Негосударственное аккредитованное некоммерческое
Частное образовательное учреждение высшего образования
«АКАДЕМИЯ МАРКЕТИНГА И СОЦИАЛЬНО-ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – ИМСИТ»
(г. Краснодар)

Факультет информатики и вычислительной техники
Кафедра математики и вычислительной техники

УТВЕРЖДАЮ
Председатель НМС,
проректор по учебной работе,
профессор
Н.Н. Павелко
16 апреля 2018г.

Б1.В.14
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОГРАММНЫХ СИСТЕМ

Рабочая программа по дисциплине для студентов
направления подготовки 09.03.04 Программная инженерия
Направленность (профиль) программы:
«Информационно-вычислительные системы»
Квалификация (степень выпускника) бакалавр

г. Краснодар
2018

Рабочая программа составлена с учётом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.04 Программная инженерия (уровень бакалавриата), утверждённого приказом Министерства образования и науки Российской Федерации от 12.03.2015 г. № 229

Составитель _____ Р.Р. Саакян

Согласовано:

Проректор по качеству, доцент К.В. Писаренко

Рецензенты:

Левченко В.И., к.т.н., доцент, доцент кафедры автоматизации производственных процессов КубГТУ

Суриков А.И., директор ООО «1С-КОНСОЛЬ»

Рабочая программа рассмотрена на заседании кафедры математики и вычислительной техники от 19.03.2018 г., протокол №8

Зав. кафедрой математики и
вычислительной техники, к.т.н., доцент _____ Н.С.Нестерова

Рабочая программа утверждена на заседании Научно-методического совета Академии от 16.04.2018 г., протокол №8.

1 Место дисциплины в структуре образовательной программы

Предшествующие дисциплины учебного плана направления подготовки бакалавриата 09.03.04, изучение которых необходимо для усвоения дисциплины «Информационная безопасность программных систем»:

- «Физика»;
- «Иностранный язык»;
- «Дискретная математика»;
- «Информатика и программирование»;
- «Базы данных»;

Данная дисциплина входит в базовую часть учебного плана подготовки по направлению 09.03.4 - Программная инженерия. Последующей дисциплиной учебного плана направления 09.03.04, изучение которой базируется на знаниях настоящей дисциплины «Веб-технологии».

2 Особенности реализации дисциплины

При реализации программы применяется электронное обучение и дистанционные образовательные технологии для поддержки самостоятельной работы обучающихся путём предоставления доступа к электронным программно-методическим комплексам дисциплин.

URL-адрес электронного обучающего ресурса по дисциплине: http://moodle.kubstu.ru (по паролю).

3 Планируемые результаты обучения по дисциплине

В результате освоения данной дисциплины у обучающегося формируются следующие компетенции (элементы компетенций):

ПК -4 владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества

4 Содержание дисциплины

ОЧНАЯ ФОРМА

Вид работы	Всего часов/зачетн. ед.	Семестр 7	Семестр 8
Общая трудоемкость (часы / зачетные единицы)	180/5	**72 / 2**	**108/3**
Аудиторная работа:	68/1,89	32/0,89	36/1
Лекции (Л)	28/0,77	16/0,44	12/0,33
Практические занятия (ПЗ)	12/0,33		12/0,33
Лабораторные работы (ЛР)	28/0,77	16/0,44	12/0,33
Самостоятельная работа (СР):	112/3,11	40/1,11	72/2
Самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, , рубежному контролю	112/3,11	40/1,11	72/2
Формарубежного/промежуточного контроля		зачет	экзамен

4.1 Тематический план дисциплины

Таблица 2

№ раздела дисциплины	Наименование раздела дисциплины	Лекции	Практические занятия	Лабораторные работы
1	Основные понятия и определения в области информационной безопасности программных систем	*		*
2	Комплексный подход к обеспечению информационной безопасности	*		*
3	Защита программ от излучения и разрушающих программных воздействий (программных закладок и вирусов).	*		*
4	Криптографические методы и средства обеспечения информационной безопасности	*		*
5	Защита программных систем от несанкционированного использования и копирования	*		*
6	Обеспечение технологической безопасности программного обеспечения	*		
7	Нормативно правовая система обеспечения информационной безопасности	*		*

4.2 Содержание лекций

Таблица 3

№ раздела дисциплины	Наименование раздела, подраздела, и их содержание	Количество часов	
		очная форма обучения	заочная форма обучения
1	**Основные понятия и определения в области информационной безопасности программных систем** Понятие национальной безопасности Понятие национальной безопасности Основные направления деятельности по обеспечению информационной безопасности в Российской Федерации. Структура государственной системы информационной безопасности. Интересы и угрозы в области национальной безопасности. Проблемы информационной войны. 1.2. Система формирования режима информационной безопасности Основные понятия и задачи информационной безопасности. Понятие и сущность защиты информации. Виды защищаемой информации. Категории доступа. Составляющие информационной безопасности. Зачем и от кого нужно защищать программное обеспечение компьютерных систем. 1.3 . Основные виды угроз и уязвимостей информационных систем Классификация угроз. Модель гипотетического нарушителя 2 информационной безопасности Классификация сетевых атак Классификация уязвимостей программных систем Логическая взаимосвязь уязвимости, атаки и их возможных последствий. Распространённые типы уязвимостей программных систем	**8** 2 2	

	1.4. Основные виды уязвимостей программных систем - Уязвимости «buffer overflow» - Уязвимости «SQL Injection» - Уязвимости «Format string» - Уязвимости «Directory traversal» - Уязвимости «Cross Site Scripting» (XSS) Уязвимости программных реализаций стека TCP/IP и протоколов стека TCP/IP.	2	
2	**14** **Комплексный подход к обеспечению информационной безопасности программных систем** 2.1. Комплексный подход к обеспечению информационной безопасности Организационно-правовое обеспечение процессов разработки и применения программных систем. Инженерно-технические методы и средства защиты информации Программные и программно-аппаратные методы и средства защиты информации. Криптографические методы и средства защиты информации. 2.2. Обеспечение безопасности межсетевого взаимодействия Основы сетевого и межсетевого взаимодействия Сетевая политика безопасности. Шаблоны политики безопасности. Эшелонированная оборона. Аудит информационной безопасности. 2.3. Типовые удаленные атаки и их характеристика Сетевые атаки. Стадии атак Обобщённый сценарий атаки Примеры атак. Классификации удалённых атак Оценивание степени серьёзности атак Возможные последствия информационных атак 2.4. Методы и средства защиты информации от несанкционированного доступа Способынесанкционированного доступа к информации в компьютерных	2 2 2 2	

	системах. - Методы аутентификации пользователей. Понятия "идентификация" и "авторизации". - Защита информации от несанкционированного доступа. - Методы управления доступом к объектам компьютерных систем. 2.5. Технологии межсетевых экранов - Развитие технологий межсетевых экранов - Характеристика межсетевых экранов - Обход межсетевых экранов. - Требования и показатели защищённости межсетевых экранов. - Тестирование межсетевых экранов. 2.6. Системы обнаружения атак и вторжений - История развития систем обнаружения вторжений - Модели систем обнаружения вторжений. - Тестирование систем обнаружения вторжений. - Системы предупреждения вторжений. - Определение и содержание регистрации и аудита информационных систем. 2.7. Обзор существующих средств защиты информации - Средства разграничения доступа пользователей к ресурсам АС. - Средства анализа защищённости программных систем - Средства защиты от спама - Средства контентного анализа.	2 2 2	
3	**Защита программ от излучения и разрушающих программных воздействий (программных закладок и вирусов)** 3.1. Вредоносные программы и защита от них - Вредоносные программы и их классификация Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов - Классификация компьютерных вирусов и их характеристика - Утилиты скрытого администрирования. 3.2. Защита программных систем от разрушающих программных воздействий	**4** 2 2	

	Профилактические меры. Защита от заражения. Внешние проявления Методы обнаружения и удаления компьютерных вирусов. Места обитания. Классификация антивирусных программ Программные закладки и способы защиты от них Факторы, определяющие качество антивирусных программ		
4	**Криптографические методы и средства обеспечения информационной безопасности** 4.1. Средства криптографической защиты информации Основные понятия криптологии. Симметричные криптосистемы Ассиметричные криптосистемы Криптографические хеш-функции. Электронная цифровая подпись и её применение Компьютерная стеганография и её применение. 4.2. Технология виртуальных частных сетей (VPN) Сущность и содержание технологии виртуальных частных сетей. Понятие "туннеля" при передаче данных в сетях. Цифровые сертификаты.	**4** 2 2	
5	**Защита программных систем от несанкционированного использования и копирования** 5.1. Защита программных средств от несанкционированного использования и копирования ринципыпостроениясистемзащитыот копирования. ащита инсталляционных дисков етоды противодействия исследованию алгоритма работы системы защиты	**2**	
6	**Обеспечение технологической безопасности программного обеспечения** 6.1. Обеспечение технологической безопасности программного обеспечения ормальные методы доказательства правильности программ и их спецификаций етоды и средства анализа безопасности	**2**	

	- программного обеспечения Методы обеспечения надежности программ для контроля их технологической безопасности		
7	**Нормативно-правовая система обеспечения информационной безопасности** 7.1. Организационно-правовое обеспечение процессов разработки и применения программного обеспечения. - Обзор российского законодательства в области информационной безопасности. - Стандарты информационной безопасности. - Международные стандарты в области информационной безопасности. - Заключение.	**2**	
Итого		36	

4.3 Практические занятия учебным планом не предусмотрены.

4.4 Лабораторные работы

Таблица 5

№ раздела дисциплины	№ и наименование лабораторной работы	Количество часов ч	
		очная форма обучения	заочная форма обучения
1	№ 1. Защита информации с помощью пароля.	2	
1	№ 2. Исследование средств аудита информационной безопасности и контроль целостности файлов ОС Windows	2	
1	№ 3. Защита файловой системы	2	
2	№ 4. Обеспечение безопасности в Windows. Предотвращение атак шпионов и взломщиков.	2	
2	№ 5. Изучение атаки "анализ сетевого трафика" и способов защиты от неё.	2	
2	№ 6. Обеспечение сетевой безопасности.	2	
2	№ 7. Обеспечение сетевой безопасности. Настройка безопасности для пользователей ОС Windows.	2	
2	№ 8. Изучение особенностей применения систем-ловушек - HONEY	2	

	POT и PADDED CELL		
2	№ 9. Изучение сканера портов и контрмер защиты от сканирования портов.	2	
2	№ 10. Программы для борьбы со спамом.	2	
3	№ 11. Работа с Антивирусом. Изучение признаков присутствия на компьютере вредоносных программ.	2	
4	№ 12. Криптографические средства защиты. Шифры перестановки.	2	
4	№ 13. Криптографические средства защиты. Шифры простой и сложной замены.	2	
4	№ 14. Изучение криптографической системы PGP.	2	
5	№ 15. Изучение хэш-функций.	2	
5	№ 16. Изучение цифровой подписи при помощи программ CryptoARM" и Microsoft Office	2	
5	№ 17. Изучение и настройка средств анализа защищённости (сканеров уязвимостей)	2	
7	№ 18. Изучение нормативно-правовой системы обеспечения информационной безопасности с использованием СПС «КонсультантПлюс».	2	
Итого		36	

5 Примерные темы курсовых проектов (работ)

Курсовой проект учебным планом не предусмотрен.

6 Учебно-методическое обеспечение дисциплин

6.1 Основная, дополнительная и нормативная литература

Основная

1 Шаньгин В.Ф. Информационная безопасность [Электронный ресурс] / В. Ф. Шаньгин. - М. : ДМК Пресс, 2014. - 702 с. - (ЭБС "Издательство Лань"). - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=50578

2 Бирюков А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А. А. Бирюков. - М. : ДМК Пресс, 2013. - 474 с. - (ЭБС "Издательство Лань"). - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990

3 Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.

Дополнительная 3 Хорев П.Б. Программно-аппаратная защита информации [Электронный ресурс]: учеб. пособие

/ П. Б. Хорев. - М. : Форум, 2009. - 352 с. - (ЭБС "znanium.com"). - Режим доступа: http://znanium.com/catalog.php?item=booksearch&code=%D0%A5%D0%BE%D1%80%D0%B5%D0%B2%20%D0%9F.%D0%91 .#none

4 Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. - 544 с.

5 Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с.

6 Технические средства и методы защиты информации [Текст] : Учеб. пособие для вузов 090102. 090105, 090106 / Зайцев А.П. и др.; Под ред. А.П. Зайцева; А.А. Шелупанова. - М.: Горячая линия - Телеком, 2009 (91035). - 615 с. : ил. - Библиогр.: с. 608-609

Нормативная

7 Конституция Российской Федерации. 12 декабря 1991 г.

8 Доктрина информационной безопасности Российской Федерации. утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895

9 Уголовный кодекс Российской Федерации от 24.05.96 // Собрание законодательства российской Федерации. 1996. № 25. Ст. 155.

10 Гражданский кодекс Российской Федерации от 22.12.95 // Собрание законодательства Российской Федерации. 1996. № 5. Ст. 410.

11 Закон Российской Федерации "О безопасности" от 05.03.92 // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 15. Ст. 769.

12 Закон Российской Федерации "О государственной тайне" от 21.07.93 // Журнал официальной информации: Кадастр. 1993. № 35. С. 3-41.

13 Закон Российской Федерации "Об оперативно-розыскной деятельности" от 03.07.95 Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

14 Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 13 июля 2015 года)

15 Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (с изменениями и дополнениями).

6.2 Средства обеспечения усвоения дисциплины

6.2.1 Учебно-методическая документация по дисциплине

Перечень учебно-методической документации по дисциплине

1. **Информационная безопасность программных систем:** методические указания по изучению дисциплины для студентов очной формы обучения направления подготовки 09.03.4 - «Программная инженерия» / Сост.: С.Ю. Фёдоров; Кубан. гос. технол. ун-т. Каф. компьютерных технологий и информационной безопасности. - Краснодар, 2015. -30 с. Режим доступа http://moodle.kubstu.ru
2. **Информационная безопасность программных систем:** методические указания по выполнению лабораторных работ для студентов очной формы обучения направления подготовки 09.03.04 - «Программная инженерия» / Сост.: С.Ю. Фёдоров; Кубан. гос. технол. ун-т. Каф. компьютерных технологий и информационной безопасности. - Краснодар, 2015. - 273 с. Режим доступа http://moodle.kubstu.ru
3. **Информационная безопасность программных систем:** методические указания по проведению занятий в активных и интерактивных формах для студентов очной формы обучения направления подготовки 09.03.04 - «Программная инженерия» / Сост.: С.Ю. Фёдоров; Кубан. гос. технол. ун-т. Каф. компьютерных технологий и информационной безопасности. - Краснодар, 2015. - 25 с.

Режим доступа http://moodle.kubstu.ru

4. **Информационная безопасность программных систем:** методические указания по самостоятельной работе для студентов очной формы обучения направления подготовки 09.03.04 - «Программная инженерия» / Сост.: С.Ю. Фёдоров; Кубан. гос. технол. ун-т. Каф. компьютерных технологий и информационной безопасности. - Краснодар, 2015. - 23 с. Режим доступа http://moodle.kubstu.ru

6.2.2 Перечень программного обеспечения

- Операционные системы - Linux; МСВС 3.0; MS Windows 7/8, 2008 Server.
- Офисные программы Microsoft Office;
- Антивирусные комплексы AVP Касперского;
- Архиваторы WINRAR и WINZIP;
- Сканеры уязвимостей Nmap, Znmap, XSpider;
- Межсетевые экраны Outpost, ZoneAlarm, Comodo и др.;
- Анализаторы сетевого трафика Wiershark, Iris, Windump;
- Средства мониторинга сетевой безопасности ОС Windows;
- Средства мониторинга и оптимизации ОС Windows.
- Программы для мониторинга и анализа сетей Netstat, Lanstate.
- Программы обнаружения беспроводной сети Kismet, Netstambler.
- Системы обнаружения вторжений Snort.
- Программы восстановления и резервирования данных.
- Средства определения производительности.
- Пакет программ VirtualBox.

Интернет-ресурсы:

- http://www.moodle.kubstu.ru

7 Материально-техническое обеспечение дисциплины

1. Компьютерные классы (К9-305, К9-205, К9-215, К9-403).
2. Комплект мультимедийной проекционной аппаратуры для проектирования мультимедийных слайдов на лекциях и лабораторных работах.

8 Оценочные средства по дисциплине

Оценочные средства включены в ПМК дисциплины.