Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.34 Защита программ и данных»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2023

Рабочая программа дисциплины «*Б1.Д.Б.34 Защита программ и данных*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "9" марта 2023 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры | *подпись* | И.В. Влацкая *расшифровка подписи*

Исполнители:
доцент | *должность* | *подпись* | И.В. Влацкая *расшифровка подписи*

должность | *подпись* | *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность
код наименование | *личная подпись* | И.В. Влацкая *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись | Н.Н. Бигалиева *расшифровка подписи* С.А. Бикташева

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

№ регистрации _____

© Влацкая И.В., 2023
© ОГУ, 2023

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 Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.16 Языки программирования, Б1.Д.Б.17 Методы программирования, Б1.Д.Б.22 Основы информационной безопасности*

Постреквизиты дисциплины: *Б1.Д.Б.44.3 Уязвимость программного обеспечения, Б1.Д.В.2 Технология построения защищенных автоматизированных систем*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1-В-2 Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ОПК-1-В-3 Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности ОПК-1-В-4 Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	**Знать:** - основные средства и способы обеспечения информационной безопасности; - принципы построения систем защиты информации. **Уметь:** - определять класс защищаемой информации повидам тайны и степеням конфиденциальности; - оценивать угрозы информационной безопасности для для объекта информатизации; - классифицировать угрозы информационной безопасности для объекта информатизации.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		Владеть: -навыками построения систем защиты информации для объектов информатизации.

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:	**91,25**	**91,25**
Лекции (Л)	30	30
Практические занятия (ПЗ)	30	30
Лабораторные работы (ЛР)	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.)*	**88,75**	**88,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Автоматизация управления сторонними приложениями	36	6	4	10	16
2	Использование существующих средств криптографической и стеганографической защиты информации.	42	10	10	6	16
3	Реализация средств криптографической защиты информации	48	6	8	8	26
4	Безопасность операционных систем	44	8	8	6	22
	Итого:	180	30	30	30	90
	Всего:	180	30	30	30	90

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 .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 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 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Управление приложениями с помощью WinAPI и AutoIt	4
2	1	Управление приложениями с помощью UI Automation	6

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
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

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Обзор основных средств защиты программ и данных	4
2	1	Алгоритмы шифрования и стеганографической защиты информации	4
3	2	Современные аппаратные и аппаратно-программные криптографические решения для идентификации, аутентификации, обеспечения конфиденциальности и целостности. Понятие идентификации и аутентификации	6
4	2	Программные средства подбора паролей	4
5	2	Технологии радиочастотной идентификации RFID.	4
6	3	Обеспечение безопасности операционных систем	4
7	4	Кибербразведка	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. : 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. – 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

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021.
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Антивирусное ПО: Kaspersky Endpoint Security для бизнеса, имеется лицензия на 2 года использования, входит в Реестр отечественного ПО

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.