МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института энергетики,
информационных технологий и
управляющих систем
_______ Белоусов А.В.
«_____» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Средства защиты от разрушающих программных компонентов

специальность:
10.05.03 Информационная безопасность автоматизированных систем

специализация:
10.05.03-07 Обеспечение информационной безопасности распределённых информационных систем

Квалификация
Специалист по защите информации

Форма обучения
очная

Срок обучения
5 лет

Институт энергетики, информационных технологий и управляющих систем
Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Белгород – 2017

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утверждённого приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1509
- плана учебного процесса БГТУ им. В. Г. Шухова по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация 10.05.03-07 «Обеспечение информационной безопасности распределённых информационных систем», введённого в действие в 2017 году

Составитель: (М.В. Панченко)

Рабочая программа согласована с выпускающей кафедрой
Программного обеспечения вычислительной техники и автоматизированных систем

Заведующий кафедрой: к.т.н., доцент (В.М. Поляков)
(подпись) (инициалы, фамилия)

« ___ » _____ 2017 г.

Рабочая программа обсуждена на заседании кафедры
Программного обеспечения вычислительной техники и автоматизированных систем

« ___ » _____ 2017 г., протокол № _____

Заведующий кафедрой: к.т.н., доцент (В.М. Поляков)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа одобрена методической комиссией института энергетики, информационных технологий и управляющих систем

« ___ » _____ 2017 г., протокол № _____

Председатель: к.т.н., доцент (А.Н. Семернин)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции			Требования к результатам обучения
№	Код компетенции	Компетенция	
Общепрофессиональные			
1	ОПК-8	Способность к освоению новых образцов программных, технических средств и информационных технологий	В результате освоения дисциплины обучающийся должен **Знать:**состав и структуру существующих программных систем для обеспечения защиты от разрушающих программных компонентов. **Уметь:**применять типовое программное обеспечение для обеспечения защиты от разрушающих программных компонентов. **Владеть:**современными, а также перспективными информационными технологиями в сфере проектирования и разработки программных средств для защиты от разрушающих программных компонентов.
Профессиональные			
1	ПК-3	Способность проводить анализ защищенности автоматизированных систем	В результате освоения дисциплины обучающийся должен **Знать:**основные угрозы защищенности автоматизированных систем, виды разрушающих программных воздействий. **Уметь:**анализировать средства защиты автоматизированных систем от разрушающих программных воздействий. **Владеть:**методами анализа защищенности автоматизированных систем.
2	ПК-9	Способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	В результате освоения дисциплины обучающийся должен **Знать:**особенности разработки и ресурсоемкость средств защиты от разрушающих программных компонентов. **Уметь:**проводить анализ и сравнение различныых средств защиты при разработке защищенных автоматизированных систем. **Владеть:**навыками презентации особенностей, достоинств и недостатков различных средств защиты от РПК при разработке защищенных автоматизированных систем.
3	ПК-13	Способность участвовать в проектировании средств защиты информации автоматизированной системы	В результате освоения дисциплины обучающийся должен **Знать:**принципы построения систем защиты информации автоматизированной системы, в том числе и перспективные. **Уметь:**проектировать средства защиты автоматизированных систем с использованием стохастических моделей и методов. **Владеть:**математическим и криптографическим аппаратом для проектирования средств защиты

			автоматизированных систем от разрушающих программных компонентов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Основы информационной безопасности
2	Криптографические методы защиты информации
3	Безопасность локальных сетей
4	Безопасность операционных систем

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Программно-аппаратные средства обеспечения информационной безопасности
2	Моделирование угроз информационной безопасности
3	Разработка и эксплуатация защищенных автоматизированных систем

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.

Вид учебной работы	Всего часов	Семестр № 7
Общая трудоемкость дисциплины, час	180	180
Контактная работа (аудиторные занятия), в т.ч.:	72	72
лекции	36	36
лабораторные	36	36
практические	-	-
Самостоятельная работа студентов, в том числе:	108	108
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	9	9
Другие виды самостоятельной работы	63	63
Форма промежуточная аттестация (зачет, экзамен)	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1 Наименование тем, их содержание и объем
Курс 4 Семестр 7

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1.	**Стохастическая компьютерная вирусология**				
1.1	Разрушающие программные воздействия (РПВ). Классификации. История появления	4		4	6
1.2	Структура комплекса программных средств антивирусной защиты	2		4	6
1.3	Критерии эффективности программных средств антивирусной защиты	1		2	4
1.4	Недостатки существующих средств защиты от РПВ	1		2	4
1.5	Перспективные методы защиты от РПВ	1		2	6
1.6	Стохастические методы, использующиеся в атаках на компьютерные системы	2			6
2.	**Стохастические разрушающие программные воздействия**				
2.1	Простой и улучшенный криптотроян	1			4
2.2	Анонимная кража информации. Криптосчетчик	2		2	4
2.3	Конфиденциальное получение информации	2		6	6
2.4	Недоказуемое и отрицаемое шифрование	1			4
2.5	Загрузчик РПВ	1			4
3.	**Симбиотические и распределенные разрушающие программные воздействия**				
3.1	Информационный шантаж	2		3	6
3.2	Распределенные вычисления. Безопасный выкуп	2		3	4
4.	**Скрытые каналы передачи данных**				
4.1	История исследования скрытых каналов, современный взгляд на скрытые каналы	2			4
4.2	Характеристики скрытых каналов. Потайные и побочные скрытые каналы	1		2	4
4.3	Скрытые каналы в системах обработки информации	1		2	8
4.4	Методы организации локальных скрытых каналов	2			6
4.5	Методы организации сетевых скрытых каналов	4		4	6

5.	**Перспективные методы противодействия вредоносным программам**				
5.1	Иммунологический подход к антивирусной защите	2			8
5.2	Архитектура компьютерной иммунной системы	1			4
5.3	Автономность надежной системы защиты	1			4
	ВСЕГО	36		36	108

4.2. Содержание практических (семинарских) занятий

Учебным планом не предусмотрены.

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов
семестр № 7			
1	1.1 - 1.2	Средства защиты компьютера от вирусов. Работа с антивирусными пакетами	4
2	1.1 - 1.4	Внешняя защита от разрушающих программных воздействий. Работа с программой XSpider	4
3	1.2 - 1.5	Разработка сигнатурного анализатора файлов с использованием различных хеш-функций	6
4	2.2 - 2.3	Изучение протокола конфиденциального получения информации (private information retrieval) и его модификаций	8
5	3.1 - 3.2	Моделирование поведения вредоносного программного обеспечения типа «Кейлогер»	6
6	4.1 - 4.5	Анализ трафика протоколов транспортного и сетевого уровней в целях выявления скрытых каналов передачи информации	8
		ИТОГО:	36

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1. Перечень контрольных вопросов (типовых заданий)

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Стохастическая компьютерная вирусология	Определение РПВ. Методы защиты от РПВ. Модель системы защиты от РПВ. Классификация вредоносных программ по методике заражения.

		Классификация вредоносных программ по наносимому ущербу. Основные разновидности вредоносных программ. Виды РПВ. Функции РПВ. Структура программного комплекса программных средств антивирусной защиты Критерии эффективности программных средств антивирусной защиты Недостатки существующих средств защиты от РПВ Перспективные методы защиты от РПВ
2	Стохастические разрушающие программные воздействия	Стохастические РПВ. Классификации полиморфных вирусов. Простой и улучшенный криптотроян. Анонимная кража информации. Криптосчетчик. Недоказуемое шифрование. Отрицаемое шифрование. Загрузчик РПВ.
3	Симбиотические и распределенные разрушающие программные воздействия	Безопасный выкуп. Информационный шантаж. Компьютерные вирусы, использующие стохастические методы для выполнения деструктивных функций (Сверхживучие вирусы. Криптографическая DoS-атака) Компьютерные вирусы, использующие стохастические методы для выполнения деструктивных функций (Вымогательство информации. Вирус, использующий разделение секрета. Кража информации).
4	Скрытые каналы передачи данных	Скрытые каналы передачи информации. История исследований. Характеристики скрытых каналов. Классификация скрытых каналов. Потайные и побочные каналы. Скрытые каналы в системах обработки информации. Методы организации локальных скрытых каналов. Методы организации сетевых скрытых каналов. Скрытые каналы на основе протоколовTCP/IP. IP протокол. Скрытые каналы на основе протоколовTCP/IP. ICMP протокол. Скрытые каналы на основе протоколовTCP/IP. TCP протокол. Скрытые каналы в протоколах уровня приложений.
5	Перспективные методы противодействия вредоносным программам	Понятие иммунной системы. Свойства иммунной системы. Архитектура компьютерной иммунной системы. В чем заключается автономность иммунной системы.

5.2. Перечень тем курсовых проектов, курсовых работ, их краткое содержание и объем.

Учебным планом не предусмотрены.

5.3. Перечень индивидуальных домашних заданий, расчетно-графических заданий.

Учебным планом предусмотрено одно индивидуальное задание (ИДЗ).

Примерные темы для выполнения ИДЗ:

1. Протокол «Покер по телефону».
2. Анализ и реализация схем разделения секрета.
3. Анализ и реализация протоколов безопасного обмена ключами.
4. Анализ и реализация протоколов электронного голосования.
5. Скрытые каналы в протоколах уровня приложений.
6. Защита программ от изучения. Методы обфускации кода.
7. WinAPI Splicing.
8. Стеганография в видео-файлах.
9. Стеганография в аудио-файлах.
10. Анализ и реализация хеш-функций.
11. Практическое применение протокола конфиденциального получения информации (PIR) и его модификаций.

Изучение библиотеки peercy, реализации протокола конфиденциального получения информации (PIR).Цель задания: развить и закрепить у обучающегося практические навыки организации всех этапов решения прикладных задач с использованием криптографических, математических и методов защиты от разрушающих программных воздействий.

На выполнение индивидуального домашнего задания предусмотрено 9 часов самостоятельной работы студента.

5.4. Перечень контрольных работ.

В качестве рубежного контроля по итогам изучения разделов 1-3 предусмотрена контрольная работа, представленная в виде тестов.

Пример тестовых вопросов:

1. Что из перечисленного не присуще для программ категории SpyWare:
   - Маскировка своего присутствия на компьютере
   - Заражение других приложений
   - Противодействие удалению
   - Замедление работы компьютера
   - Расход интернет траффика
   - Рассылка своих копий на другие компьютеры

2. Лечение вируса сводится
   - К удалению машинного кода вируса из тела программы
   - К поиску и удалению зараженного файла
   - К помещению зараженного файла в «карантин»

3. Выберите неверные утверждения

- Вредоносные программные воздействия можно отнести к одной конкретной категории
- Почтовый червь может выполнять функции троянской программы
- Троянская программа может быть внедрена в систему по вирусному принципу
- Лечение троянской программы сводится к удалению ее файлов
- Программы категории Adware могут заражать другие приложения

4. Классификация программ по наносимому ущербу, какая категория в ней отсутствует
   - Безопасные программы
   - Программы уничтожающие и повреждающие данные
   - Программы, собирающие и передающие третьим лицам конфиденциальную информацию
   - Программы, нейтрализующие или повреждающие специализированное ПО, применяемое для защиты компьютера
   - Все вышеперечисленные категории присутствуют

5. Какие вредоносные программы можно отнести к категории SpyWare\AdWare?
   - Trojan
   - Hijacker
   - BHO
   - Hoax
   - Trojan-Downloader
   - Backdoor

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 с.— Режим доступа: http://www.iprbookshop.ru/7943.— ЭБС «IPRbooks», по паролю;
2. Проскурин, В. Г. Защита программ и данных : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 090900 "Информац. безопасность" (бакалавр) и специальностям 090301 "Компьютер. безопасность", 090303 "Информац. безопасность автоматизир. систем" / В. Г. Проскурин. - 2-е изд., стер. - Москва : Академия, 2012. - 198 с.
3. Гошко С.В. Технологии борьбы с компьютерными вирусами [Электронный ресурс]: учебное пособие/ Гошко С.В.— Электрон. текстовые данные.— М.: СОЛОН-ПРЕСС, 2009.— 351 с.— Режим доступа: http://www.iprbookshop.ru/8721.— ЭБС «IPRbooks», по паролю.
4. Лапонина, О. Р. Основы сетевой безопасности : криптографические алгоритмы и протоколы взаимодействия : учеб. пособие / О. Р. Лапонина. - 2-е изд., испр. . - М. : Интернет-Университет Информационных Технологий ; М. : БИНОМ. Лаборатория знаний, 2007. - 531 с. -

(Основы информационных технологий). - ISBN 978-5-9556-0102-1. - ISBN 978-5-94774-650-1

6.2. Перечень дополнительной литературы

1. Разрушающие программные воздействия: Учебно-методическое пособие / А.Б. Вавренюк, Н.П. Васильев, Е.В. Вельмякина, Д.В. Гуров, М.А., Иванов, И.В. Матвейчиков, Н.А. Мацук, Д.М. Михайлов, Л.И. Шустова; под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2011. — 328 с.
2. Стохастические методы и средства защиты информации в компьютерных системах и сетях / М. А. Иванов [и др.]; ред. И. Ю. Жуков. – М. : [б. и.], 2009. – 510 с.
3. Таненбаум, Э. Компьютерные сети. - СПб: Питер, 2009. - 992с.
4. Гультяева, Т.А. Основы теории информациии криптографии: конспект лекций [Электронный ресурс] / Т.А. Гультяева. - Новосибирск: НГТУ, 2010. - 88с.
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год. http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god
6. Родичев, Ю. А. Информационная безопасность : нормативно-правовые аспекты : учеб. пособие / Ю. А. Родичев. - СПб. : ПИТЕР, 2008. - 271 с. - (Учебное пособие). - ISBN 978-5-388-00069-9

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Компьютерный класс с интерактивной доской и проектором. Персональные компьютеры под управлением ОС Windows. Среда разработки MS Visual Studio. Бесплатно-распространяемое программное обеспечение для анализа сетевого траффика WireShark. 25% от объема аудиторных занятий проходят в интерактивной форме. В частности, предусмотрены следующие методы и формы обучения: интерактивные лекции, групповые задания, а также закрепление нового материала при помощи метода «каждый учит каждого».

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

8.1. Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 20 /20 учебный год.

Протокол № _____ заседания кафедры от «___»_____ 20 г.

Заведующий кафедрой_____

подпись, ФИО

Директор института _____

подпись, ФИО

(или)

8.2. Утверждение рабочей программы с изменениями, дополнениями

Рабочая программа с изменениями, дополнениями утверждена на 20 /20 учебный год.

Протокол № _____ заседания кафедры от «___»_____ 20 г.

Заведующий кафедрой_____

подпись, ФИО

Директор института _____

подпись, ФИО