Методы	Лекц.	Лаб. раб.	Пр. зан./ Сем.,	Тр*., Мк**	СРС	К. пр.
IT-методы		+			+	
Работа в команде			+			
Case-study		+			+	
Игра						
Методы проблемного обучения.	+					
Обучение на основе опыта		+				
Опережающая самостоятельная работа					+	
Проектный метод						
Поисковый метод					+	
Исследовательский метод		+				
Другие методы						

* – Тренинг, ** – Мастер-класс

6. ОРГАНИЗАЦИЯ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6.1 Самостоятельную работу студентов (СРС) можно разделить на текущую и творческую

Текущая СРС – работа с лекционным материалом, подготовка к лабораторным работам, практическим занятиям с использованием сетевого образовательного ресурса (Web CT); опережающая самостоятельная работа; выполнение домашних заданий; изучение тем, вынесенных на самостоятельную проработку; подготовка к экзамену.

Творческая проблемно-ориентированная самостоятельная работа (ТСР) – поиск, анализ, структурирование и презентация информации по теме лабораторных работ.

6.2 Контроль самостоятельной работы

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль в обучающей программе, контроль знаний, полученных с помощью обучающей программы (контролирующие тесты).

Текущий контроль в виде защит лабораторных работ.

По результатам текущего контроля формируется допуск студента к экзамену. Экзамен проводится в письменной форме и оценивается преподавателем.

6.3 Учебно-методическое обеспечение самостоятельной работы студентов

Для самостоятельной работы студентов используются сетевые образовательные ресурсы, представленные в среде Web CT, сеть Internet для работы с Web-серверами ведущих компьютерных фирм – производителей систем защиты информации.

7. СРЕДСТВА (ФОС) ТЕКУЩЕЙ И ИТОГОВОЙ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ МОДУЛЯ

Для организации текущего контроля полученных студентами знаний по данной дисциплине используются тесты. Образец контролирующего теста приведен ниже (ПРИЛОЖЕНИЕ 1). Экзаменационный билет содержит 2 вопроса и задание на практическое выполнение.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1.Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачева С.В., 2001, 352 с

2.Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем М.: Горячая линия-Телеком, 2000, 452 с.

3.Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2000, 320 с.

4.Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001, 376 с.

5.Пятибратов А.П., Гудыко Л.П., Кириченко А.А. Вычислительные системы и телекоммуникации: Учебник. – 2-ое изд. / Под ред. А.П. Пятибратова.– М.: Финансы и статистика, 2002.

6. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009. – 352 с.

7. Петренко С. А., Курбатов В. А. Политики информационной безопасности. – М.: Компания АйТи, 2006. – 400 с.

Галатенко В. А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий, 2006. – 264 с.

8. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

9. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. – 544 с.

10. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. – 176 с.

11. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000. – 428 с.

Дополнительная литература:

1.Ярочкин В.И. Информационная безопасность. М.: Международные отношения, 2000, 400 с.

Программное обеспечение и Internet-ресурсы:

CIT Forum. URL: http://www.citforum.ru (дата обращения 12.06.2011).

Журнал «Защита информации. Инсайд». URL: https://www.inside-zi.ru/ (дата обращения 12.06.2011).

InformationSecurity: Информационная безопасность. URL: http://www.itsec.ru/main.php (дата обращения 12.06.2011).
Информационная безопасность. URL: https://securityvulns.ru/ (дата обращения 12.06.2011).

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Компьютерный класс. 12 и более компьютеров, проектор, экран 9или интерактивная доска)

ПРИЛОЖЕНИЕ 1

Томский политехнический университет
Кафедра информатики и проектирования систем
Направление 230100 – Информатика и вычислительная техника;
Дисциплина – «Защита информации»

Т Е С Т № 1

Фамилия студента_____
Группа _____ ____

1. Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:

❖ **со стороны злоумышленника**
❖ со стороны законного отправителя сообщения
❖ со стороны законного получателя сообщения

2. Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?

❖ асимметричный
❖ **симметричный**
❖ правильного ответа нет

3. Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется:

❖ шифрование
❖ дешифровка
❖ расшифровка

4. В каких основных форматах существует симметричный алгоритм?

❖ блока и строки;
❖ **потока и блока;**
❖ потока и данных

5. Открытым текстом в криптографии называют:

❖ расшифрованный текст
❖ любое послание
❖ **исходное послание**

6. Какой ключ известен только приемнику?

- открытый
- **закрытый**

7. Наука, занимающаяся защитой информации, путем преобразования этой информации это:

- криптография
- **криптология**
- криптоанализ

8. В каких шифрах результат шифрования очередного блока зависит только от него самого и не зависит от других блоков шифруемого массива данных?

- в потоковых
- **в блочных**

9. Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:

- шифр функциональных преобразований
- шифр замен
- **шифр перестановок**

10. Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется:

- **функция шифрования шага преобразования**
- инвариант стандартного шага шифрования

11. Шифрование-это:

- процесс создания алгоритмов шифрования
- процесс сжатия информации
- **процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется**

12. В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией?

- **при шифровании с помощью ассимметричного алгоритма**
- при шифровании с помощью симметричного алгоритма
- арбитр необходим всегда

13. Можно ли отнести слабую аутентификацию к проблемам безопасности?

- нет
- **да**
- в редких случаях

14. Возможно ли расшифровывать информацию без знания ключа?

- нет
- **да**
- в редких случаях

15. Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый?

- **нет**
- да
- в редких случаях

16. Характерная черта алгоритма Эль-Гамаля состоит в :

- **протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя**
- в точной своевременной передаче сообщения
- алгоритм не имеет особенностей и идентичен RSA

17. Аутентификацией называют:

- процесс регистрации в системе
- способ защиты системы
- **процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов**

18. Аутентификация бывает:

❖статическая

❖устойчивая

❖постоянная

❖**все варианты правильные**

❖правильного варианта нет

19. Стойкость ключа характеризуется

❖длинной

❖непредсказуемостью

❖ **все варианты правильные**

❖правильного варианта нет

20. Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:

❖**на основе произвольно выбранного шифротекста**

❖на основе произвольно выбранного открытого текста

❖на основе только шифротекста

21. Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им *массива открытых данных* размера n используется в анализе:

❖на основе произвольно выбранного шифротекста

❖**на основе произвольно выбранного открытого текста**

❖правильного ответа нет

ПРИЛОЖЕНИЕ 2

Рейтинг-план освоения дисциплины «Защита информации»

Недели	Текущий контроль										
	Теоретический материал				Практическая деятельность						
	Название раздела	Темы лекций	Контролир. материал	Баллы	Название лаб. работ	Баллы	Темы практ. занятий.	Баллы	Индивид. задание	Баллы	Итого
1	Концептуальная модель информационной безопасности.	Концептуальная модель информационной безопасности.			Исследование и изучение структуры средств безопасности операционных систем и использование их для конфиденциального доступа к информации.	9			Поиск информации по теме лабораторной работы	1	10
2	Обзор и сравнительный анализ стандартов информационной безопасности	Обзор и сравнительный анализ стандартов информационной безопасности									
3	Исследование причин нарушений безопасности	Исследование причин нарушений безопасности (часть 1)	Тест 1.	1	Разработка и реализация алгоритма функционирования системы безопасности объектов.	8			Поиск информации по теме лабораторной работы	1	10
4		Исследование причин нарушений безопасности (часть 2)									
Всего по контрольной точке (аттестации) № 1											**20**
5	Понятие политики безопасности. Реализация и гарантирование политики безопасности.	Понятие политики безопасности. Реализация и гарантирование политики безопасности.	Тест 2.	1	Разработка и реализация алгоритма функционирования системы безопасности объектов.	7			Поиск информации по теме лабораторной работы	2	10
6	Модели безопасного субъектного взаимодействия в компьютерной	Модели безопасного субъектного взаимодействия в компьютерной									

	системе. Аутентификация пользователей. Сопряжение защитных механизмов.	системе. Аутентификация пользователей. Сопряжение защитных механизмов (часть 1).									
7		Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов (часть 2).	Тест 3.	1	Разработка и реализация алгоритма функционирования системы безопасности субъектов.	7			Поиск информации по теме лабораторной работы	2	10
8	Архитектура защищенных операционных систем.	Архитектура защищенных операционных систем (часть 1).									
Всего по контрольной точке (аттестации) № 2											**20**
9	Архитектура защищенных операционных систем.	Архитектура защищенных операционных систем (часть 2).	Тест 4.	1	Разработка и реализация алгоритма функционирования системы безопасности субъектов.	5			Поиск информации по теме лабораторной работы	1	7
10	Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе.	Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе (часть 1).			Разработка и реализация алгоритма сетевого фильтра.	8			Поиск информации по теме лабораторной работы	3	13
11		Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной систе-	Тест 5.	1							

		ме (часть 2).									
12	Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей	Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей (часть 1)	Тест 6.	1							
Всего по контрольной точке (аттестации) № 3											**20**
13	Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей	Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей (часть 2)			Разработка и реализация алгоритма криптографического преобразования.	18					20
14	Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная	Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая элек-	Тест 7.	1							

	подпись.	тронная подпись (часть 1).									
15		Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись (часть 2).	Тест 8.	**1**							