Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ОД.10 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

Год набора 2017

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра программного обеспечения вычислительной техники и автоматизированных систем
наименование кафедры

протокол № 6 от "14" 02 2017 г.

Заведующий кафедрой
Кафедра программного обеспечения вычислительной техники и автоматизированных систем
наименование кафедры *подпись* Н.А. Соловьев *расшифровка подписи*

Исполнители:
доцент *подпись* Н.А.Тишина
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
09.03.01 Информатика и вычислительная техника Н.А. Соловьев
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись Н.Н. Грицай *расшифровка подписи*

Уполномоченный по качеству факультета
личная подпись И.В. Крючкова *расшифровка подписи*

№ регистрации 56671

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 и навыков их применения для защиты информационных процессов в компьютерных системах

Задачи:

Изучить: основные понятия и определения; угрозы и риски безопасности информации в компьютерных системах; стандарты безопасности; основные понятия, методы и средства криптографии; модели безопасности компьютерных систем; технологию аутентификации; принципы функционирования основных программно-аппаратных средств обеспечения безопасности информации.

Научиться разрабатывать и применять программные средства защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения в компьютерных системах.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б.1.Б.15 Операционные системы, Б.1.Б.16 Сети электронно-вычислительных машин и телекоммуникации*

Постреквизиты дисциплины: *Б.1.В.ОД.14 Проектирование автоматизированных информационных систем, Б.2.В.П.2 Технологическая 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: Теоретические основы разработки компонентов аппаратно-программных комплексов, обеспечивающих безопасность информации в компьютерных системах: основные термины; основы криптосистем; технологию аутентификации; модели разграничения доступа. Обзор программно-аппаратных средств защиты **Уметь:** разрабатывать компоненты программно-аппаратных комплексов, обеспечивающих защиту информации в процессе ее сбора, хранения, обработки, передачи и распространения в компьютерных системах **Владеть:** стандартными библиотеками объектно - ориентированного языка для разработки компонентов, реализующих методы 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 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	**216**	**216**
Контактная работа:	**73,25**	**73,25**
Лекции (Л)	36	36
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	18	18
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю и т.п.)*	**142,75**	**142,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1.	Введение. Проблемы безопасности информации.	30	6	2	2	20
2.	Криптографические методы защиты информации	58	12	8	6	32
3.	Технология аутентификации	40	6	2	4	28
4.	Модели безопасности компьютерных систем	28	4	2	2	20
5.	Программно-аппаратные средства защиты информации в компьютерных системах	30	4	2	2	22
6.	Безопасность распределенных приложений	30	4	2	2	22
	Итого:	216	36	18	18	144
	Всего:	216	36	18	18	144

4.2 Содержание разделов дисциплины

№ раздела	Наименование раздела	Содержание раздела
1	Введение. Проблемы безопасности информации.	Основные понятия защиты информации и информационной безопасности. Угрозы и риски безопасности информации. Современные тенденции в области обеспечения и нарушения безопасности информации. Стандарты и правовое обеспечение информационной безопасности.

№ раздела	Наименование раздела	Содержание раздела
2	Методы и средства криптографической защиты информации	Основные понятия криптографии, классификация криптографических алгоритмов. Симметричные криптосистемы. Ассиметричные криптосистемы. Хэш-функция. Цифровая подпись. Протоколы обмена и распределения ключей. Шифрование сетевого трафика, SSL / TLS.
3	Технология аутентификации	Аутентификация, авторизация, администрирование. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация. Протоколы аутентификации. BAN –логика.
4	Модели безопасности компьютерных систем	Понятие политики и модели безопасности, монитор безопасности. Модели безопасности на основе дискреционной политики. Модели безопасности на основе мандатной политики. Модели безопасности на основе ролевой политики.
5	Программно-аппаратные средства защиты информации в компьютерных системах	Классификация и обзор программно-аппаратных средств защиты информации в компьютерных системах: антивирусы, межсетевые экраны, VPN, системы обнаружения вторжений.
6	Безопасность распределенных приложений	Обзор проблем и технологий обеспечения безопасности баз данных, электронной почты, социальных сетей, платежных систем, облачных сред.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	1	Анализ угроз безопасности информации	2
2.	2	Поиск десятизначных простых чисел	2
3.	2	Программная реализация симметричных шифров	2
4.	2	Программная реализация ассиметричных шифров	2
5.	3	Программная реализация криптографических протоколов	2
6.	3	Программная реализация методов аутентификации	2
7.	4	Программная реализация политики разграничения доступа	2
8.	5	Мониторинг безопасности в компьютерных системах	2
9.	6	Разработка компонентов безопасности распределенных приложений	2
		Итого:	18

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1.	1	Современные технологии защиты информации (семинар)	2
2.	2	Стеганография (семинар)	2
3.	2	Арифметика по модулю простого числа	2
4.	2	Симметричные алгоритмы шифрования	2
5.	2	Асимметричные алгоритмы шифрования	2
6.	3	Протоколы защиты информации (семинар)	2
7.	4	Модели безопасности компьютерных систем.	2

№ занятия	№ раздела	Тема	Кол-во часов
8.	5	Средства защиты информации (семинар)	2
9.	6	Проблемы и технологии обеспечения безопасности распределенных приложений.	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

2 Смарт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. - Москва: Техносфера, 2006. - 528 с.

5.2 Дополнительная литература

3 Бернет, С.. Криптография. Официальное руководство RSA Security = RSA Security'sOfficialGuidetoCryptography / С. Бернет, С. Пэйн ; пер. с англ. под ред. А. И. Тихонова. - М. : Бином, 2009. - 382 с. (фнб-8; фнб чз-2)

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 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)

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 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)

5.3 Периодические издания

Журналы:

1. Открытые системы. СУБД : журнал. - М. : Агентство "Роспечать", 2016.
2. Программные продукты и системы : журнал. - М. : Агентство "Роспечать", 2016.

5.4 Интернет-ресурсы

- ФСТЭК России. Федеральная служба по техническому и экспортному контролю http://fstec.ru/

Информация об уязвимостях http://www.iso27000.ru/katalog-ssylok/informaciya-ob-uyazvimostyah

- Информационный портал по ИТ безопасности http://www.securitylab.ru/
- Информационный сайт: Безопасникhttp://bezopasnik.org/article
- Виртуальные учебные курсы и сайты дистанционного образования:

• Интернет университет информационных технологий: https://www.intuit.ru/studies/courses?service=0&option_id=9&service_path=1

- Энциклопедии и справочные сайты:

• Свободная энциклопедия https://ru.wikipedia.org/wiki/Информационная_безопасность

https://www.lektorium.tv/course/22929 - «Лекториум», Курс лекций: Сложность вычислений и основы криптографии

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

- Банк данных угроз безопасности информации ФСТЭК РОССИИ https://bdu.fstec.ru/threat
- База данных угроз безопасности информации Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org/data/downloads/index.html
- ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2016]. – Режим доступа в сети ОГУ для установки системы: \\fileserver1\GarantClient\garant.exe
- КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2016]. – Режим доступа к системе в сети ОГУ для установки системы: \\fileserver1\!CONSULT\cons.exe

- Операционная система Microsoft Windows
- OpenOffice/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
- Средства для разработки и проектирования: Microsoft Visual Studio.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный компьютерной техникой, удовлетворяющей требованиям к конфигурации аппаратного обеспечения используемых программ.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

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