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 ИТУС
_____ В.Г. Рубанов
«__» _____ 2016 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Программно-аппаратные средства обеспечения информационной безопасности

Направление подготовки:
09.03.01 Информатика и вычислительная техника

профиль подготовки:
Вычислительные машины, комплексы, системы и сети

Квалификация (степень)
бакалавр

Форма обучения
очная

Институт Информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и автоматизированных систем

Белгород – 2016

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 «Информатика и вычислительная техника» (уровень бакалавриата), утверждённого приказом Министерства образования и науки Российской Федерации № 5 от 12 января 2016 г.
- плана учебного процесса БГТУ им. В. Г. Шухова по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль «Вычислительные машины, комплексы, системы и сети».

Составитель: к.ф.-м.н. (С. В. Зуев)
(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)

«11» 03 2016 г.

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

«11» 03 2016 г., протокол № 7

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

Рабочая программа одобрена методической комиссией института
Информационных технологий и управляющих систем

«24» 03 2016 г., протокол № 7

Председатель: к.т.н., доцент (Ю. И. Солопов)
(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-4	способность участвовать в настройке и наладке программно-аппаратных комплексов	В результате освоения дисциплины обучающийся должен **Знать:** программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях. **Уметь:** проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы. **Владеть:** навыками настройки и наладки программно-аппаратных средств обеспечения информационной безопасности
2	ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	В результате освоения дисциплины обучающийся должен **Знать:** современное состояние исследований в области построения программно-аппаратных средств обеспечения информационной безопасности. **Уметь:** разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем. **Владеть:** навыками использования программно-аппаратных средств обеспечения информационной безопасности
Профессиональные			
1	ПК-2	способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования	В результате освоения дисциплины обучающийся должен **Знать:** основные средства обеспечения информационной безопасности **Уметь:** применять средства обеспечения безопасности данных при разработке компонент аппаратно-программных комплексов и баз данных. **Владеть:** навыками разработки компонентов аппаратно-программных комплексов и баз данных с учетом требований информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Операционные системы
2	Базы данных
3	Архитектура вычислительных систем
4	Основы информационной безопасности

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Государственная итоговая аттестация

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зач. единицы, 108 часа.

Вид учебной работы	Всего часов	Семестр № 8
Общая трудоемкость дисциплины, час	108	108
Контактная работа (аудиторные занятия), в т.ч.:	21	21
лекции	7	7
лабораторные	14	14
практические		
Самостоятельная работа студентов, в том числе:	87	87
курсовой проект		
курсовая работа		
расчетно-графическое задание		
индивидуальное домашнее задание		
другие виды самостоятельной работы	51	51
Форма промежуточной аттестации (зачет, экзамен)	36	Э

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.	Вводный раздел				
	Стандарты информационной безопасности. Назначение и функции программно аппаратных средств обеспечения информационной безопасности. Функции программно аппаратных средств защиты информации.	1			3
2.	Технологии идентификации, аутентификации и авторизации.				
	Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Аутентификация пользователя по отпечаткам пальцев с помощью программно-аппаратных средств Biolink.	2		4	14
3.	Программно-аппаратный комплекс «Аккорд».				
	Построение системы защиты информации на основе комплекса. Состав комплекса. Принцип работы комплекса.	2		4	14
4.	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.	2		6	20
	ВСЕГО	7		14	51

4.2. Содержание практических (семинарских) занятий

Практические занятия учебным планом не предусмотрены.

4.3.Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 8				
1	Технологии идентификации, аутентификации и авторизации.	Аутентификация пользователя по отпечаткам пальцев с помощью программно-аппаратных средств Biolink.	4	12
2	Программно-аппаратный комплекс «Аккорд»	Программно-аппаратный комплекс «Аккорд»	4	12
3	Программно-аппаратный комплекс «SecretNet»	Программно-аппаратный комплекс «SecretNet»	6	18
		ИТОГО:	14	42
		ВСЕГО:	14	42

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

Курсовые проекты учебным планом не предусмотрены.

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

Индивидуальные домашние задания, расчетно-графические задания учебным планом не предусмотрены.

5.4. Перечень контрольных работ.

Контрольные работы учебным планом не предусмотрены.

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками :учеб.пособие / П. Н.Девянин. – М.: Горячая линия – Телеком, 2011. – 319 с. - Режим доступа: http://www.iprbookshop.ru/52225
2. 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
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 литературы

1. Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие – М.:Машиностроение-1, 2006.
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 : Издательский центр "Академия", 2012. - 198 с.
3. Касперски Крис Фундаментальные основы хакерства. Искусство дизассемблирования [Электронный ресурс]/ Касперски Крис— Электрон.

текстовые данные.— М.: СОЛОН-ПРЕСС, 2007.— 448 с.— Режим доступа: http://www.iprbookshop.ru/20925.

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»

Интернет-ресурсы:

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

Учебные аудитории для проведения занятий лекционного типа, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

Аудитории для проведения лабораторных занятий оснащены специализированной мебелью, аппаратными и программными средствами в составе:

Сканер отпечатков пальцев BioLink U-Match 3.5;

Аппаратно-программная платформа для распознавания лиц Face-Интеллект;

Средство защиты информации SecretNet 7;

USB-ключи Рутокен 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»;

Серверные платформы:

Intel S1200BTL, 1x Intel Xeon E31220 4x@3.10GHz (4 thread), 4x 4Gb, 931.5 Gb SATA 3.5;

IBM System x3550 M3, 2x Intel Xeon E5630 4x@2.53Ghz (8 thread), 6x 4Gb, 136 Gb SAS Raid;

IBM System x3550 M3, 2x Intel Xeon E5620 4x@2.40Ghz (8 thread), 2x 4Gb, 136 Gb SAS Raid;

IBM System x3550 M3, 2x Intel Xeon E5675 4x@3.07Ghz (12 thread), 3x 4Gb, 136 Gb SAS Raid;

IBM System x3550 M3, 2x Intel Xeon E5620 4x@2.40Ghz (8 thread), 2x 4Gb, 136 Gb

SAS Raid.

Монитор DISPLAY E24-8 TS Pro, EU.

ПК CPU Core i5-7500, Fujitsu ESPRIMO P556/2/E85+, RAM 8GB DDR4-2400, SSD SATA III 128GB, Optical USB mouse black, KB410 USB Black RU/US.

3D плазменный телевизор SAMSUNG PS64E8007GU.

Для освоения дисциплины могут быть использованы программные средства:

1. Microsoft Windows;
2. Microsoft Office;
3. Kaspersky Endpoint Security 10 для Windows;
4. СОТСБИ-guard;
5. Positive Technologies Application Firewall Educstion;
6. Операционная система Ubuntu, Linux Mandriva;
7. Системы обеспечения защиты межсетевого взаимодействия iptables, shorewall, Microsoft firewall;
8. XSpider Education;
9. MaxPatrol SIEM Education;
10. MaxPatrol Education;
11. Positive Technologies Application Firewall Educstion 149-17/EMicrosoft Visual Studio;
12. Microsoft Visio;
13. DevC++, CodeBlocks (компиляторы gcc);
14. Пакеты компонентов Dev Express и Component One Studio;
15. Комплект разработчика BioLink для ОС Windows;
16. Комплект разработчика Face-Интеллект для ОС Windows;
17. Стартовый комплект SecretNet 7 для Windows;
18. Стартовый комплект Рутокен для Windows;
19. Стартовый комплект eToken для Windows;
20. Стартовый комплект «Соболь» для Windows;
21. Стартовый комплект «Шипка» для Windows;
22. Стартовый комплект «Аккорд-У» для Windows дог. № 15-15к от 17.04.2015.

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2016/2017 учебный год.

Протокол № 12 заседания кафедры от «20» 06 2016 г.

Заведующий кафедрой _____ В.М. Поляков
подпись ФИО

Директор института _____ А.В. Белоусов

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2017 /2018 учебный год.

Протокол № 11 заседания кафедры от «22» 05 2017 г.

Заведующий кафедрой _____ В.М. Поляков
подпись, ФИО

Директор института _____ А.В. Белоусов

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2018/2019 учебный год.

Протокол № 10 заседания кафедры от «21» 05 2019 г.

Заведующий кафедрой _____ В.М. Поляков

подпись, ФИО

Директор института _____ А.В. Белоусов

ПРИЛОЖЕНИЯ

Приложение №1. Методические указания для обучающегося по освоению дисциплины

Целью изучения дисциплины является овладение студентами основами разработки приложения с использованием web-технологий: html, css, javascript, php, фреймворка yii.

Занятия проводятся в виде лекций и лабораторных занятий. Важное значение для изучения курса имеет самостоятельная работа студентов.

Формы контроля знаний студентов предполагают текущий и итоговый контроль. Текущий контроль знаний проводится в форме защиты лабораторных работ и расчетно-графических заданий. Формой итогового контроля является зачёт.

Распределение материала дисциплины по темам и требования к ее освоению содержатся в рабочей программе дисциплины, которая определяет содержание и особенности изучения курса.

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

Исходный этап изучения курса «Технологии web-программирования» 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 учебниках и учебных пособиях, 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.

Для более глубокого изучения проблем курса необходимо ознакомиться с публикациями в периодических изданиях и информацией в сети Интернет.

Для обеспечения систематического контроля над процессом усвоения тем курса следует пользоваться перечнем контрольных вопросов для проверки знаний по дисциплине, содержащихся в планах и заданиях к лабораторным работам. Если при ответах на сформулированные в перечне вопросы возникнут затруднения, необходимо очередной раз вернуться к изучению соответствующей темы, либо обратиться за консультацией к преподавателю.

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

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2019/2020 учебный год.

Протокол № 10 заседания кафедры от «18» мая 2019 г.

Заведующий кафедрой _____ В.М. Поляков
подпись, ФИО

Директор института _____ А.В. Белоусов

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений
Рабочая программа без изменений утверждена на 2020/2021 уч. год.

Протокол № 8 заседания кафедры от «21» 04 2020 г.

Заведующий кафедрой _____ Поляков В.М.
подпись, ФИО

Директор института _____ Белоусов А.В.
подпись, ФИО

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ[1]

Рабочая программа утверждена на 2021/2022 учебный год без изменений[2]

Протокол № 8 заседания кафедры от « 15 » мая 2021 г.

Заведующий кафедрой _____ Поляков В.М.
подпись, ФИО

Директор института _____ Белоусов А.В.
подпись, ФИО

[1] Заполняется каждый учебный год на отдельных листах
[2] Нужное подчеркнуть