Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»
Таганрогский институт имени А. П. Чехова (филиал) «РГЭУ (РИНХ)»

УТВЕРЖДАЮ
Директор филиала
_____ А. Ю. Голобородько
«___» _____ 2016г.

Рабочая программа дисциплины

Б1.Б.13.5 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки

09.03.03 «Прикладная информатика»

Профиль

09.03.03.01 «Прикладная информатика в менеджменте»

Уровень образования

бакалавриат

Таганрог
2016 г.

ФАКУЛЬТЕТ	1	физики, математики, информатики
КАФЕДРА	2	Информатики
	(код)	(наименование)

ОБЩИЙ ОБЪЕМ* работы обучающихся в час.	уч. план **144**	Очная форма	Заочная форма 4г 6 м	
Всего аудиторных занятий, час., в том числе:			**12**	
- лекций,			4	
по семестрам			4 (7)	
- лабораторные занятия,			8	
по семестрам				8 (8)
- практические занятия,				
по семестрам				
В интерактивной форме, час			2	
Всего самостоятельной работы, час., в том числе:			**92**	
- контрольные работы по семестрам				
- курсовые работы по семестрам				
- курсовые проекты по семестрам				
- другое			32 (7)	60 (8)
Изучено и переаттестовано, час.				
Зачеты, по семестрам, час				4 (8)
Экзамены, по семестрам, час				
Всего ЗЕТ по учебному плану		3		

* Объем часов по всем видам работ переносится из учебного плана.

ОСНОВАНИЕ

ФГОС ВО по направлению подготовки направление 09.03.03 «Прикладная информатика» (квалификация «бакалавр») утвержден Приказом Министерства образования и науки Российской Федерации от 12.03.2015 г. №207

Учебный план направления 09.03.03 «Прикладная информатика»профиль 09.03.03.01 «Прикладная информатика в менеджменте» одобрен Ученым советом вуза 31.05.2016 г. протокол № 11.

АВТОР (Ы) канд. техн. наук, доцент, доцент кафедры информатики		Драгныш Н.В.	02.06.2016
(ученая степень, звание, должность)	(подпись)	(Ф.И.О.)	(дата)

ОБСУЖДАЛАСЬ И СОГЛАСОВАНА

Кафедрой информатики		Ромм Я.Е.	02.06.2016
	(подпись)	(Ф.И.О.)	(дата)
Факультет физики, математики, информатики		Донских С.А.	09.06.2016
(наименование)	(подпись)	(Ф.И.О.)	(дата)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. **Цели** освоения дисциплины: формирование у студентов знаний, способствующих решению профессиональных задач с помощью современных методов защиты информации; исследование моделей и методов информационной безопасности компьютерных систем при решении практических задач; повышение уровня грамотности в области информационной безопасности; формирование профессиональной информационной культуры.

1.2. **Задачи:** обучение студентов теоретическим основам курса, овладение методами решения практических задач и приобретение навыков самостоятельной научной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. **Цикл (раздел) ОП:** Б1.Б.13

2.2. **Связь с другими дисциплинами учебного плана**

Перечень предшествующих дисциплин	Перечень последующих дисциплин, видов работ
Б1.Б.8 Информатика и программирование Б1.Б.12.1 Вычислительные системы, сети и телекоммуникации	Б2.П Производственная практика Б3 Государственная итоговая аттестация

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Студент должен знать:
основные методы защиты информации; основные угрозы информационной безопасности; основные требования информационной безопасности; основные методы и средства обеспечения информационной безопасности (ОПК-1, ОПК-4)
Студент должен уметь:
вести безопасную информационную деятельность в условиях агрессивной среды; идентифицировать и оперативно устранять угрозы информационной безопасности; анализировать и выбирать методы и средства обеспечения информационной безопасности (ОПК-1, ОПК-4)
Студент должен владеть:
методами сокрытия и защиты информации; навыками анализа информационной безопасности прикладных объектов; навыками использования средств информационной безопасности при решении прикладных задач (ОПК-1, ОПК-4)
У студента должны быть сформированы элементы следующих компетенций:
ОПК-1: способность использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий
ОПК-4: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Аудиторные занятия − заочная форма обучения

Неделя	Кол. Час	в том числе в интерактивной форме, час.	Вид занятия, модуль, тема и краткое содержание	Формируемые компетенции
5-6	***4***	–	**Лекции**	
	4	–	**Модуль 1 «Основные понятия курса»**	ОПК-1, ОПК-4
19	*2*		**Тема 1.1.** Введение в информационную безопасность компьютерных систем. Понятия и составляющие информационной безопасности. Классификация угроз. Примеры угроз.	
20	*2*		**Тема 1.2.** Комплексный подход к обеспечению безопасности. Уровни информационной безопасности. Стандарты и спецификации в области информационной безопасности. Административный уровень. Политика информационной безопасности. Основные программно-технические меры	
	8	***2***	**Лабораторные работы**	
	2	***2***	**Модуль 2 «Основы криптографии. Сетевая защита»**	ОПК-1, ОПК-4
40	*2*	*2*	Лабораторная работа №1. Абсолютно стойкий шифр. Применение режима однократного гаммирования	
41	*2*		Лабораторная работа №2. Использование однократного гаммирования. Шифрование (кодирование) различных исходных текстов одним ключом	
42-43	*4*		Лабораторные работы №3-4. Моделирование работы n разрядного скремблера	

4.2. Самостоятельная работа студента – заочная форма обучения

Неделя	Кол. час	Темы, разделы, вынесенные на самостоятельную подготовку, тематика рефератной работы, контрольных работ, рекомендации по использованию литературы, ЭВМ и др.	Формируемые компетенции
		Темы, разделы, вынесенные на самостоятельную подготовку	ОПК-1, ОПК-4
19-22	16	1. Классификация криптографических систем. Криптография как наука. Основные понятия. Типы криптосистем. Типы криптоатак и стойкость алгоритмов. 2. Основы криптографии с секретным ключом. Сети Файстеля. Характеристика современных симметричных блочных шифров. Объединение блочных шифров. 3. Управление криптографическими ключами. Криптографические протоколы. Криптографические протоколы. Распределение секретных ключей. Распределение открытых ключей. Распределение секретных ключей с помощью системы с открытым ключом. Обмен ключами по схеме Диффи-Хеллмана.	
19-22	16	1. Аутентификация. Основные понятия. Парольная аутентификация. Методы аутентификации сообщений. Коды аутентичности сообщений. 2. Использование алгоритмов. Канальное шифрование. Сквозное шифрование. Оконечное (абонентское, сквозное) шифрование. Объединение канального и сквозного шифрования. Шифрование данных для хранения. Аппаратное и программное шифрование. Программное шифрование. 3. Протокол аутентификации Kerberos. Основные концепции. Диалог аутентификации. Области Kerberos. Флаги мандата.	
25-40	26	1. Защита на сетевом уровне Характеристика протокола IPSec. Протоколы IPSec. Управление политикой IPSec в Windows. 2. Защита WWW. Угрозы и способы защиты потока данных в WWW. Протоколы SSL и TLS. Архитектура SSL. 3. Защищенные многоцелевые расширения электронной почты S/MIME. RFC 822 и Многоцелевые расширения электронной почты. Типы содержимого и кодировки MIME. Функции и алгоритмы S/MIME. Обработка сертификатов S/MIME 4. Защита электронной почты с помощью PGP Функции PGP. Генерирование ключей PGP. Формат сообщения PGP. 5. Нарушители и вирусы Основные понятия. Обнаружение вторжений. Защита от вирусов. Методы обнаружения и удаления.	
25-40	**34**	**Темы и вопросы, определяемые преподавателем с учетом интересов студента** *Темы рефератов*	ОПК-1, ОПК-4

		1. Информационное право и информационная безопасность. 2. Концепция информационной безопасности. 3. Основы экономической безопасности предпринимательской деятельности. 4. Анализ законодательных актов об охране информационных ресурсов открытого доступа. 5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа. 6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность. 7. Информационная безопасность (по материалам зарубежных источников и литературы). 8. Правовые основы защиты конфиденциальной информации. 9. Экономические основы защиты конфиденциальной информации. 10. Организационные основы защиты конфиденциальной информации. 11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне. 12. Составление инструкции по обработке и хранению конфиденциальных документов. 13. Направления и методы защиты документов на бумажных носителях. 14. Направления и методы защиты машиночитаемых документов. 15. Архивное хранение конфиденциальных документов. 16. Направления и методы защиты аудио- и визуальных документов. 17. Порядок подбора персонала для работы с конфиденциальной информацией. 18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы. 19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы. 20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам. 21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний. 22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы. 23. Порядок защиты информации в рекламной и выставочной деятельности. 24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники. 25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы). 26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.	

		27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе). 28. Назначение, виды, структура и технология функционирования системы защиты информации. 29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов. 30. Аналитическая работа по выявлению каналов утечки информации фирмы. 31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации. 32. Направления и методы защиты профессиональной тайны. 33. Направления и методы защиты служебной тайны. 34. Направления и методы защиты персональных данных о гражданах. 35. Методы защиты личной и семейной тайны. 36. Построение и функционирование защищенного документооборота. 37. Защита секретов в дореволюционной России. 38. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.	
	92	**Общая трудоемкость самостоятельной работы (час)**	
	4	**Подготовка к зачету**	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

1. Управление рисками
2. Основные определения и критерии классификации угроз
3. Вредоносное программное обеспечение
4. Основные угрозы конфиденциальности
5. Ролевое управление доступом
6. Протоколирование и аудит

5.2. Фонд оценочных средств для проведения текущего контроля

1. В чём заключается смысл однократного гаммирования?
2. Как по открытому тексту и ключу получить шифртекст?
3. Назовите недостатки шифрования одним ключом двух видов открытого текста?
4. Объясните основной принцип работы скремблера.
5. Какова идея составных блочных шифров?
6. Метод двусторонней атаки.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Основная и дополнительная литература

№	Выходные данные	Количество экземпляров[1]
	Основная литература[2]	
1	Спицын В. Г. Информационная безопасность вычислительной техники: учебное пособие. – Томск: Эль Контент, 2011	ЭБС Университетская библиотека ONLINE
2	Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012	ЭБС Университетская библиотека ONLINE
3	Аверченков В. И. , Рытов М. Ю. Организационная защита информации: учебное пособие для вузов. – М.: Флинта, 2011	ЭБС Университетская библиотека ONLINE
	Дополнительная литература[3]	
1	Сычев Ю. Н. Основы информационной безопасности: учебно-практическое пособие. – М.: Евразийский открытый институт, 2010	ЭБС Университетская библиотека ONLINE

[1] Указывается в соответствии с фактическим наличием в библиотеке РГЭУ (РИНХ). Для определения количества экземпляров следует воспользоваться программой «Книгообеспеченность», установленной на кафедре.
[2] Указывается не более пяти источников. Год издания должен соответствовать требованиям образовательного стандарта.
[3] Перечень дополнительной литературы не ограничен по числу источников и году издания.

№	Выходные данные	Количество экземпляров[1]
2	Редактор: Рытенкова О. Журнал "Information Security / Информационная безопасность. – М.: ГРОТЕК, 2012-2016	ЭБС Университетская библиотека ONLINE

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

№	Выходные данные
	http://www.intuit.ru, http://e.lanbook.com, http://biblioclub.ru, http://www.sbup.com/

6.3. Перечень программного обеспечения

№	Наименование программного обеспечения[4]
1	MS Office 2007

6.4. Перечень информационно-справочных систем

№	Наименование информационно-справочных систем
1	http://elibrary.ru
2	http://biblioclub.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

[4] Указываются только лицензионные программные средства

Лист переутверждения рабочей программы учебной дисциплины

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2017 - 2018 учебном году на заседании кафедры информатики, протокол № 10 от «04» мая 2017 г.

Зав. кафедрой информатики Ромм Я.Е.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2017 - 2018 учебном году на заседании совета факультета физики, математики, информатики, протокол № 22 от «11» мая 2017 г.

Декан факультета физики, математики, информатики Донских С.А.