

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«С.1.Б.34 Защита программ и данных»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность

10.05.01 Компьютерная безопасность
(код и наименование специальности)

Разработка защищенного программного обеспечения
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация

Специалист по защите информации

Форма обучения

Очная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 3 от "14" декабре 2017г.

Заведующий кафедрой

Кафедра компьютерной безопасности и математического обеспечения информационных систем

И.В. Влацкая
наименование кафедры подпись расшифровка подписи

Исполнители:

доцент
должность И.В. Влацкая
подпись расшифровка подписи

старший преподаватель
должность П.Н. Полежаев
подпись расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по специальности

10.05.01 Компьютерная безопасность
код наименование И.В. Влацкая
личная подпись расшифровка подписи

Заведующий отделом комплектования научной библиотеки

Н.Н. Грицай
личная подпись расшифровка подписи

Уполномоченный по качеству факультета

И.В. Крючкова
личная подпись расшифровка подписи

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Развитие у будущих специалистов навыков защиты программ и данных с помощью специализированных инструментов, а также путем разработки программных решений.

Задачи:

- получение навыков автоматизации управления программами через их интерфейс;
- получение навыков использования и разработки программных и аппаратных криптографических средств аутентификации, обеспечения конфиденциальности и целостности информации;
- получение навыков использования средств радиочастотной идентификации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *С.1.Б.22 Языки программирования, С.1.Б.23 Методы программирования, С.1.Б.28 Основы информационной безопасности*

Постреквизиты дисциплины: *С.1.Б.41.3 Уязвимость программного обеспечения, С.1.В.ОД.4 Технология построения защищенных автоматизированных систем*

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
<u>Знать:</u> - современные алгоритмы и схемы криптографической защиты информации. <u>Уметь:</u> - выбирать подходящие алгоритмы и схемы криптографической защиты информации. <u>Владеть:</u> - навыками реализации алгоритмов и схем криптографической защиты информации в виде программных модулей.	ОПК-10 способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах
<u>Знать:</u> - основные стандарты в области криптографической защиты информации. <u>Уметь:</u> - подбирать необходимую научно-техническую информацию, методические материалы по криптографическим алгоритмам, схемам и протоколам. <u>Владеть:</u> - навыками классификации и обобщения научно-технической информации по криптографическим методам защиты.	ПК-1 способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности
<u>Знать:</u> - основные классификации информационных систем по степени защищенности, методы оценки защищенности компьютерных систем по различным критериям. <u>Уметь:</u>	ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- определять основные этапы теоретических и научно-исследовательских работ по оценке защищенности компьютерных систем. <u>Владеть:</u> - первичными навыками проведения экспериментально-исследовательских работ по сертификации средств защиты программ и данных для компьютерных систем.	защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований
<u>Знать:</u> - основные виды подсистем информационной безопасности компьютерной системы. <u>Уметь:</u> - применять средства криптографической защиты информации для обеспечения безопасности программ и данных. <u>Владеть:</u> - навыками программной реализации криптографических средств защиты информации, систем аутентификации пользователей.	ПК-8 способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы
<u>Знать:</u> - теоретические основы современных технологий программирования: объектно-ориентированного программирования, функционального программирования, рекурсивно-логического программирования, параллельного программирования. <u>Уметь:</u> - использовать защищенный цикл разработки программного обеспечения на практике. <u>Владеть:</u> - навыками применения технологий программирования для разработки защищенного программного обеспечения.	ПСК-1 способностью использовать современные технологии программирования для разработки защищенного программного обеспечения

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	180	180
Контактная работа:	61,25	61,25
Лекции (Л)	30	30
Практические занятия (ПЗ)	30	30
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 практическим занятиям; - подготовка к коллоквиумам; - подготовка к рубежному контролю и т.п.)	118,75	118,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	экзамен	

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Автоматизация управления сторонними приложениями	36	4	10		22
2	Использование существующих средств криптографической и стеганографической защиты информации.	42	10	8		24
3	Реализация средств криптографической защиты информации	48	6	8		34
4	Безопасность операционных систем	54	10	4		40
	Итого:	180	30	30		120
	Всего:	180	30	30		120

4.2 Содержание разделов дисциплины

1 Автоматизация управления сторонними приложениями. Управление окнами других приложений. Мотивация, способы управления. Просмотр структуры окон приложений. Использование Windows API, AutoIt, UI Automation для управления окнами.

2 Использование существующих средств криптографической и стеганографической защиты информации. Программа TrueCrypt. Назначение, достоинства, недостатки, история создания. Основные возможности программы. Устройство тома. Используемая криптографическая схема, используемые алгоритмы шифрования и хеширования, режим XTS, алгоритм PBKDF2.

Программа KeePass Password Safe. Назначение, достоинства, недостатки. Основные возможности программы, включая создание и использование паролей TAN, а также настройку специальных параметров безопасности. Используемая криптографическая схема, принципы работы генератора псевдослучайных чисел, средства защиты процесса (защита памяти процесса DP API, Secure Desktop, двухканальная обфускация автовода).

Понятие атаки полного перебора и перебора по словарю. Демонстрация использования данных атак на примере подбора парольных фраз для тома TrueCrypt и защищенного хранилища KeePass.

Основные характеристики и принципы работы. Основные понятия: симметричные и асимметричные криптосистемы, PKI, сертификат (OpenPGP и X.509), удостоверяющий центр, проверка сертификата, списки отзывов сертификатов, сеть доверия, MITM-атака. Способы избежать MITM-атаки при использовании OpenPGP и X.509. Программы GnuPG и Gpg4Win.

Современные аппаратные и аппаратно-программные криптографические решения для идентификации, аутентификации, обеспечения конфиденциальности и целостности. Понятие идентификации и аутентификации. Способы аутентификации. Смарт-карты. Биометрические системы. Аппаратные токены.

Стеганография. Направления стеганографии. Компьютерная стеганография и её методы. Стеганоанализ и методы стеганоанализа изображений. OpenPuff. Цифровые водяные знаки (ЦВЗ). Метод LSB. Особенности файлов, сжатых с потерей данных (JPEG). Атаки на системы встраивания ЦВЗ. Соккрытие данных в видеопоследовательностях.

Технологии радиочастотной идентификации RFID. Основные понятия: RFID-метка, считыватель, RFID-система. Устройство RFID-метки. Классификация RFID-систем, RFID-меток (по частоте, источнику питания, типу используемой памяти), считывателей. Основные достоинства и недостатки RFID. Примеры и сферы использования.

3 Реализация средств криптографической защиты информации. Криптографические средства .NET. Поддерживаемые криптографические примитивы. Симметричные и асимметричные алгоритмы и их использования с помощью соответствующих классов .NET.

Генерация псевдослучайных чисел в .NET, классы обычных хеширующих алгоритмов и хеширующих алгоритмов с ключом. Понятие HMAC.

4 Безопасность операционных систем. Безопасность ОС Linux. Пользователи, группы и права доступа. Средства разграничения прав пользователей и программ. Сетевая безопасность, межсетевой экран netfilter. Шифрование файлов и жёсткого диска. dm-crypt и TrueCrypt.

Безопасность ОС Windows. Пользователи, группы пользователей и политики групп. Контроль учетных записей пользователей UAC. Аутентификация, протокол Kerberos. Шифрование данных EFS, BitLocker и их отличия. Протокол IPSec. Средство управления приложениями AppLocker. Примеры.

Безопасность мобильных ОС. Встроенные средства защиты. Сторонние приложения для защиты мобильных ОС.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Управление приложениями с помощью WinAPI и AutoIt	4
2	1	Управление приложениями с помощью UI Automation	6
3	2	Стандарты X.509 и OpenPGP. GnuPG	4
4	2	Использование программ TrueCrypt и KeePass Password Safe	2
5	2	Реализация атак полного перебора и перебора по словарю	2
6	3	Криптография в .NET	8
7	4	Конкурентная разведка в сети Интернет	4
		Итого:	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Торстейнсон, П. Криптография и безопасность в технологии. NET [Текст] / П. Торстейнсон, Г. А. Ганеш; пер. с англ. В. Д. Хорева; под ред. С. М. Молявко. - М. : Бином, 2007. - 480 с. : ил. - Предм. указ.: с. 448-472. - ISBN 978-5-94774-312-8.

5.2 Дополнительная литература

1. Соловьев, Н.А. Системы автоматизации разработки программного обеспечения [Текст] : учеб. пособие / Н. А. Соловьев, Е. Н. Чернопрудова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург : Университет, 2012. - 192 с. : ил. - Библиогр.: с. 182-183. - Прил.: с. 184-191. - ISBN 978-5-4417-0086-3.

2. Фаулер, М. UML в кратком изложении [Текст] : применение стандартного яз. объектного моделирования: пер. с англ. / М. Фаулер, К. Скотт; под ред. Л. А. Калиниченко. - М. : Мир, 1999. - 191 с. : ил. - Библиогр.: с. 186-188. - ISBN 5-03-003331-9.

3. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] : учеб. пособие для вузов / А. А. Малюк. - М. : Горячая линия-Телеком, 2004. - 280 с. : ил. - Библиогр.: с. 276-278. - ISBN 5-93517-197-X.

5.3 Периодические издания

1. Вестник информационной безопасности : журнал. - М. : Агентство "Роспечать".
2. Системы безопасности : журнал. - М. : Агентство "Роспечать".
3. Проблемы информационной безопасности. Компьютерные системы : журнал. - М. : АПР.

5.4 Интернет-ресурсы

1. Взгляд изнутри: RFID и другие метки. – Режим доступа: <https://habrahabr.ru/post/161401/>
2. NET Framework Cryptography Model. – Режим доступа: <https://docs.microsoft.com/en-us/dotnet/standard/security/cryptography-model>
3. Автоматизация тестирования Windows-приложений с использованием .Net. – Режим доступа: <https://habrahabr.ru/post/100749/>

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

1. Операционная система Microsoft Windows.
2. Open Office/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Среда разработки Microsoft Visual Studio.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, курсового проектирования, 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 практических занятий используется компьютерный класс, оснащенный персональными компьютерами с установленным программным обеспечением.

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.