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 (модуля)

Моделирование угроз информационной безопасности

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

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	
Профессиональные			
	ПК-3	Способность проводить анализ защищенности автоматизированных систем	В результате освоения дисциплины обучающийся должен **Знать:** источники и классификацию угроз информационной безопасности. **Уметь:** анализировать и оценивать угрозы информационной безопасности объекта. **Владеть:** методами выявления угроз информационной безопасности автоматизированных систем.
1	ПК-4	Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	В результате освоения дисциплины обучающийся должен **Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах. **Уметь:** строить и анализировать модели угроз и модели нарушителей в автоматизированных системах. **Владеть:** методологией анализа автоматизированных систем на наличие уязвимостей.
2	ПСК-7.1	Способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	В результате освоения дисциплины обучающийся должен **Знать:** основные принципы функционирования распределенных информационных систем и подходы для анализа их защищенности. **Уметь:** проводить инструментальный мониторинг информационно-технологических ресурсов на наличие уязвимостей. **Владеть:** инструментарием для моделирования угроз информации в распределенных информационных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Сети и системы передачи информации
2	Средства защиты от разрушающих программных компонентов

4	Безопасность сетей ЭВМ

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Информационная безопасность распределенных информационных систем
2	Технология построения защищенных распределенных приложений

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единицы, 144 часа.

Вид учебной работы	Всего часов	Семестр № 8
Общая трудоемкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т.ч.:	54	54
лекции	36	36
лабораторные	18	18
практические		
Самостоятельная работа студентов, в том числе:	90	90
Курсовой проект		
Курсовая работа		
Расчетно-графическое задания		
Индивидуальное домашнее задание		
Другие виды самостоятельной работы	54	54
Форма промежуточная аттестация (зачет, экзамен)	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем

Курс 4 Семестр 8

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1.	**Угрозы безопасности информации в информационной системе**				

1.1	Модель угроз информационной безопасности в информационных системах	2			3
1.2	Модель нарушителя информационной безопасности	1			3
1.3	Актуальные угрозы информации в информационных системах	1			3
2.	**Тестирование безопасности информационных систем**				
2.1	Сбор информации о тестируемой системе	6		2	10
2.2	Тестирование конфигурации и бизнес-логики	6		2	10
2.3	Тестирование политики пользовательской безопасности	2		1	6
2.4	Тестирование аутентификации/авторизации	2		2	6
2.5	Тестирование механизмов управления сессиями	2		2	6
2.6	Тестирование уязвимостей на стороне пользователя	2		1	6
3.	**Моделирование атак на веб-приложения**				
3.1	Sql-инъекции (SQL-injection). Описание, методы выявления, рекомендации по предупреждению	4		2	10
3.2	Межсайтовый скриптинг (XSS). Классификация, способы обнаружения, механизмы проведения.	4		2	10
3.3	Межсайтовая подделка запросов (CSRF). Особенности реализации. Методы защиты.	4		2	10
3.4	Удаленное внедрение кода (RCE). Методы удаленного внедрения кода в веб-приложения			2	7
	ВСЕГО	36		18	90

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 № 8			
1	2.1–2.2	Сбор информации о веб-приложении	2
2	2.2–2.3	Анализ защищенности транспортного уровня	2
3	2.4	Изучение защищенности механизма управления доступом	3
4	2.5	Тестирование защищенности механизма управления сессиями	3
5	3.1	Моделирование атак типа SQL-injection	2
6	3.2	Моделирование XSS атак	2
7	3.3	Поиск уязвимостей к атакам CSRF	2
8	3.4	Анализ уязвимостей к атакам RCE	2
		ИТОГО:	18

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	Угрозы безопасности информации в информационной системе	Процесс определения угроз ИБ в информационной системе. Оценка возможностей нарушителей по реализации угроз безопасности информации. Оценка вероятности реализации угрозы безопасности информации. Оценка степени возможного ущерба от реализации угрозы безопасности информации.
2	Тестирование безопасности информационных систем	Тестирование на проникновение. Методология. Тестирование сетевого уровня и уровня приложений. Методы аудита при проведении пентеста. Сбор информации о веб-приложении. Определение веб-сервера и фреймворка веб-приложения. Определение веб-приложений на сервере. Поиск информации в мета-файлах и на веб-сервере. Определение точек входа. Тестирование конфигурации и инфраструктуры веб-приложения. Логирование. Рекомендации по ведению. Использование логов в пентесте. Угрозы от старых версий веб-приложения, скрытых файлов и резервных копий. Небезопасное использование методов протокола http. Механизм HSTS.
3	Моделирование атак на веб-приложения	SQL-инъекции. Виды, примеры. SQL-инъекции методы и способы защиты. XSS атаки. Хранимые. Последствия проведения. XSS атаки. Отраженные. Последствия проведения. XSS атаки. DOM-модели. Последствия проведения. Методы защиты от XSS. Кодирование. Методы защиты от XSS. Валидация. CSRF-атака. Описание. Разновидности. CSRF-атака. Методы защиты.

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 не предусмотрены.

5.4. Перечень контрольных работ.

Учебным планом не предусмотрены.

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Дэвид М. Ахмад. Защита от хакеров корпоративных сетей 2008 / Дэвид М. Ахмад, Идо Дубравский, Хал Флинн, Джозеф «Кингпин», ДМК Пресс. Режим доступа: http://www.iprbookshop.ru/6923.html.— ЭБС «IPRbooks», по паролю
2. Макнамара, Дж. Секреты компьютерного шпионажа : тактика и контрмеры / Дж. Макнамара ; пер. с англ. А. В. Бутко ; ред. С. М. Молявко. – М. : БИНОМ. Лаборатория знаний, 2006. – 536 с.
3. Максим Мерритт. Безопасность беспроводных сетей / Максим Мерритт, Дэвид Поллино— Электрон. текстовые данные.— М.: ДМК Пресс, 2008.— 288 с. Режим доступа: http://www.iprbookshop.ru/7852.html.— ЭБС «IPRbooks», по паролю
4. Кристиан Барнс Защита от хакеров беспроводных сетей [Электронный ресурс]/ Кристиан Барнс— Электрон. текстовые данные.— М.: ДМК Пресс, 2008.— 480 с.— Режим доступа: http://www.iprbookshop.ru/7768.html.— ЭБС «IPRbooks», по паролю
5. Митник, К. Искусство вторжения : пер. с англ. / К. Митник. - Москва : Академия АйТи, 2005. - 279 с.
6. Глушаков, С. В. Секреты хакера: защита и атака / С. В. Глушаков, М. И. Бабенко, Н. С. Тесленко. - 2-е изд., доп. и перераб. - Москва : АСТ : Хранитель, 2008. - 536 с.
7. Атака из Internet / И. Д. Медведовский [и др.]. - Москва : СОЛОН-Р, 2002. - 356 с.

6.2. Перечень дополнительной литературы

1. М.А. Иванова. 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. Левин, М. Введение в хакинг / М. Левин. – М. : Новый издательский дом, 2005. – 173 с.
3. Левин, М. Как стать хакером : интеллектуал. рук. по хакингу и фрикингу / М. Левин. – 3-е изд., доп. и испр. – М. : Новый издательский дом, 2005. – 319 с.

4. Мауфер, Т. WLAN: практическое руководство для администраторов и профессиональных пользователей / Т. Мауфер. – М. : КУДИЦ-ОБРАЗ, 2005. – 365 с.

6.3 Перечень интернет ресурсов

1. http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Наименование специальных помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программмного обеспечения. Реквизиты подтверждающего документа**
Лекционная аудитория. Аудитория для проведения лабораторных и практических занятий: Лаборатория безопасности сетей ЭВМ: ГК 426	Поточная аудитория с доской. Компьютерный класс – Рабочие места учащихся – Коммутатор третьего уровня CiscoCatalyst 3560 WS-C3560V2-24TS-S – 1 шт; – Управляемый коммутатор второго уровня CiscoCatalyst 2960 WS-C2960-8TC-S – 1 шт; – Неуправляемый коммутатор Cisco SF 100D-05 – 1 шт; – Маршрутизатор Cisco RV120W – 2 шт; – Брандмауэр Cisco ASA 5505 – 2 шт. (предназначены для построения сетей, применения технологии VLAN, настройки подсетей и маршрутизаторов, изучения работы межсетевых экранов) – Учебный комплекс СОТСБИ-guard в составе 3 KVM серверов, содержа-щих: • Редактор учебных курсов, • ПО для РМ преподавателя и ученика; • NFS сервер; • Почтовый, DNS и RADIUS серверы; • Web сервер, Kerberos сервер, сканер безопасности, гейткипер H.323;	Открытая система обнаружения вторжений SuricataOpenSource IDS / IPS / NSM engine КОМПЛЕКС ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СОТСБИ: - Программное обеспечение (ПО) сервера для обеспечения процесса обучения СОТСБИ-У; - ПО для рабочего места преподавателя СОТСБИ – guard; - ПО для рабочего места учащегося СОТСБИ – guard; - ПО для проведения лабораторных работ для изучения информационно-компьютерной безопасности СОТСБИ – guard; - ПО для проведения практических работ по изучению семиуровневой эталонной модели взаимодействия открытых систем OSI; - Интерактивный учебный курс СОТСБИ-У «Информационно-компьютерная безопасность» - Интерактивный учебный курс СОТСБИ-У «Изучение модели OSI» - ПО рабочего места учащегося; - ПО рабочего места преподавателя.

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программмного обеспечения. Реквизиты подтверждающего документа
	• Firewall Zyxel USG60 – 5 шт. (предназначен для изучения технологии виртуальных сетей, моделирования сетевых атак и изучения средств защиты от них).	

8. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ).

Курс «Моделирование угроз информационной безопасности» является дисциплиной вариативной части блока профессиональных дисциплин в подготовке студентов по специальности 090303 – Информационная безопасность автоматизированных систем.

Целью преподавания дисциплины является подготовка студентов для решения задач моделирования угроз информационной безопасности и противостояния им.

Для успешного освоения дисциплины студенты должны изучить (повторить) содержание таких курсов как «Сети и системы передачи информации», «Средства защиты от разрушающих программных компонентов» и «Безопасность сетей ЭВМ».

Аудиторные занятия проводятся в виде лекций, лабораторных и практических работ. Важное значение для изучения курса имеет самостоятельная работа студентов.

Курс состоит из нескольких крупных разделов.

Вводный раздел – понятие угрозы информационной безопасности. При изучении этого раздела следует акцентировать внимание студентов на изучении способов и подходов в моделировании угроз информационной безопасности.

Первый раздел курса посвящён изучению технологии безопасного программирования. Здесь следует подробнее остановиться на видах угроз для компилируемых языков программирования и методах противодействия данным угрозам.

Второй раздел предназначен для изучения угроз, реализуемых различными скриптами.

В **третьем разделе** рассматриваются типовые угрозы безопасности РВС. Необходимо подробно рассмотреть модели механизмов реализации типовых угроз безопасности. Привести примеры реализации нескольких (на выбор) типовых угроз РВС.

Четвёртый раздел – угрозы криптографии. Здесь следует заострить внимание на примерах реализации атак на общепринятые и часто используемые криптографические протоколы.

Наконец, **пятый раздел** посвящен изучению методов для выявления уязвимостей.

Итоговый контроль осуществляется в форме экзамена.

Самостоятельная работа является главным условием успешного освоения изучаемой учебной дисциплины и формирования высокого профессионализма будущих специалистов по обеспечению информационной безопасности.

Исходный этап изучения курса «Моделирование угроз информационной безопасности» предполагает ознакомление с Рабочей программой, характеризующей границы и содержание учебного материала, который подлежит освоению.

Изучение отдельных тем курса необходимо осуществлять в соответствии с поставленными в них целями, их значимостью, основываясь на содержании и вопросах, поставленных в лекции преподавателя и приведенных в планах и заданиях к лабораторным работам.

В книгах, представленных в списке рекомендуемой литературы, содержатся возможные ответы на поставленные вопросы. Инструментами освоения учебного материала являются основные термины и понятия, составляющие категориальный аппарат дисциплины. Их осмысление, запоминание и практическое использование являются обязательным условием овладения курсом.

Успешное освоение курса дисциплины возможно лишь при систематической работе, требующей глубокого осмысления и повторения пройденного материала, поэтому необходимо делать соответствующие записи по каждой теме.

9. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

9.1. Утверждение рабочей программы без изменений

Рабочая программа и ГРС без изменений утверждена на 20__ /20__ учебный год.
Протокол № _____ заседания кафедры от «___»_____ 20 г.

Заведующий кафедрой_____
(подпись, ФИО)

Директор института _____
(подпись, ФИО)

(или)

9.2. Утверждение рабочей программы и ГРС с изменениями, дополнениями
Рабочая программа и ГРС с изменениями, дополнениями утверждена на 20 /20 учебный год.

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

Заведующий кафедрой_____
(подпись, ФИО)

Директор института _____
(подпись, ФИО)