

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий
Герасименко С.А.
(подпись, раскраска подписи)
"26" февраля 2016 г.



РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ОД.11 Защита информационных процессов в компьютерных системах»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки)

Общий профиль

(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа академического бакалавриата

Квалификация

Бакалавр

Форма обучения

Очная

Оренбург 2015

Рабочая программа дисциплины «Б.1.В.ОД.11 Защита информационных процессов в компьютерных системах» /сост.

Н.А. Тишина - Оренбург: ОГУ, 2015

Рабочая программа предназначена студентам очной формы обучения по направлению подготовки 09.03.01 Информатика и вычислительная техника

© Тишина Н.А., 2015
© ОГУ, 2015

Содержание

1 Цели и задачи освоения дисциплины	4
2 Место дисциплины в структуре образовательной программы	4
3 Требования к результатам обучения по дисциплине	5
4 Структура и содержание дисциплины.....	6
4.1 Структура дисциплины	6
4.2 Содержание разделов дисциплины.....	7
4.3 Лабораторные работы	8
4.4 Практические занятия (семинары).....	8
5 Учебно-методическое обеспечение дисциплины	8
5.1 Основная литература.....	8
5.2 Дополнительная литература	8
5.3 Периодические издания	9
5.4 Интернет-ресурсы.....	10
5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий	10
6 Материально-техническое обеспечение дисциплины.....	10
Лист согласования рабочей программы дисциплины.....	12
Дополнения и изменения в рабочей программе дисциплины	
Приложения:	
Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	
Методические указания для обучающихся по освоению дисциплины.....	

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Формирование теоретических знаний по методам и средствам защиты информационных процессов в компьютерных системах и практических умений применения их для защиты информации в компьютерных системах

Задачи:

Изучить: основные понятия и определения; источники, риски и формы атак на информацию; политика безопасности; стандарты безопасности; криптографические модели; алгоритмы шифрования; модели безопасности основных ОС; алгоритмы аутентификации пользователей; принципы функционирования основных программно-аппаратных средств обеспечения безопасности информации

Научиться применять методы и средства защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения в компьютерных системах: формировать рекомендации по обеспечению безопасности компьютерных систем; реализовывать криптографические методы защиты компьютерной информации; конфигурировать основные средства защиты информации

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.3 Иностранный язык, Б.1.Б.10.2 Алгебра и геометрия, Б.1.Б.10.3 Теория вероятностей и математическая статистика, Б.1.Б.11 Дискретная математика, Б.1.Б.16 Программирование*

Требования к входным результатам обучения, необходимым для освоения дисциплины

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции <i>В таблице оставляются только строки с компетенциями, по которым предварительные результаты обучения должны быть сформированы до начала изучения данной дисциплины. Остальные строки удаляются разработчиком рабочей программы</i>
Знать: идиоматически ограниченную речь, а также освоить стиль нейтрального научного изложения; основы аннотирования, реферирования и перевода научной литературы по безопасности информации. Уметь: применять знания в практике профессиональной коммуникации и перевода текстов со словарем и без словаря; применять иноязычные навыки для изучения и анализа новейшей информации в области безопасности информации. Владеть: иностранным языком в объеме, необходимом для возможности полу-	ОК-5 способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции <i>В таблице оставляются только строки с компетенциями, по которым предварительные результаты обучения должны быть сформированы до начала изучения данной дисциплины. Остальные строки удаляются разработчиком рабочей программы</i>
чения информации из зарубежных источников по безопасности информации;	
Знать: функциональную и структурную организацию компьютера, понятие и структуру программного и аппаратного обеспечения для информационных и автоматизированных систем Уметь: использовать основные технологические и функциональные возможности операционных систем Владеть: навыками инсталлирования инструментальных средств разработки программ	ОПК-1 способностью инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем
Знать: базовые понятия линейной алгебры, теории вероятностей и математической статистики, дискретной математики; современные технологии программирования, способы и механизмы управления данными в процессе разработки, отладки, тестирования программ для решения широкого круга задач на ЭВМ; инструментальные средства разработки программ Уметь: использовать математические методы для решения практических задач; разрабатывать программы на языке высокого уровня для решения практических задач; работать с современными системами программирования; Владеть: навыками программирования на языке высокого уровня	ОПК-2 способностью осваивать методики использования программных средств для решения практических задач

Постреквизиты дисциплины: *Б.1.В.ОД.16 Проектирование автоматизированных систем, Б.2.В.П.1 Научно-исследовательская работа (распределенная), Б.2.В.П.2 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: принципы функционирования основных программно-аппаратных средств обеспечения информационной безопасности, методы и средства защиты информации в процессе хранения и передачи по компьютерным сетям: классификация, функции; технологии криптографической защиты информации, технологии аутентификации, модели безопасности операционных систем Уметь: применять технологии криптографической защиты информации, технологии аутентификации для защиты информации в компьютерных системах, выбирать инструментальные средства и методы управления средствами сетевой безопасности, уметь	ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
применять сетевые сканеры для выявления уязвимостей компьютерных систем. Владеть: методами аутентификации на основе паролей и PIN кодов, строгой аутентификации	информационной безопасности
Знать: математические основы криптографических методов защиты информации; современные криптографические алгоритмы ; способы обеспечения информационной безопасности компьютерных систем Уметь: разрабатывать компоненты средств защиты информации, реализующие криптографические методы защиты компьютерной информации Владеть: стандартными библиотеками объектно-ориентированного языка для реализации криптографических методов защиты информации	ПК-2 способностью разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	180	180
Контактная работа:	73,25	73,25
Лекции (Л)	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	36	36
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - выполнение индивидуального творческого задания (ИТЗ); - выполнение расчетно-графического задания (РГЗ); - написание реферата (Р); - написание эссе (Э); - самостоятельное изучение разделов (перечислить); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - подготовка к лабораторным занятиям; - подготовка к практическим занятиям; - подготовка к коллоквиумам; - подготовка к рубежному контролю и т.п.)	106,75 30 16,75 24 36	106,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	экзамен	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1.	Введение. Проблемы безопасности информации. Математические основы криптографии. Вычислительная сложность	37	4	4	8	21
2.	Криптографические методы защиты информации	52	6	6	16	24
3.	Технологии аутентификации	24	2	2	4	16
4.	Протоколы защиты информации	24	2	2	4	16
5.	Программные средства защиты информации в компьютерных системах	24	2	2	4	16
6.	Модели безопасности операционных систем	19	2	2	0	15
	Итого:	180	18	18	36	108
	Всего:	180	18	18	36	108

4.2 Содержание разделов дисциплины

№ раздела	Наименование раздела	Содержание раздела
1	Введение. Проблемы безопасности информации. Математические основы криптографии. Вычислительная сложность	Основные понятия защиты информации и информационной безопасности. Анализ угроз безопасности информации. Современные тенденции в области обеспечения и нарушения безопасности информации. Стандарты и правовое обеспечение информационной безопасности. Арифметика остатков. Расширенный алгоритм Евклида. Теорема Лагранжа. Китайская теорема об остатках. Поиск простых чисел. Основы теории вычислительной сложности. Оценка сложности алгоритмов. Машина Тьюринга. P и NP - задачи. Односторонние функции.
2	Криптографические методы защиты информации	Основные понятия криптографии, классификация криптографических алгоритмов. Исторические шифры Стеганография. Шифры замены и перестановки. Поточковые шифры. Симметричные шифры. Ассиметричные шифры. Хэш-функция. Цифровая подпись. Управление криптографическими ключами.
3	Технологии аутентификации	Аутентификация, авторизация, администрирование. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация. Аппаратно-программные системы идентификации и аутентификации.
4	Протоколы защиты информации	Протоколы аутентификации. Протоколы обмена ключами. Шифрование сетевого трафика. Анализ протоколов распределения ключей. BAN –логика.
5	Программные средства защиты информации в компьютерных системах	Классификация. Антивирусы. Межсетевые экраны. VPN. Системы обнаружения вторжений.
5	Модели безопасности	Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС. Избирательная модель. Изолированная среда.

№ раздела	Наименование раздела	Содержание раздела
	операционных систем	Полномочная модель.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	1	Стеганография.	4
2.	1	Поиск десятизначных простых чисел	4
3.	2	Шифры замены и перестановки	4
4.	2	Симметричные шифры	6
5.	2	Ассиметричные шифры	6
6.	3	Реализация проверки подлинности	4
7.	4	Реализация протоколов защиты информации	4
8.	5	Анализ сетевого трафика	4
		Итого:	36

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
	1	Современные технологии защиты информации (семинар)	2
1.	1	Стеганография (семинар)	2
2.	1	Оценка сложности алгоритмов	2
3.	1	Арифметика по модулю простого числа	2
4.	2	Симметричные алгоритмы шифрования	2
5.	2	Асимметричные алгоритмы шифрования	2
6.	2,3	Проверка подлинности документов, субъектов (семинар)	2
7.	4	Протоколы защиты информации (семинар)	2
8.	5	Средства защиты информации (семинар)	2
9.	1-5	Модели безопасности операционных систем. Дифференцированный зачет	2
		Итого:	18

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие [Электронный ресурс] / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4. – Режим доступа: <http://znanium.com/bookread2.php?book=402686>

5.2 Дополнительная литература

- 1 Бернет, С.. Криптография. Официальное руководство RSA Security = RSA Security's Official Guide to Cryptography / С. Бернет, С. Пэйн ; пер. с англ. под ред. А. И. Тихонова. - М. : Бином, 2009. - 382 с. (фнб-8; фнб чз-2)
- 2 Бондаренко, И. И. Криптографические средства защиты информации [Текст] : метод. указания к лаб. и самостоят. работе студентов / И. И. Бондаренко, И. В. Влацкая, М. Ю. Нестеренко; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. мат. обеспечения информ. систем. - Оренбург : ГОУ ОГУ, 2005. - 29 с. - Библиогр.: с. 29. Издание на др. носителе [Электронный ресурс] (ентл-7; кх-3)
- 3 Костин, В. Н. Проектирование систем физической защиты потенциально опасных объектов на основе развития современных информационных технологий и методов синтеза сложных систем [Текст] : монография / В. Н. Костин, С. Н. Шевченко, Н. В. Гарнова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. прогр. обеспечения вычисл. техники и автоматизир. систем. - Оренбург : Университет, 2014. - 202 с. : ил; 12,63 печ. л. - Библиогр.: с. 198-202. - ISBN 978-5-4417-0413-7. (ентл-20)
- 4 Мельников, В. П. Защита информации [Текст] : учебник для подготовки бакалавров по направлению 230100 "Информатика и вычислительная техника" / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе; под ред. В. П. Мельникова. - Москва : Академия, 2014. - 297 с. - (Высшее образование. Бакалавриат). - Библиогр.: с. 291-293. - ISBN 978-5-4468-0332-3. (10)
- 5 Методы спектрального анализа в задаче обнаружения аномалий информационных процессов телекоммуникационных сетей [Текст] : монография / Н. А. Соловьев [и др.]; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. прогр. обеспечения вычисл. техники и автоматизир. систем. - Оренбург : Университет, 2013. - 172 с. : ил. - Библиогр.: с. 113-123. - Прил.: с. 124-171. - ISBN 978-5-4417-0330-7.
- 6 Семененко, В. А. Программно-аппаратная защита информации: учеб. пособие для вузов / В. А. Семененко, Н. В. Федоров. - М. : МГИУ, 2007. - 340 с.(15)
- 7 Смарт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. - Москва: Техносфера, 2006. - 528 с. (22)
- 8 Торстейнсон, П.. Криптография и безопасность в технологии . NET/ П. Торстейнсон, Г. А. Ганеш; пер. с англ. В. Д. Хорева ; под ред. С. М. Молявко. - М. : Бином, 2007. - 480 с. (11)
- 9 Шалкина, Т. Н. Методы и средства защиты компьютерной информации [Электронный ресурс] : метод. указания к лаб. практикуму / Т. Н. Шалкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычислит. техники. - Электрон. текстовые дан. (1 файл: Kb). - Оренбург : ОГУ, 2006. -Adobe Acrobat Reader 5.0 Издание на др. носителе [Текст]
- 10 Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: учеб. пособие для студентов вузов, обучающихся по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с. (12)

5.3 Периодические издания

Журналы:

- «Безопасность информации»;
- «Программирование»;
- «Программные продукты и системы»;
- «Информационные технологии»;
- «Безопасность информационных технологий»;
- «Хаккер»

5.4 Интернет-ресурсы

- ФСТЭК России. Федеральная служба по техническому и экспортному контролю <http://fstec.ru/>
- Информационный портал по ИТ безопасности <http://www.securitylab.ru/>
- Информационный сайт: Безопасник <http://bezopasnik.org/article>
- Образовательные порталы:
 - Интернет университет информационных технологий: <http://www.intuit.ru/>
 - Все образование в Интернете <http://all.edu.ru/>
 - Сервер Центра информатизации Министерства общего и профессионального образования Информика <http://www.informika.ru/>
- Виртуальные учебные курсы и сайты дистанционного образования:
 - Дистанционное образование в Интернете <http://www.lessons.ru/>
 - Центр дистанционного образования <http://www.eidos.ru/>
 - Центр дистанционного обучения <http://www.cdo.ru/>
- Энциклопедии и справочные сайты:
 - Свободная энциклопедия <https://ru.wikipedia.org/wiki>
 - Словари и энциклопедии на Академике <http://dic.academic.ru/dic.nsf/ruwiki/8410>
 - Море аналитической информации <http://www.citforum.ru>
 - RSDN-magazine <http://rsdn.ru/>

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

- интегрированный пакет *Open Office*;
- среды программирования *MS Visual Studio*, *NetBeans*;

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами.

Лекционные занятия проводятся в аудитории № 1318, имеющей материально-техническое обеспечение:

- компьютер модели Intel Celeron-S -1шт.;
- монитор модели Samsung 793 DF – 1шт.;
- экран настенный стационарный – 1шт.;
- проектор модели Viewsonic PJ510 – 1шт.;
- источник бесперебойного питания – 1шт.;
- сервер модели Intel Xeon – 1шт.;
- сервер модели 2x DualCore AMD Opteron 2218 – 1шт.

Лабораторные работы и практические занятия проводятся в компьютерных классах кафедры ПОВТАС – ауд. №№ 3310, 1318, 2214.

В компьютерных классах установлено оборудование:

- системные блоки модели Intel Celeron – 10шт.;
- мониторы модели Samsung 793 DF – 10шт.;
- принтер лазерный модели Canon LBP-3000 – 1шт.;
- проектор модели NEC PORTABLE ПРОЕКТОР VT46/G – 1шт.;
- экран настенный стационарный – 1шт.;

- источник бесперебойного питания – 10шт.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.

ЛИСТ

согласования рабочей программы

Направление подготовки: 09.03.01 Информатика и вычислительная техника
код и наименование

Профиль: Общий профиль

Дисциплина: Б.1.В.ОД.11 Защита информационных процессов в компьютерных системах

Форма обучения: очная
(очная, очно-заочная, заочная)

Год набора 2015

РЕКОМЕНДОВАНА заседанием кафедры

Кафедра программного обеспечения вычислительной техники и автоматизированных систем
наименование кафедры

протокол № 6 от "9" 02 2016 г.

Ответственный исполнитель, заведующий кафедрой

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

наименование кафедры

подпись

Соловьев Н.А.

расшифровка подписи

Исполнители:

доцент

должность

подпись

Тишина Н.А.

расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

09.03.01 Информатика и вычислительная техника

код наименование

личная подпись

Соловьев Н.А.

расшифровка подписи

Заведующий отделом комплектования научной библиотеки

личная подпись

Истомина Т.В.

расшифровка подписи

Уполномоченный по качеству факультета

личная подпись

Крючкова И.В.

расшифровка подписи

Начальник отдела информационных образовательных технологий ЦИТ

личная подпись

Дырдина Е.В.

расшифровка подписи

Дополнения и изменения в рабочей программе учебной дисциплины
«Б.1.В.ОД.11 Защита информационных процессов в компьютерных системах» Направление
подготовки 09.03.01 Информатика и вычислительная техника профиля «Общий профиль»

на 2016 год набора

Внесенные изменения на 2016 год набора

УТВЕРЖДАЮ
/ Декан факультета математики и информационных технологий
Герасименко С.А.
(подпись/расшифровка подписи)
"19" 08 2016 г.

В рабочую программу внесены следующие изменения:

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

В блок основной литературы рабочей программы включены следующие электронные издания:

1 Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие [Электронный ресурс] / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2017. - 592 с.; ил.; 70х100 1/16. - (Высшее образование: бакалавриат). (переплет) ISBN 978-5-8199-0411-4. – Режим доступа: <http://znanium.com/bookread2.php?book=546679>

5.4 Интернет-ресурсы

- ФСТЭК России. Федеральная служба по техническому и экспортному контролю <http://fstec.ru/>
- Информационный портал по ИТ безопасности <http://www.securitylab.ru/>
- Информационный сайт: Безопасник <http://bezopasnik.org/article>
- Образовательные порталы:
 - Все образование в Интернете <http://all.edu.ru/>
 - Виртуальные учебные курсы и сайты дистанционного образования:
 - Дистанционное образование в Интернете <http://www.lessons.ru/>
 - Центр дистанционного образования <http://www.eidos.ru/>
 - Центр дистанционного обучения <http://www.cdo.ru/>
- Энциклопедии и справочные сайты:
 - Свободная энциклопедия <https://ru.wikipedia.org/wiki>
 - Словари и энциклопедии на Академике <http://dic.academic.ru/dic.nsf/ruwiki/8410>
 - Море аналитической информации <http://www.citforum.ru>

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

интегрированный пакет Open Office;
среда программирования MS Visual Studio

Рабочая программа пересмотрена на заседании кафедры программного обеспечения
вычислительной техники и автоматизированных систем

28 июня 2016 года, протокол №10

Соловьев Н.А.

(дата, номер протокола заседания кафедры, подпись зав. кафедрой)

СОГЛАСОВАНО:

Заведующий отделом комплектования научной библиотеки

Н.Н. Грицай

личная подпись

расшифровка подписи

Уполномоченный по качеству факультета

И.В.Крючкова

личная подпись

расшифровка подписи