МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Томский государственный университет систем управления и радиоэлектроники»
(ТУСУР)

УТВЕРЖДАЮ

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

«___» _____ 2016 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень основной образовательной программы бакалавриат

Направление подготовки (специальность) 01.03.02 - Прикладная математика и информатика

Форма обучения очная

Факультет систем управления

Кафедра автоматизированных систем управления

Курс 3

Семестр 6

Учебный план набора 2013 **года и последующих лет.**

Распределение рабочего времени:

Виды учебной работы	Семестр 6	Всего	Единицы
Лекции	28	28	часов
Лабораторные работы	26	26	часов
Практические занятия	18	18	часов
Курсовой проект/работа (КРС) (аудиторная)	не предусмотрено	не предусмотрено	часов
Всего аудиторных занятий	72	72	часов
Из них в интерактивной форме	8	8	часов
Самостоятельная работа студентов (СРС)	72	72	часов
Всего (без экзамена)	144	144	часов
Самост. работа на подготовку и сдачу экзамена	36	36	часов
Общая трудоемкость	180	180	часов
(в зачетных единицах)	5	5	ЗЕТ

Экзамен: 6 семестр

Зачет: не предусмотрено **Диф. зачет:** не предусмотрено

Томск 2016

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта профессионального образования (ФГОС ПО) по направлению 01.02.03 Прикладная математика и информатика (квалификация (степень) бакалавр), утвержденного Приказом Министерства образования и науки Российской Федерации 12.03.2015 №228, рассмотрена и утверждена на заседании кафедры «12» февраля 2016 г., протокол № 5.

Разработчик д.т.н., профессор каф. АСУ _____ А.Н. Горитов

Зав. кафедрой д.т.н., профессор каф. АСУ _____ А.М. Кориков

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами специальности.

Декан ФСУ к.т.н., доцент _____ П.В. Сенченко

Зав. профилирующей и выпускающей
кафедрой АСУ д.т.н., профессор _____ А.М. Кориков

Эксперт:

Кафедра АСУ, доцент _____ А.И. Исакова

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

В современных условиях хозяйствования актуальным становится требование подготовки специалистов, обладающих необходимыми навыками использования современных информационных систем и технологий в различных областях. Необходимой составляющей такой подготовки являются как теоретические знания, так и практические навыки в области защиты информации и информационной безопасности.

Цель дисциплины – дать студентам необходимые знания, умения и навыки в области современных информационных технологий, применяемых в настоящее время, а также защиты информации. При этом основными задачами дисциплины являются:

- 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 ООП

Дисциплина «Информационная безопасность» относится к числу дисциплин вариативной частиучебного плана. «Информационная безопасность» как учебная дисциплина в системе подготовки бакалавров по направлению 01.03.02 связана с дисциплинами учебного плана: «Алгебра и геометрия», «Математическая логика и теория алгоритмов», «Организация и функционирование ЭВМ», «Архитектура компьютеров», «Языки и методы программирования». Знания и навыки, полученные при изучении этой дисциплины, используются в последующей дисциплине профессионального цикла: «Программное обеспечение ЭВМ и сетей» и при подготовке выпускной квалификационной работы.

После изучения дисциплины «Информационная безопасность» студент должен

знать:

- основные понятия и направления в защите компьютерной информации,
- принципы защиты информации,
- принципы классификации и примеры угроз безопасности компьютерным системам,
- современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности,
- основные инструменты обеспечения многоуровневой безопасности в информационных системах.

уметь:

- конфигурировать встроенные средства безопасности в операционной системе,
- проводить анализ защищенности компьютера и сетевой среды;
- устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи;
- устанавливать и использовать один из межсетевых экранов;
- организовывать регистрацию пользователей в сетевой операционной системе,
- организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа,
- организовывать безопасную работу в Интернет;
- организовывать отправку почтовых сообщений с использованием глобальной сети Интернет;
- использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.

владеть:

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

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование общепрофессиональной компетенций ОПК-4: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Вид учебной работы	Всего часов	Семестры			
		1	2	3	4
Аудиторные занятия (всего)	**72**				**72**
В том числе:					
Лекции	28				28
Лабораторные работы (ЛР)	26				26
Практические занятия (ПЗ)	18				18
Семинары (С)	–				–
Коллоквиумы (К)	–				–
Курсовой проект (работа) (аудиторная нагрузка)	–				–
Другие виды аудиторной работы					
Самостоятельная работа (всего)	**72**				**72**
В том числе:					
Курсовой проект (работа) (самостоятельная работа)	–				–
Расчетно-графические работы	–				–
Реферат	–				–
Другие виды самостоятельной работы					
Проработка лекционного материала	16				16
Подготовка к практическим занятиям	18				18
Подготовка к лабораторным занятиям	26				26
Самостоятельное изучение тем теоретической части	12				12
Подготовка к экзамену	**36**				**36**
Вид промежуточной аттестации (зачет, экзамен)	экзамен				экзамен
Общая трудоемкость час	**180**				**180**
зач. ед.	**5**				**5**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Лаб. зан.	Практ. зан.	СРС	Всего часов	Формируемые компетенции
1.	Введение в информационную безопасность.	2	–	2	3	7	ОПК-4
2.	Законодательные и правовые основы защиты компьютерной информации.	3	–	4	6	13	ОПК-4
3.	Математические методы и модели в задачах защиты информации.	4	11	2	27	44	ОПК-4
4.	Математические основы криптографических методов.	3	–	2	4	9	ОПК-4
5.	Криптография с открытым ключом	4	15	–	17	36	ОПК-4
6.	Методы идентификации и аутентификации пользователей.	3	–	2	4	9	ОПК-4
7.	Межсетевые экраны и VPN сети.	4	–	2	4	10	ОПК-4
8.	Защита компьютерных систем от вредоносных программ.	3	–	2	4	9	ОПК-4
9.	Комплексная защита информации.	2	–	2	3	7	ОПК-4
	ИТОГО	**28**	**26**	**18**	**72**	**144**	

5.2. Содержание разделов дисциплины (по лекциям)

№ п/п	Наименование разделов	Содержание разделов	Трудоемкость (час.)	Формируемые компетенции
1.	Введение в информационную безопасность	Исторические аспекты и современная постановка задач обеспечения информационной безопасности (ИБ) и защиты информации, связь проблем ИБ с развитием информационных технологий (ИТ) и процессами глобализации. Основные понятия и определения: конфиденциальность, целостность, доступность, угроза, уязвимость, риски. Обзор и параметры классификации угроз безопасности информации. Принципы защиты информации. Классы средств защиты информации. Государственная стратегия обеспечения ИБ в России.	2	ПК-3
2.	Законодательные и правовые основы	Основы российского законодательства в сфере защиты информации: закон об информации, информационных технологиях и за-	3	ПК-3

	защиты компьютерной информации	щите информации; закон о государственной тайне; закон о защите персональных данных; закон об электронной цифровой подписи. Ответственность за правонарушения и преступления в сфере компьютерной информации и защиты информации. Политика безопасности. Модели безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем.		
3.	Математические методы и модели в задачах защиты информации	Основные понятия криптографии. Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. Симметричные системы шифрования. Основные понятия и определения. Классификация симметричных систем шифрования: поточные шифры, блочные шифры. Блочные шифры. Сеть Фейштеля. Потоковые шифры. Основные понятия. Алгоритм потокового шифрования.	4	ПК-3
4	Математические основы криптографических методов	Основные понятия и определения теории информации. Основные теоремы теории чисел: арифметика вычетов, малая теорема Ферма, теорема Эйлера, разложение числа на простые сомножители. Наибольший общий делитель. Алгоритм Евклида. Обобщенный алгоритм Евклида. Возведение в степень по модулю. Дискретные логарифмы в конечном поле. Понятия однонаправленной функции и однонаправленной функции с лазейкой. Элементы теории сложности проблем. Классы сложности проблем.	3	ПК-3
5	Криптография с открытым ключом	Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. Шифр Шамира. Шифр Эль-Гамаля. Алгоритм RSA. Вопросы стойкости. Задача распределения ключей. Метод Диффи-Хеллмана. Криптографические хеш-функции. Основные сведения о функциях хеширования. Хеш-функции на базе блочных шифров. Общие сведения об электронной цифровой подписи (ЭЦП). Основные процедуры цифровой подписи. Вопросы стойкости ЭЦП. Сертификат открытого ключа.	4	ПК-3
6.	Методы идентификации и аутентификации пользователей	Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации, использующие пароли и PIN-коды: на основе многоразовых паролей, на основе одноразовых паролей, на основе сертификатов. Строгая аутентификация, основанная: на симметричных алгоритмах, на асимметричных алгоритмах, на однонаправленных хеш-функциях. Биометрическая аутентификация пользователя.	3	ПК-3
7.	Межсетевые экраны и VPN сети	Межсетевые экраны. Режим функционирования межсетевых экранов и их основные компоненты. Экранирующий маршрутизатор. Шлюзы сетевого уровня. Прикладной шлюз. Основные схемы сетевой защиты на базе межсетевых экранов. Формирование политики межсетевого взаимодействия. Персональные межсетевые экраны. Виртуальные защищенные сети. Концепция построения виртуальных защищенных сетей (VPN). Основные понятия и функции. Классификация VPN сетей. Основные варианты архитектуры VPN. Достоинства применения технологии VPN. Программно-аппаратные средства защиты ПЭВМ и сетей; методы средства ограничения доступа к компонентам сети; методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям: методы и средства хранения ключевой информации; защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.	4	ПК-3
8.	Защита компьютерных систем от	Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов.	3	ПК-3

	вредоносных программ.	Программные закладки и методы защиты от них.		
9.	Комплексная защита информации	Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Постановка задачи оптимизации системы защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ. Перспективы КЗИ: защищенные информационные технологии.	2	ПК-3
	ИТОГО		**28**	

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

№ п/п	Наименование обеспечивающих (предыдущих) дисциплин	№ № разделов данной дисциплины, для которых необходимо изучение обеспечивающих (предыдущих) дисциплин								
		1	2	3	4	5	6	7	8	9
	Предшествующие дисциплины									
1.	Алгебра и геометрия			+	+	+	+	+		
2.	Математическая логика и теория алгоритмов			+	+	+	+	+		
3.	Организация и функционирование ЭВМ						+	+	+	
4.	Архитектура вычислительных сетей и систем						+	+		+
5.	Языки и методы программирования			+	+	+	+	+	+	
	Последующие дисциплины									
1.	Программное обеспечение ЭВМ и сетей	+	+	+	+	+	+	+	+	+
2.	Выпускная квалификационная работа			+	+	+	+	+	+	+

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

Перечень компетенций	Виды занятий				Формы контроля
	Л	Лаб.	Прак.	СРС	
ОПК-4		+			Устный ответ на лаб. работе, опрос на лекции, подготовка отчета и защита лабораторной работы, дом. задание, тест, опрос на прак.

Л – лекция, Прак. – практические работы, Лаб. – лабораторные работы, СРС – самостоятельная работа студента

6. МЕТОДЫ И ФОРМЫ ОРГАНИЗАЦИИ ОБУЧЕНИЯ

Для успешного освоения дисциплины применяются различные образовательные технологии, которые обеспечивают достижение планируемых результатов обучения согласно основной образовательной программе, с учетом требований к объему занятий в интерактивной форме.

Технологии интерактивного обучения при разных формах занятий

Формы / Методы	Лекции (час)	Лабораторные занятия (час)	Практические занятия (час)	Всего (час)
Работа в команде		2	**2**	**4**
Пресс-конференция	2			**2**
Поисковый метод		2		**2**
Итого интерактивных занятий	**2**	**4**	**2**	**8**

Примечание.

1. «Работа в команде» происходит при коллективном решении задачи на лабораторной работе № 4 и на практическом занятии № 5.
2. «Поисковый метод» студенты используют при выполнении лабораторной работы № 6.
3. «Пресс-конференция» используется для обсуждения вопросов, связанных с разработкой алгоритмов криптографической защиты информации.

7. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Методические указания по лабораторным работам и задания к ним приведены в разделе 12.3 [2].

№ п/п	№ раздела дисциплины из табл. 5.1	Наименование лабораторных работ	Трудоемкость (час.)	Компетенции
1.	3	Блочное симметричное шифрование	4	ОПК-4

2.	3	Изучение ППП систем криптографической защиты информации, классическая криптография	4	ОПК-4
3.	5	Асимметричное шифрование	4	ОПК-4
4.	5	Электронная цифровая подпись (ЭЦП)	4	ОПК-4
5.	5	Практическое применение криптографии с открытым ключом. Пакет PGP	4	ОПК-4
6.	3, 5	Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI	6	ОПК-4
	ИТОГО		**26**	

8. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ (СЕМИНАРЫ)

Методические указания по практическим занятиям и задания к ним приведены в разделе 12.3 [1].

№ п/п	№ раздела дисциплины из табл. 5.1	Темы практических занятий (семинарских)	Трудоемкость (час.)	Компетенции
1.	1	Принципы защиты информации. Методы оценки уязвимости информации.	2	ОПК-4
2.	2	Федеральное законодательство о защите информации.	2	ОПК-4
3.	2	Государственные стандарты и руководящие документы.	2	ОПК-4
4.	3	Современные приложения криптографии.	2	ОПК-4
5.	4	Математические основы криптографических методов.	2	ОПК-4
6.	6	Методы идентификации и аутентификации.	2	ОПК-4
7.	7	Основные технологии построения защищенных информационных систем.	2	ОПК-4
8.	8	Место информационной безопасности информационной системы в национальной безопасности страны. Концепция информационной безопасности.	2	ОПК-4
9.	9	Комплексная система обеспечения информационной безопасности.	2	ОПК-4
	ИТОГО		**18**	

9. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	№ раздела дисциплины из табл. 5.1	Тематика самостоятельной работы *(детализация)*	Трудоемкость (час.)	Компетенции	Контроль выполнения работы
1.	1 ÷ 9	Проработка лекционного материала	16	ОПК-4	Опрос на занятиях
2.	1 ÷ 9	Подготовка к практическим занятиям	18	ОПК-4	Дом. задание, проверка решения задач
3.	3 ÷ 9	Подготовка к лабораторным занятиям	26	ОПК-4	Отчет, защита лаб. работы
4.	3	Самостоятельное изучение тем теоретической части	12	ОПК-4	Дом. задание, устный опрос, тест
5.	1 ÷ 9	Подготовка и сдача экзамена	36	ОПК-4	Оценка за экзамен
		ИТОГО	**108**		

Темы для самостоятельного изучения

1) Блочный шифр BLOWFISH (3 час).
2) Блочный шифр RC5 (3 час).
3) Блочный шифр RC6 (3 час).
4) Блочный шифр IDEA (3 час).

Темы для самостоятельного изучения входят в раздел № 3 изучаемой дисциплины.

10. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ

Учебным планом не предусмотрены.

11. РЕЙТИНГОВАЯ СИСТЕМА ДЛЯ ОЦЕНКИ УСПЕВАЕМОСТИ СТУДЕНТОВ

Курс 3, семестр 6 Контроль обучения – Экзамен.
Максимальный семестровый рейтинг – 100 баллов.

По дисциплине «Информационная безопасность» итоговой формой отчетности в 6 семестре является **экзамен**, все 100 баллов входят в семестровую составляющую.

Для стимулирования планомерности работы студента в семестре в раскладку баллов по элементам контроля введен компонент своевременности, который применяется только для студентов, без опозданий, отчитывающихся по предусмотренным элементам контроля (лабораторные работы).

На протяжении всего семестра текущая успеваемость **оценивается только в баллах** нарастающим итогом, в том числе и результаты контрольных точек.

В таблице 11.1 содержится распределение баллов в течение 6 семестра для дисциплины «Информационная безопасность», завершающейся **экзаменом** и содержащей 14 лекций (28 часов), 6 лабораторных работ (26 часов), 9 практических занятий и 3 итоговых теста во время проведения двух контрольных точек и между ними. В таблице 11.2 представлен пересчет суммы баллов по 1 и 2 контрольной точке в традиционную оценку.

Таблица 11.1 – Дисциплина «Информационная безопасность» (**экзамен**, лекции, лабораторные работы, практические занятия)

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
Посещение занятий	4	3	3	**10**
Тестовый контроль	6	6	6	**18**
Выполнение и защита лабораторных работ	6	12	12	**30**
Компонент своевременности	4	4	4	**12**
Итого максимум за период:	**20**	**25**	**25**	**70**
Сдача экзамена (максимум)				**30**
Нарастающим итогом	**20**	**45**	**70**	**100**

По результатам текущего контроля формируется допуск студента к итоговому контролю – экзамену по дисциплине. Экзамен осуществляется в форме опроса по теоретической части дисциплины. В составе суммы баллов, полученной студентом по дисциплине, заканчивающейся **экзаменом**, экзаменационная составляющая должна быть не менее 10 баллов. В противном случае экзамен считается не сданным, студент в установленном в ТУСУРе порядке обязан его пересдать.

Методика выставления баллов за ответы на **экзамене** определяется из расчета до **10 баллов** за каждый из **3 вопросов в билете**.

Неудовлетворительной сдачей экзамена считается экзаменационная составляющая **менее 10 баллов**. При неудовлетворительной сдаче экзамена (<10 баллов) или неявке на экзамен экзаменационная составляющая приравнивается к нулю (0).

Таблица 11.2 – Пересчет суммы баллов по 1 и 2 контрольной точке в традиционную оценку

Оценка (ГОС)	**Сумма баллов, на 1-ую контрольную точку с начала семестра**	**Сумма баллов, на 2-ую контрольную точку за период между 1КТ и 2КТ**
5 (отлично)	**18 – 20**	**40 – 45**
4 (хорошо)	**15 – 17**	**31 – 39**
3 (удовлетворительно)	**10 – 14**	**27 – 30**
2 (неудовлетворительно)	**Ниже 10 баллов**	**Ниже 27 баллов**

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично)	90 – 100	A (отлично)
4 (хорошо)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно), (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

12.1 Основная литература

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие для вузов. – М.: ФОРУМ, 2012. – 592 с. (30 экз.)

12.2 Дополнительная литература

1. Бацула А.П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (25 экз.)

2. Партыка Т.Л. Информационная безопасность: Учебное пособие для вузов. 3-е изд., испр. и доп. – М.: Форум, 2007. – 367 с. (20 экз.)

2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2005. – 144 с. (50 экз.)

3. Мельников В.П. Информационная безопасность и защита информации: учебн. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред.: С. А. Клейменов. – М.: Academia, 2006. – 330 с. (30 экз.)

4. Куприянов А.И. Основы защиты информации: учебн. пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. – М.: Academia, 2006. – 253 с. (50 экз.)

5. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др]. – М.: Горячая линия – Телеком, 2006. – 544 с. (80 экз.)

6. Смарт Н. Криптография: учебник для вузов: пер. с англ. / пер. С. А. Кулешов, ред. пер. С. К. Ландо. – М.: Техносфера, 2005. – 525 с. (11 экз.)

12.3 Перечень пособий, методических указаний и материалов, используемых в учебном процессе

Перечень методических указаний по практической работе:

1. Горитов А.Н. Информационная безопасность: методические указания к практическим занятиям по дисциплине «Информационная безопасность» для направления подготовки 010400.62 – «Прикладная математика и информатика». – Томск: ТУСУР, 2011. – 8 с. [Электронный ресурс]. – Режим доступа: http://asu.tusur.ru/learning/010302/d42/010302-d42-pract.pdf

Перечень методических указаний по лабораторным работам:

2. Горитов А.Н. Информационная безопасность: методические указания по выполнению лабораторных работ студентов всех форм обучения для направления подготовки 010400.62 – «Прикладная математика и информатика». – Томск: ТУСУР, 2011. – 7 с. [Электронный ресурс]. – Режим доступа: http://asu.tusur.ru/learning/010302/d42/010302-d42-lab.pdf

Перечень методических указаний по самостоятельной работе студентов:

3. Горитов А.Н. Информационная безопасность: методические указания по самостоятельной и индивидуальной работе студентов всех форм обучения для направления подготовки 010400.62 – «Прикладная математика и информатика». – Томск: ТУСУР, 2011. – 9 с. [Электронный ресурс]. – Режим доступа: http://asu.tusur.ru/learning/010302/d42/010302-d42-work.pdf

Операционная система MS Windows, MicroSoft Visual C++ Express Edition.

12.4 Базы данных, информационно-справочные и поисковые системы

Не требуются.

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения лекций по дисциплине используются персональный ПК с проектором. Лабораторные занятия осуществляются в компьютерном классе кафедры АСУ.

Приложение к рабочей программе

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Томский государственный университет систем управления и радиоэлектроники»
(ТУСУР)

УТВЕРЖДАЮ

Проректор по учебной работе

_____ П.Е.Троян

«___» _____ 2016 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень основной образовательной программы бакалавриат

Направление подготовки (специальность) 01.03.02 - Прикладная математика и информатика

Форма обучения очная

Факультет систем управления

Кафедра автоматизированных систем управления

Курс 3

Семестр 6

Учебный план набора 2013 **года и последующих лет.**

Экзамен: 6 семестр

Зачет: не предусмотрено

Диф. зачет: не предусмотрено

Томск 2016

1. ВВЕДЕНИЕ

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины «**Информационная безопасность»** и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной «**Информационная безопасность»** компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенции
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** • основные понятия и направления в защите компьютерной информации, • принципы защиты информации, • принципы классификации и примеры угроз безопасности компьютерным системам, • современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности, • основные инструменты обеспечения многоуровневой безопасности в информационных системах. **Уметь:** • конфигурировать встроенные средства безопасности в операционной системе, • проводить анализ защищенности компьютера и сетевой среды; • устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; • устанавливать и использовать один из межсетевых экранов; • организовывать регистрацию пользователей в сетевой операционной системе, • организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа, • организовывать безопасную работу в Интернет; • организовывать отправку почтовых сообщений с использованием глобальной сети Интер-

		нет; • использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов. **Владеть:** • навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.

2. РЕАЛИЗАЦИЯ КОМПЕТЕНЦИЙ

Компетенция ОПК-4

ОПК-4: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания, представлены в таблице 2.

Таблица 2 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	– Знает методы решения стандартных залач профессиональной деятельности с учетом основных требований информационной безопасности.	– Умеет решать стандартные залачи профессиональной деятельности с учетом основных требований информационной безопасности.	– Владеет методами решения стандартных залач профессиональной деятельности с учетом основных требований информационной безопасности.
Виды занятий	– Лекции; – Практические занятия – Групповые консультации	– Практические занятия; – Самостоятельная работа студентов	– Практические занятия; – Самостоятельная работа студентов
Используемые средства оценивания	– Тест; – Контрольная работа; – Выполнение домашнего задания;	– Подготовка и устная защита индивидуального домашнего задания (презентация); – Конспект самостоятельной работы	– Защита отчета индивидуальной работы, – Защита домашнего задания;

Общие характеристики показателей и критериев оценивания компетенции на всех этапах приведены в таблице 3.

Таблица 3 – Общие характеристики показателей и критериев оценивания компетенции по этапам

Показатели и критерии	Знать	Уметь	Владеть
ОТЛИЧНО (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
ХОРОШО (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
УДОВЛЕТВОРИТЕЛЬНО (низкий уровень)	Обладает низким уровнем общих знаний	Обладает умениями на низком уровне, которые не достаточны для выполнения даже простых задач	Работает только при прямом наблюдении

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Показатели и критерии	**Знать**	**Уметь**	**Владеть**
ОТЛИЧНО (высокий уровень)	– Знает основные понятия и направления в защите компьютерной информации; – Знает принципы защиты информации; – Знает принципы классификации и примеры угроз безопасности компьютерным системам; – Знает современные подходы к защите продуктов и систем информационных технологий; – Знает основные инструменты обеспечения многоуровневой безопасности в информационных системах.	Умеет конфигурировать встроенные средства безопасности в операционной системе, Умеет проводить анализ защищенности компьютера и сетевой среды; Умеет устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; Умеет устанавливать и использовать один из межсетевых экранов; Умеет организовывать регистрацию пользователей в сетевой операционной системе; Умеет организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа, Умеет организовывать безопасную работу в Интернет; Умеет организовывать отправку почтовых сообщений с использованием глобальной сети Интернет; Умеет использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;	Владеет навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.

ХОРОШО (базовый уровень)	Знает основные понятия и направления в защите компьютерной информации; Знает принципы защиты информации; Знает принципы классификации и примеры угроз безопасности компьютерным системам; Знает современные подходы к защите продуктов и систем информационных технологий; Имеет представление о основных инструментах обеспечения многоуровневой безопасности в информационных системах.	Умеет конфигурировать встроенные средства безопасности в операционной системе; Умеет проводить анализ защищенности компьютера и сетевой среды; Умеет устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; Умеет устанавливать и использовать один из межсетевых экранов; Умеет организовывать регистрацию пользователей в сетевой операционной системе; Умеет организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа; Умеет организовывать безопасную работу в Интернет; Умеет организовывать отправку почтовых сообщений с использованием глобальной сети Интернет; Умеет использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.	– Хорошо владеет навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.
УДОВЛЕТВОРИТЕЛЬНО (низкий уровень)	Понимает важность защиты информиции; Знает основные понятия и направления в защите компьютерной информа-	Умеет конфигурировать встроенные средства безопасности в операционной системе; Умеет проводить	Владеет основными приемами применения методов и средств защиты информации

	ции; Знает базовые принципы классификации и примеры угроз безопасности компьютерным системам; Имеет представление о современным подходе к защите продуктов и систем информационных технологий; Знает основные инструменты обеспечения безопасности в информационных системах.	анализ защищенности компьютера и сетевой среды; Умеет устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; Умеет устанавливать и использовать один из межсетевых экранов; Умеет организовывать регистрацию пользователей в сетевой операционной системе; Умеет организовывать безопасную работу в Интернет; Умеет организовывать отправку почтовых сообщений с использованием глобальной сети Интернет; Умеет использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.	для обеспечения информационной безопасности на предприятии или организации.

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ

Для реализации вышеперечисленных задач обучения используются следующие материалы: типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в составе, приведенном ниже.

Темы лабораторных работ

1) Блочное симметричное шифрование.
2) Изучение ППП систем криптографической защиты информации, классическая криптография.
3) Асимметричное шифрование.
4) Электронная цифровая подпись (ЭЦП).
5) Практическое применение криптографии с открытым ключом. Пакет PGP.
6) Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI.

Темы практических занятий

1) Принципы защиты информации. Методы оценки уязвимости информации.
2) Федеральное законодательство о защите информации.
3) Государственные стандарты и руководящие документы.
4) Современные приложения криптографии.
5) Математические основы криптографических методов.
6) Методы идентификации и аутентификации.
7) Основные технологии построения защищенных информационных систем.
8) Место информационной безопасности информационной системы в национальной безопасности страны. Концепция информационной безопасности.
9) Комплексная система обеспечения информационной безопасности.

Пример типовых вопросов по тестам

Вопрос:

К какой главе УК РФ относятся ст. 272, ст. 273, ст. 274 в области информационной безопасности:

Выберите один из 3 вариантов ответа:

1) 25
2) 28
3) 27

Вопрос:

Что такое политика информационной безопасности организации:

Выберите один из 3 вариантов ответа:

1) совокупность механизмов компьютерных систем
2) инструкции администраторам по настройке информационных систем
3) набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию

Вопрос:

К биометрической системе защиты относятся:
(выберите несколько вариантов ответа)

Выберите несколько из 5 вариантов ответа:

1) Защита паролем
2) Физическая защита данных
3) Антивирусная защита
4) Идентификация по радужной оболочке глаз
5) Идентификация по отпечаткам пальцев

Вопрос:

Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

Выберите один из 5 вариантов ответа:

1) Загрузочный вирус
2) Макровирус
3) Файловый вирус
4) Сетевой червь
5) Троян

Темы для самостоятельной работы (темы рефератов)

1) Блочный шифр BLOWFISH.
2) Блочный шифр RC5.
3) Блочный шифр RC6.
4) Блочный шифр IDEA.

Вопросы для подготовки к экзамену

1) Законодательные и нормативные документы информационной безопасности.
2) Алгоритмы симметричного шифрования.
3) Шифрование информации на основе сети Фейштеля.
4) Алгоритм шифрование TEA
5) Алгоритм шифровании DES
6) Алгоритм шифрования ГОСТ 28147-89.
7) Алгоритм шифрования AES.
8) Режимы выполнения алгоритмов симметричного шифрования.
9) Потоковое шифрование.
10) Алгоритмы потокового шифрования.
11) Криптографические хеш-функции.
12) Хеш-функции на основе блочных шифров.
13) Функция хеширования MD4.
14) Основные теоремы теории чисел.
15) Наибольший общий делитель. Алгоритмы Евклида.
16) Односторонняя функция.
17) Криптография с открытым ключом.
18) Задача распределения ключей.
19) Алгоритм Диффи-Хеллмана.
20) Алгоритм шифрования RSA.
21) Комбинированная криптосистема.
22) Электронная цифровая подпись.
23) Алгоритм цифровой подписи RSA.
24) Алгоритм цифровой подписи DSA.
25) Алгоритм цифровой подписи ГОСТ 3410-94.
26) Инфраструктура открытых ключей.
27) Сертификат открытого ключа.
28) Идентификация, аутентификация, авторизация.
29) Методы аутентификации, использующие одноразовые и многоразовые пароли.
30) Методы аутентификации, использующие симметричные и ассиметричные алгоритмы.
31) Биометрическая аутентификация пользователя.
32) Межсетевые экраны. Функции межсетевых экранов.
33) Основные типы межсетевых экранов.
34) Виртуальные частные сети.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, в составе:

Основная литература

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие для вузов. – М.: ФОРУМ, 2012. – 592 с. (30 экз.)

Дополнительная литература

1. Бацула А.П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (25 экз.)

2. Партыка Т.Л. Информационная безопасность: Учебное пособие для вузов. 3-е изд., испр. и доп. – М.: Форум, 2007. – 367 с. (20 экз.)

2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2005. – 144 с. (50 экз.)

3. Мельников В.П. Информационная безопасность и защита информации: учебн. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред.: С. А. Клейменов. – М.: Academia, 2006. – 330 с. (30 экз.)

4. Куприянов А.И. Основы защиты информации: учебн. пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. – М.: Academia, 2006. – 253 с. (50 экз.)

5. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др]. – М.: Горячая линия – Телеком, 2006. – 544 с. (80 экз.)

6. Смарт Н. Криптография: учебник для вузов: пер. с англ. / пер. С. А. Кулешов, ред. пер. С. К. Ландо. – М.: Техносфера, 2005. – 525 с. (11 экз.)

Методические указания к практическим занятиям

1. Горитов А.Н. Информационная безопасность: методические указания к практическим занятиям по дисциплине «Информационная безопасность» для направления подготовки 010400.62 – «Прикладная математика и информатика». – Томск: ТУСУР, 2011. – 8 с. [Электронный ресурс]. – Режим доступа:
http://asu.tusur.ru/learning/010302/d42/010302-d42-pract.pdf

Методические указания к лабораторным работам

1. Горитов А.Н. Информационная безопасность: методические указания по выполнению лабораторных работ студентов всех форм обучения для направления подготовки 010400.62 – «Прикладная математика и информатика». – Томск: ТУСУР, 2011. – 7 с. [Электронный ресурс]. – Режим доступа:
http://asu.tusur.ru/learning/010302/d42/010302-d42-lab.pdf

Методические указания по самостоятельной работе

1. Горитов А.Н. Информационная безопасность: методические указания по самостоятельной и индивидуальной работе студентов всех форм обучения для направления подготовки 010400.62 – «Прикладная математика и информатика». – Томск: ТУСУР, 2011. – 9 с. [Электронный ресурс]. – Режим доступа:
http://asu.tusur.ru/learning/010302/d42/010302-d42-work.pdf