МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В. Г. ШУХОВА»
(БГТУ им. В. Г. Шухова)
Кафедра программного обеспечения вычислительной техники и автоматизированных систем

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

РАБОЧАЯ ПРОГРАММА

дисциплины

Программно-аппаратные средства обеспечения 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

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: к.т.н. (И.П. Бойчук)
(ученая степень и звание, подпись) (инициалы, фамилия)

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 (ПРАКТИКЕ)

Формируемые компетенции			Требования к результатам обучения
№	Код компетенции	Компетенция	
Профессиональные			
1.	ПК-10	способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	В результате освоения дисциплины обучающийся должен **Знать:** Принципы и основные алгоритмы работы программно-аппаратных компонентов защищенных автоматизированных систем **Уметь:** Составлять технические задания на проектирование программно-аппаратных средств защиты информации в составе автоматизированных систем **Владеть:** Практическими навыками разработки и тестирования наиболее распространенных программно-аппаратных компонентов защищенных автоматизированных систем
2.	ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы	В результате освоения дисциплины обучающийся должен **Знать:** Принципы проектирования программно-аппаратных средств защиты информации **Уметь:** Разрабатывать предложения и участвовать в работе рабочих групп по проектированию программно-аппаратных средств защиты информации **Владеть:** Проектным мышлением и навыками проектного подхода к программно-аппаратной части системы защиты информации
3.	ПК-14	способностью проводить контрольные проверки работоспособности	В результате освоения дисциплины обучающийся должен **Знать:** Методики проведения контрольных проверок и требования других управляющих документов

		применяемых программно-аппаратных, криптографических и технических средств защиты информации	в сфере контроля работы программно-аппаратных средств защиты информации **Уметь:** Составлять регламенты и расписания контрольных проверок программно-аппаратных средств защиты информации в организации **Владеть:** Практическими навыками проведения контроля функционирования программно-аппаратных средств защиты информации
4.	ПК-24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	В результате освоения дисциплины обучающийся должен **Знать:** Правила инвентаризации и способы организации использования программно-аппаратных средств защиты информации на предприятии **Уметь:** Разрабатывать и внедрять правила использования информационно-технологических ресурсов автоматизированной системы предприятия с учетом имеющихся программно-аппаратных средств защиты информации для целей соблюдения требований информационной безопасности **Владеть:** Навыками работы с программно-аппаратными средствами защиты информации в применении к различным информационно-технологическим ресурсам автоматизированной системы
5.	ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности	В результате освоения дисциплины обучающийся должен **Знать:** Способы применения программно-аппаратных средств защиты информации при создании частных политик ИБ **Уметь:** Самостоятельно разрабатывать частные политики ИБ с учетом имеющихся программно-аппаратных средств защиты информации **Владеть:** Навыками проведения мониторинга и аудита

		автоматизированной системы	безопасности автоматизированной системы с применением программно-аппаратных средств

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Информатика
2	Языки программирования
3	Основы информационной безопасности
4	Криптографические методы защитыинформации
5	Безопасность операционных систем
6	Средства защиты от разрушающих программных компонентов

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Технология построения защищенных распределенных приложений

3. ОБЪЁМ ДИСЦИПЛИНЫ

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

Вид учебной работы	Всего часов	Семестр №8
Общая трудоёмкость 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	45	45
Курсовая работа	–	–
Расчетно-графическое задание	–	–
Индивидуальное домашнее задание	–	–
Другие виды самостоятельной работы	63	63
Форма промежуточной аттестации - экзамен	ЗО	ЗО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1.Наименование тем, их содержание и объем

Курс4 Семестр №8

№ п/п	Наименование раздела (модуля)	К-во лекционных часов	Объем на тематический раздел, час		
			Практические и др. занятия	Лабораторные занятия	Самостоятельная работа
1	2	3	4	5	6
1	Вводный раздел. Стандарты информационной безопасности. Назначение и функции программно аппаратных средств обеспечения информационной безопасности. Функции программно аппаратных средств защиты информации.	6		2	8
2	Программные закладки. Модели воздействий программных закладок на вычислительные системы. Обнаружение программных закладок. Методы защиты от программных закладок. Вредоносное ПО. Классификация вредоносного ПО. Технологии вредоносных программ и принципы их работы. UserModeRootkit. KernelModeRootkit.	6		8	20
3	Политика информационной безопасности. Структура политики безопасности организации. Базовая и специализированные политики безопасности. Процедуры безопасности. Разработка политики безопасности организации. Компоненты архитектуры безопасности. Роли и ответственности.	4		4	15
4	Модели безопасности компьютерных систем.Виды политик управления доступом и информационными потоками. Модели компьютерных систем с дискреционным, мандатным, ролевым управлением доступом. Модели изолированной программной среды.	6		2	15
5	Технологии идентификации, аутентификации и авторизации. Аутентификация, авторизация и администрирование действий	4		8	15

	пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Программно-аппаратные системы идентификации и аутентификации.				
6	Программно-аппаратные комплексы защиты информации. Программно-аппаратный комплекс «Аккорд». Построение системы защиты информации на основе комплекса. Состав комплекса. Принцип работы комплекса. Программно-аппаратный комплекс «SecretNet».Функциональные возможности системы. Общая архитектура. Основные компоненты. Защитные механизмы SecretNet. Механизмы контроля входа в систему. Механизм идентификации и аутентификации пользователей. Аппаратные средства защиты от несанкционированного входа. Механизмы управления доступом и защиты ресурсов. Механизм замкнутой программной среды. Механизмы контроля и регистрации. Средства аппаратной поддержки SecretNet.	10		12	35
	ВСЕГО	36		36	108

4.2.Перечень практических (семинарских) занятий. Их содержание и объем в часах (аудиторных).

Учебным планом не предусмотрено.

4.3.Перечень лабораторных занятий и объем в часах

Курс 4 Семестр №8

№ п/п	№ раздела дисциплины (в соответствии с п.5.1)	Наименование лабораторной работы	К-во часов
1	1 - 2	Аппаратные решения для выявления и предотвращения утечек конфиденциальной информации	4

2	2	Симметричное и ассиметричное шифрование данных средствами криптографического пакета OpenSSL	4
3	2	Создание криптографических сообщений с использованием интерфейса MicrosoftCryptoAPI и цифровых сертификатов x.509.	4
4	6	Аппаратная реализация криптографических средств защиты информации	8
5	3-5	Программно-аппаратныйкомплекс «Аккорд»	4
6	3-5	Система защиты нформации "Secret Net"	4
7	4	Программное средство PGP	4
8	6	Средства защиты информации Dallas Lock	8
	ИТОГО		36

4.4 Балльно-рейтинговая система контроля успеваемости

В учебном процессе не применяется.

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 вопросов
1	Дать определение понятию «угроза безопасности» вычислительной системы (ВС).
2	Перечислить виды угроз безопасности ВС.
3	Дать определение понятию«программная закладка».
4	Методы внедрения программных закладок.
5	Перечислить виды негативных воздействий программных закладок на ВС.
6	Перечислить виды вредоносного программного обеспечения.
7	Дать определение понятию «Rootkit».
8	Описание методик внедрения UserModeруткитов.
9	Описание методик внедрения KernelModeруткитов.
10	Дать определение понятию «изолированная программная среда» (ИПС)
11	Дать определение понятию «монитор безопасности объектов» (МБО)
12	Дать определение понятию «монитор безопасности субъектов» (МБС)
13	Объяснить, почему для реализации ИПС необходимо требовать наличие контроля порождения субъектов и объектов
14	Дать определение понятию «политика информационной безопасности».
15	Перечислить компоненты политики безопасности.
16	Дать определение понятию «процедуры безопасности».
17	Описать какие проблемы решает верхний уровень политики безопасности.
18	Описать какие проблемы решает средний уровень политики безопасности.
19	Описать какие проблемы решает нижний уровень политики безопасности.
20	Описать, что представляют собой специализированные политики безопасности.
21	Дать определение понятиям «идентификация», «аутентификация»и «авторизация».

22	Перечислить способы аутентификации.
23	Описать методы аутентификации на основе пароля.
24	Описать методы аутентификации на основесмарт-карт.
25	Описать методы биометрической аутентификации.

5.2.Перечень контрольных работ.

Учебным планом не предусмотрено

5.3.Перечень расчетно-графических заданий.

Учебным планом не предусмотрено

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

№ п/п	Наименование темы и краткое содержание
1	Комплекс программных продуктов защиты корпоративных информационных систем «Застава». Реализация программных средств обеспечения информационной безопасности с использованием криптографических пакетов и интерфейсов
2	Программно-аппаратный комплекс обнаружения вторжений «ViPNet IDS». Реализация программных средств обеспечения информационной безопасности с использованиемкриптографических пакетов и интерфейсов
3	Персональное средство криптографической защиты информации ШИПКА. Основные этапы установки, настройки и функционирования ПСКЗИ Шипка.
4	Система автоматического распознавания лиц Face-Интеллект. Основные методы и подходы к распознаванию лиц.
5	Программно-аппаратный комплекс средств защиты информации «Аккорд - АМДЗ». Установка и основы работы с комплексом.
6	Аутентификация пользователя по отпечаткам пальцев с помощью программно-аппаратных средств Biolink.
7	Средство защиты информации SecretNet. Установка и основы работы со средством контроля каналов распространения конфиденциальной информации.
8	Персональное средство аутентификации eToken: аутентификация с помощью электронных ключей
9	Персональное средство аутентификации Rutoken: аутентификация с помощью электронных ключей
10	Программно-аппаратный комплекс предотвращения несанкционированного доступа к ресурсам компьютера «Соболь»: установка, настройка и эксплуатация комплекса.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной литературы

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон.текстовыеданные.— М.: ДМК Пресс, 2010.— 544 c. — Режим доступа: http://www.iprbookshop.ru/7943
2. Касперски Крис Фундаментальные основы хакерства. Искусство дизассемблирования [Электронный ресурс]/ Касперски Крис— Электрон. текстовые данные.— М.: СОЛОН-ПРЕСС, 2007.— 448 c.— Режим доступа: http://www.iprbookshop.ru/20925.
3. Помешкин А.А. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» [Электронный ресурс]: учебно-методическое пособие/ Помешкин А.А., Коротких И.В.— Новосибирск: Новосибирский государственный технический университет, 2012.— 47 c.— Режим доступа: http://www.iprbookshop.ru/45015.
4. Гайдамакин, Н. А. Автоматизированные информационные системы, базы и банки данных. Вводный курс : учеб. пособие / Н. А. Гайдамакин. - М. : Гелиос АРВ, 2002.
5. Платонов, В.В.Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие / В. В. Платонов. - М. : Академия, 2006. - 239 с.
6. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие / П. Б. Хорев. - М. : Академия, 2005. - 255 с

6.2. Перечень дополнительной и справочной литературы

1. ЗайцевО.В. Rootkits, SpyWare/AdWare, Keyloggers&BackDoors. Обнаружение и защита - СПб.: БХВ-Петербург, 2006. - 304 с
2. Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие – М.:Машиностроение-1, 2006.
3. 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 : Издательский центр "Академия", 2012. - 198 с.

Справочная и нормативная литература:

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»
3. Закон Российской Федерации от 21 июля 1993 г. N 5485-1 «О государственной тайне»

6.3. Перечень интернет ресурсов

1. http://www.intuit.ru - ИНТУИТ - сайт, который предоставляет возможность дистанционногообучения по нескольким образовательным программам, касающимся, восновном, информационных технологий.
2. http://ru.wikipedia.org - Википедия – свободная общедоступная мультиязычная универсальнаяинтернет-энциклопедия.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Средства обеспечения освоения дисциплины:

- Стартовые комплекты SecretNet 7, Рутокен, eToken, Соболь, Шипка, Аккорд-У, лицензия БГТУ
- Программный комплект разработчика для решений CryptoPROSDK;
- Программный комплект разработчика для решений ViPNetJCrypto SDK;
- Программный комплект разработчика для решений Рутокен (SDK)

Для лабораторных занятий используется Лаборатория программно-аппаратных средств обеспечения информационной безопасности: ГК 425б Аппаратные и программные средства в составе:

- Сканер отпечатков пальцев BioLink U-Match 3.5
- Аппаратно-программная платформа для распознавания лиц Face-Интеллект
- Средство защиты информации SecretNet 7
- USB-ключиРутокен для Windows
- USB-ключи eToken с комплектом разработчика для ОС Windows
- Персональное средство криптографической защиты «Шипка

- Программно-аппаратный комплекс «Соболь» версия 3.0.
- Универсальный программно-аппаратный комплекс СЗИ НСД «Аккорд-У»
- Электронный ключ GuardantCode
- Программно-аппаратный комплекс обеспечения информационной безопасности периметра ЛВС предприятия CheckPointAppliance 2200

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

8.1. Утверждение рабочей программы без изменений

Рабочая программа и ГРС без изменений утверждена на 201_/201_ учебный год.

Протокол № _____ заседания кафедры от «___»_____ 201_г.

Заведующий кафедрой_____

подпись, ФИО

Директор института _____

подпись, ФИО

(или)

8.2. Утверждение рабочей программы и ГРС с изменениями, дополнениями

Рабочая программа и ГРС с изменениями, дополнениями утверждена на 201_/201_ учебный год.

Протокол № _____ заседания кафедры от «___»_____ 201_ г.

Заведующий кафедрой_____

подпись, ФИО

Директор института _____

подпись, ФИО

ПРИЛОЖЕНИЯ

Приложение №1. Методические указания для обучающегося по освоению дисциплины

Примерным учебным планом на изучение дисциплины отводится один семестр. В качестве итогового контроля предусмотрен зачет с оценкой. Форма поведения зачета - устный опрос по билетам.

В процессе изучения дисциплины упор делается на сочетание методов активизации познавательной деятельности с лекционными и лабораторными занятиями.

Во введении отмечается назначение и функции программно- аппаратных средств обеспечения информационной безопасности, указать цели и задачи курса.

При изучении первой темы рассматриваютсяфункции программно-аппаратных средств защиты информации, стандарты информационной безопасности.

При изучении второй темы обращается внимание программным закладкам (классификация программных закладок;модели воздействий программных закладок на вычислительные системы;обнаружение программных закладок;методы защиты от программных закладок) ивредоносному ПО (классификация вредоносного ПО;технологии вредоносных программ и принципы их работы;UserModeRootkit;методики внедрения машинного кода в процесс;внедрение DLL с помощью ловушек и с помощью удаленных потоков;внедрение машинного кода с помощью VirtualAllocEx). Рассматриваются методики перехвата функций. Перехват модификацией машинного кода приложения. Перехват подменой адресов функций. Перехват модификацией первых байтов/команд функции. KernelModeRootkit. Основные типы KernelMode-руткитов. Перехват функций с помощью правки KiST. Перехват функций модификацией машинного кода ядра. Вмешательство в работу системы без перехвата функций.

В третьем разделе рассматриваются основные понятия политики безопасности, структураи разработкаполитики безопасности организации (базовая политика безопасности;специализированные политики безопасности;процедуры безопасности).

В четвертом разделе уделено вниманиеосновным понятиям и определениям, используемым при описании моделей безопасности компьютерных систем,видам политик управления доступом и информационными потоками,моделям компьютерных систем с мандатным, дискреционным и с ролевым управлением доступом.

При изучении пятой темы рассматриваютсятехнологии аутентификации, авторизация и администрирование действий пользователей. Методы

аутентификации, использующие пароли и PIN-коды. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация. Основные понятия строгой аутентификации. Строгая аутентификация, основанная на симметричных алгоритмах. Строгая аутентификация, основанная на асимметричных алгоритмах. Биометрическая аутентификация пользователей. Программно-аппаратные системы идентификации и аутентификации.

В шестом разделе отмечаются общие, технические и организационные сведения о программно-аппаратных комплексах защиты информации «Аккорд» и «SecretNet». рассматривается построение системы защиты информации на основе этих комплексов.