205

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий
_____ С.А. Герасименко
(подпись, расшифровка подписи)
"26" сентября 2014 г.

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.6.1 Защита программ и данных»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
02.03.01 Математика и компьютерные науки
(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Оренбург 2015

500727

Рабочая программа дисциплины «*Б.1.В.ДВ.6.1 Защита программ и данных***» /сост. П.Н. Полежаев - Оренбург: ОГУ, 2015. – 10 стр.**

Рабочая программа предназначена студентам очной формы обучения по направлению подготовки 02.03.01 Математика и компьютерные науки

Содержание

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Развитие у будущих бакалавров 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 дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.В.ОД.3 Криптографические методы защиты информации, Б.1.В.ОД.7 Теория кодирования, сжатия и восстановления информации*

Требования к входным результатам обучения, необходимым для освоения дисциплины

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изученияДисциплины	Компетенции
Знать: - основные понятия в области криптографической защиты информации. **Уметь:** - работать с симметричными и асимметричными алгоритмами защиты информации. **Владеть:** - навыками реализации простейших алгоритмов шифрования.	ОПК-4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем
Знать: - основные тенденции в области защиты информации. **Уметь:** - выявлять угрозы для безопасности информационных систем. **Владеть:** - базовыми навыками проектирования средств защиты информации.	ПК-1 способностью к определению общих форм и закономерностей отдельной предметной области

Постреквизиты дисциплины: *Б.2.В.П.1 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: - основные тенденции в развитии криптографических и стеганографических средств защиты информации. **Уметь:** - работать с криптографическими провайдерами, и использующими их программными инструментами.	ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа,

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Владеть: - навыками реализации криптографических схем и протоколов для защиты программ и данных.	алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности
Знать: - общие принципы автоматизации управления программами разного типа и для разных платформ. **Уметь:** - разрабатывать сценарии для автоматизации управления программами разного типа. **Владеть:** - получение навыков автоматизации управления программами через их интерфейс	ПК-1 способностью к определению общих форм и закономерностей отдельной предметной области
Знать: - основные стандарты в области радиочастотной идентификации. **Уметь:** - разрабатывать алгоритмические и программно-аппаратные решения для радиочастотной идентификации. **Владеть:** - навыками использования средств радиочастотной идентификации.	ПК-3 способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**40,25**	**40,25**
Лекции (Л)	16	16
Практические занятия (ПЗ)	24	24
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самостоятельное изучение разделов (безопасность операционных систем);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;*	**103,75** 20 30	**103,75** 20 30

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
- подготовка к практическим занятиям; *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	30 10 13.75	30 10 13.75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Автоматизация управления сторонними приложениями	26	2	4		20
2	Использование существующих средств криптографической и стеганографической защиты информации.	36	10	6		20
3	Реализация средств криптографической защиты информации	46	2	10		34
4	Безопасность операционных систем	36	2	4		30
	Итого:	144	16	24		104
	Всего:	144	16	24		104

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 автоввода).

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. Сокрытие 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 и библиотеки. Поддерживаемые криптографические примитивы. Симметричные и асимметричные алгоритмы и их использования с помощью соответствующих классов библиотек. Генерация псевдослучайных чисел, классы обычных хеширующих алгоритмов и хеширующих алгоритмов с ключом. Понятие HMAC.*

4 Безопасность операционных систем.*Безопасность ОС Linux. Пользователи, группы и права доступа. Средства разраничения 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	2	Стандарты X.509 и OpenPGP. GnuPG	2
3	2	Использование программ TrueCrypt и KeePass Password Safe	2
4	2	Реализация атак полного перебора и перебора по словарю	2
5	3	Реализация алгоритмов идентификации и аутентификации	4
6	3	Реализация криптографических алгоритмов шифрования	6
7	4	Настройка средств защиты в ОС Windows	4
		Итого:	24

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.

2. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]. - М.: ДМК Пресс, 2010. - 544 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=86475&sr=1

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, Фе-

дер. 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. Буч Г. Язык UML Руководство пользователя [Электронный ресурс] / Буч Г., Рамбо Д., Якобсон И. - ДМК Пресс, б.г.. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=86127.

4. 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. Дудихина О. В. Конкурентная разведка в Internet. Советы аналитика [Электронный ресурс] / Дудихина О. В., Дудихин В. В. - ДМК Пресс, 2009. - Режим доступа:http://www.biblioclub.ru/index.php?page=book&id=131362

5.3 Периодические издания

1. Вестник информационной безопасности : журнал. - М. : Агенство "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. – Режимдоступа: 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 текущей версии. Доступна в рамках подписки Microsoft DreamSpark Premium. Разработчик: компания Microsoft. Режим доступа: https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain=bdba23cf-e05e-e011-971f-0030487d8897&ws=58727022-4bac-e211-88b7-f04da23e67f4&vsro=8

2. Офисныйпакет Microsoft Office (Word, Excel, Power Point) текущейверсии. Доступен в рамках лицензионного соглашения OVS-ES. Разработчик: компания Microsoft. Режим доступа: https://products.office.com/en/home

3. Среда разработки Microsoft Visual Studio текущей версии. Доступна в рамках подписки Microsoft DreamSpark Premium. Разработчик: компания Microsoft. Режим доступа: https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain=bdba23cf-e05e-e011-971f-0030487d8897&ws=58727022-4bac-e211-88b7-f04da23e67f4&vsro=8

4. Криптографическая система TheGNUPrivacyGuardтекущей версии. Доступна бесплатно по свободной лицензииGNUGPL. Разработчик:The GnuPG Project. Режим доступа: https://gnupg.org/

5. Система шифрования логических контейнеров и физических томов жесткого диска VeraCrypttекущей версии. Доступна бесплатно. Разработчик: IDRIX. Режим доступа: https://veracrypt.codeplex.com/

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерным и мультимедийным оборудованием. Рабочие станции студентов и преподавателя объединены в локальную сеть с подключением к Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным проектором и экраном.

Практические занятия проходят в компьютерных классах, в которых установлено оборудование:

- системные блоки с процессором IntelCore 2 Duo;
- мониторы модели Samsung 793 DF.

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: 02.03.01 Математика и компьютерные науки
код и наименование

Профиль: Алгоритмы и приложения компьютерной математики

Дисциплина: Б.1.В.ДВ.6.1 Защита программ и данных

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

Год набора 2015

РЕКОМЕНДОВАНА заседанием кафедры
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 1 от "28" августа 2014 г.

Ответственный исполнитель, заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Преподаватель каф. КБМОИС — П.Н. Полежаев
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Заведующий кафедрой Кафедра алгебры и дискретной математики О.А. Пихтилькова
наименование кафедры *личная подпись* *расшифровка подписи*

Председатель методической комиссии по направлению подготовки
02.03.01 Математика и компьютерные науки
код наименование *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*

Рабочая программа зарегистрирована в ОИОТ ЦИТ
Начальник отдела информационных образовательных технологий ЦИТ
Е.В. Дырдина
личная подпись *расшифровка подписи*