МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»**
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института ИТУС

_____ В. Г. Рубанов

«24» 06 2015 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Безопасность программно-информационных систем

Направление подготовки:
09.03.04 Программная инженерия

профиль подготовки:

Разработка программно-информационных систем

Квалификация (степень)
бакалавр

Форма обучения
очная

Институт информационных технологий и управляющих систем

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Белгород – 2015

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.04 «Программная инженерия» (уровень бакалавриата), утверждённого приказом Министерства образования и науки Российской Федерации № 229 от 12 марта 2015 г.
- плана учебного процесса БГТУ им. В.Г. Шухова по направлению подготовки 09.03.04 «Программная инженерия», профиль «Разработка программно-информационных систем».

Составитель: старший преподаватель (И.Н. Гвоздевский)
(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)
(ученая степень и звание, подпись) (инициалы, фамилия)

« 16 » 04 2015 г.

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

« 16 » 04 2015 г., протокол № 11

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

« 23 » 04 2015 г., протокол № 9/12

Председатель: 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-2	владение архитектурой электронных вычислительных машин и систем	В результате освоения дисциплины обучающийся должен **Знать:** принципы построения и обеспечения безопасности станций и узлов с программным управлением; принципы построения защищенных систем и сетей передачи дискретных сообщений; средства обеспечения защиты операционных систем, информационных прикладных систем; принципы построения подсистем управления безопасностью в локальных информационных и вычислительных сетях; **Уметь:** проводить системный анализ и инжиниринг современных конвергентных инфокоммуникационных систем обеспечения безопасности; производить оценку эффективности и качества функционирования инфокоммуникационных систем. **Владеть:** инструментами обеспечения информационной безопасности в рамках современной структуры предприятия, навыками настройки и развертывания программно-аппаратных комплексов обеспечения защиты информационных систем.
2	ПК-4	владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	В результате освоения дисциплины обучающийся должен **Знать:** Основы теории защиты информационных систем; методы системного анализа и инжиниринга систем обеспечения защиты персональных систем и сетей; подходы к построению и управлению безопасностью современными персональными и комплексными системами и сетями. **Уметь:** проводить системный анализ и инжиниринг современных систем обеспечения защиты в проводных и беспроводных персональных инфокоммуникационных системах; производить оценку эффективности и качества функционирования систем обеспечения защиты. **Владеть: о**снованиями проектирования и внедрения в практику современных достижений в области информационно-телекоммуникационных технологий и систем обеспечения защиты; методиками

			проведения самостоятельных системных научных исследований в области систем обеспечения защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Архитектура вычислительных систем
2	Операционные системы
3	Основы информационной безопасности
4	Теория информации
5	Базы данных
6	Организация ЭВМ и вычислительных систем

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Управление программными проектами
2	Проектирование ВКР

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зач. единиц, 108 часов.

Вид учебной работы	Всего часов	Семестр № 6
Общая трудоемкость дисциплины, час	108	108
Контактная работа (аудиторные занятия), в т.ч.:	51	51
лекции	17	17
лабораторные	34	34
практические	—	—
Самостоятельная работа студентов, в том числе:	57	57
Курсовой проект	—	—
Курсовая работа	—	—
Расчетно-графическое задание	—	—
Индивидуальное домашнее задание	9	9
Другие виды самостоятельной работы	48	48
Форма промежуточная аттестация (зачет, экзамен)	*Диф. Зачет*	*Диф. Зачет*

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1 Наименование тем, их содержание и объем
Курс 3 Семестр 6

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1. Программно-информационные системы: основные понятия					
	Класификация программно-информационных систем. Общие вопросы оценки безопасности компьютерных систем.	2		4	8
2. Программно-информационные системы: средства обеспечения безопасности					
	Комплексные средства обеспечения информационных объектов. Классификация программных, аппаратных и гибридных методов и средств обеспечения информационной безопасности.	3		6	9
3. Средства контроля доступа к информационным объектам					
	Системы аутентификации, авторизации; межсетевой, межпрограммный уровень взаимодействия систем обеспечения безопасности; средства контроля доступа, системы разграничения доступа к ресурсам	3		6	10
4. Безопасность информационных систем и сетей					
	Безопасность информационных систем локальных, городских глобальных информационных вычислительных сетей. Проектирование и управление системами обеспечения информационной безопасности в вычислительных сетях различного уровня.	3		6	10
5. Протоколы авторизации, аутентификации и проверки подлинности					
	Протоколы авторизации, аутентификации и проверки подлинности в различных информационных системах. Инфраструктура открытого ключа PKI, Комплексные системы обеспечения антивирусной, антифишинговой, проактивной защиты.	3		6	10
6. Сетевая защита					
	Безопасность программных информационных систем. Сетевая защита, защита почтовых серверов, защита критических элементов инфраструктуры.	3		6	10
	ВСЕГО	17		34	57

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 лекц. часов	К-во часов СРС
семестр № 6				
1	Программно-информационные системы: основные понятия	Знакомство с программно-аппаратными комплексами обеспечение безопасности локально-вычислительных систем различного уровня.	4	8
2	Программно-информационные системы: средства обеспечения безопасности	Беспроводные системы обеспечения доступа к локально вычислительным сетям.	6	9
3	Средства контроля доступа к информационным объектам	Средства обеспечения безопасности сложных инфокоммуникационных систем. Создание и управление системами контроля ЛВС.	6	10
4	Безопасность информационных систем и сетей	Разработка документации согласно требованиям стандартов и ГОСТов, при построении комплексных систем обеспечения безопасности вычислительных сетей и комплекса управления ими. Системы реакции на инциденты безопасности.	6	10
5	Протоколы авторизации, аутентификации и проверки подлинности	Безопасность информационных систем. Технология PKI в доменной инфраструктуре. Протоколы Radius, TACACS+	6	10
6	Сетевая защита	Безопасность информационных систем. Применение внутренних и внешних систем обеспечения информационной безопасности. Системы на базе продуктов Checkpoint.	6	10
		ИТОГО:	34	57

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	Программно-информационные системы: основные понятия	1. Необходимость обеспечения безопасности в информационных системах. 2. Прогресс информационных технологий и информационная безопасность. 3. Нормативно-правовые аспекты информационной

		безопасности. 4. Классификация угроз безопасности информационных объектов. 5. Основные виды каналов утечки информации. 6. Умышленные и неумышленные угрозы информационной безопасности. 7. Внешние угрозы информационной безопасности. 8. Мотивы и цели компьютерных преступлений. 9. Статьи уголовного кодекса о компьютерных преступлениях 10.Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение. 11.Объекты информационной безопасности на предприятии. 12.Организационные методы обеспечения информационной безопасности. 13.Физическая защита информационных систем. 14.Программно - технические методы обеспечения информационной безопасности.
2	Программно-информационные системы: средства обеспечения безопасности	1. Организация системы защиты информации экономических систем. 2. Этапы построения системы защиты информации. 3. Политика безопасности. 4. Оценка эффективности инвестиций в информационную безопасность. 5. Обеспечение информационной безопасности автоматизированных банковских систем (АБС). 6. Информационная безопасность электронной коммерции (ЭК). 7. Обеспечение компьютерной безопасности учетной информации. 8. Сущность криптографических методов. 9. Организационно-административные мероприятия обеспечения компьютерной безопасности. 10.Организация конфиденциального делопроизводства. 11.Принципы обеспечения информационную безопасности на основе инженерно-технического обеспечения. 12.Типы и субъекты информационных угроз.
3	Средства контроля доступа к информационным объектам	1. Технологии аутентификации 2. Факторы аутентификации человека 3. Аутентификация на основе паролей 4. Аутентификация на основе аппаратных аутентификаторов 5. Аутентификация информации.Электронная подпись 6. Аутентификация на основе цифровых сертификатов 7. Аутентификация программных кодов 8. Технологии управления доступом и авторизации 9. Формы представления ограничений доступа 10.Дискреционный метод управления доступом 11.Мандатный метод управления доступом 12.Ролевое управление доступом 13.Системы аутентификации и управления доступом операционных систем 14.Аутентификации пользователей ОС 15.Аутентификация в ОС семейства Unix.Протокол SSH 16.Управление доступом в операционных системах

		17.Централизованные системы аутентификации и авторизации
4	Безопасность информационных систем и сетей	1. Кто разрабатывает стратегию информационной безопасности и защиты управленческой информации? 2. Какие современные средства защиты информации применяются в корпоративных информационных системах? 3. Что включает в себя понятие "модель информационной безопасности предприятия"? 4. Перечислите внешние и внутренние угрозы для информационных потоков и систем компании. 5. Что такое "политика информационной безопасности" и какие элементы она содержит? 6. Перечислите ключевые вопросы обеспечения информационной безопасности. 7. Какие программно-аппаратные средства применяются при обеспечении информационной безопасности предприятия? 8. Этапы проектирования сети. 9. Сетевые операционные системы. 10.Алгоритм установки сетевой ОС. 11.Служба доменных имен DNS. 12.Пространство доменных имен. 13.Работа запросов DNS. 14.Процесс рекурсии при разрешении имени. 15.Локальная система разрешения имени. 16.Типы ответов DNS-сервера. 17.Обратный просмотр. 18.Динамическое обновление. 19.Службы каталогов. 20.Active Directory. 21.Объекты службы каталогов. 22.Алгоритм добавления объекта в службу каталогов
5	Протоколы авторизации, аутентификации и проверки подлинности	1. Протокол kerberos 2. Протокол kerberos + pkinit 3. Бщие сведения о криптографии с открытым ключом 4. Авторизация и обеспечение юридической значимости электронных документов 5. Конфиденциальность и контроль целостности передаваемой информации 6. Аутентификация связывающихся сторон 7. Установление аутентичного защищенного соединения 8. Инфраструктура открытых ключей (pki) 9. Аутентификация с помощью открытого ключа на основе сертификатов 10.Организация хранения закрытого ключа 11.Интеллектуальные устройства и аутентификация с помощью открытого ключа 12.Недостатки аутентификации с помощью открытых ключей. 13.Протокол ppp pap 14.Протокол ppp chap 15.Протокол ppp eap 7 16.Протокол tacacs+ 17.Протокол radius 18.Стандарт ieee 802.1x и протокол eapol 19.Протокол eap-tls с использованием российской криптографии

6	Сетевая защита	1. Средства защиты операционной системы и ее конфигурации, программного и информационного обеспечения от потерь и несанкционированного доступа; 2. Системы доступа к информации по ключам и паролям; 3. Средства архивации данных на машинных носителях, в том числе, под паролями; 4. Антивирусные и профилактические средства; 5. Средства кодирования и раскодирования данных; 6. Средства восстановления данных при их частичной и полной утрате; 7. Автоматизированная система копирования и дублирования наборов данных на архивные носители; 8. Система программ и утилит по восстановлению наборов данных с архивных или эталонных носителей. 9. Информационные системы резервирования служб каталогов 10.Инструменты резервирования почтовых серверов 11.Средства программной защиты от преднамеренных сетевых атак на критические элементы инфраструктуры. 12.Безопасность веб-сервиса 13.Безопасность веб-браузера 14.Приватность и куки 15.Протокол https 16.Безопасность средств создания динамических страниц 17.Безопасность электронной почты 18.Угрозы приватности почтового сервиса 19.Аутентификация отправителя 20.Шифрование содержимого письма 21.Защита метаданных пользователя 22.Спам 23.Атаки почтовых приложений 24.Облачные сервисы и их безопасность 25.Концепция облачных вычислений 26.Определение облачных вычислений 27.Модели сервисов облачных сервисов 28.Облачные вычисления как источник угрозы 29.Облачные сервисы как средство повышения сетевой безопасности

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 выполнений одного индивидуального домашнего задания. ИДЗ выполняется в форме реферата. На выполнение ИДЗ предусмотрено 9 часов самостоятельной работы студента.

1. Примерная тематика ИДЗ:
2. Технология PKI в доменной инфраструктуре.
3. Протоколы Radius.
4. Протокл TACACS+.
5. Протокол HTTPS.

6. Протокол ppp pap.
7. Протокол ppp chap.
8. Протокол ppp eap 7.
9. Протокол tacacs+.
10. Протокол radius.
11. Служба доменных имен DNS.
12. Active Directory.
13. Антивирусные и профилактические средства.
14. Системы на базе продуктов Checkpoint.
15. Безопасность веб-сервиса.

5.4. Перечень контрольных работ.

Учебным планом не предусмотрены.

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. В. С. Горбатов, О. Ю. Полянская - Основы технологии PKI - 2-е изд. - Телеком, 2011
2. Д.П. Зегжда, А.М. Ивашко. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.
3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб.: Питер, 2011.

6.2. Перечень дополнительной литературы

1. Голицына, О. Л. Программное обеспечение: учеб. пособие / О. Л. Голицына, Т. Л. Партыка, И. И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2010.
2. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004.
3. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
4. Кравченко, Т. К. Инфокоммуникационные технологии управления предприятием: учеб. пособие / Т. К. Кравченко, В. Ф. Пресняков. - М. : ГУ ВШЭ, 2003.
5. Fuzzing: исследование уязвимостей методом грубой силы - ("High Tech") /Саттон М., Амини П., Грин А., Саттон М., Александр Грин, Амини П. Символ-Плюс, 2009.
6. Основы современных компьютерных технологий : учеб. / Г. А. Брякалов [и др.] ; ред. А. Д. Хомоненко. - СПб. : КОРОНА принт, 2005.

6.3. Перечень интернет ресурсов

1. Библиотека TechNet [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/ru-ru/library/aa991542
2. Библиотека OsZone [Электронный ресурс]. – Режим доступа: http://www.oszone.net/1/Windows

3. Форум информационной безопасности SecurityLab | Уязвимости [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/vulnerability/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Компьютерные классы, оснащённые компьютерами с установленными программными продуктами:

1. Операционная система Microsoft Windows, Ubuntu, Linux Mandriva. Cisco IOS, GNS, CISCO Packet Tracer (свободно-распространяемое ПО).
2. Комплексные средства обеспечения антивирусной защиты Kaspersky Antivirus, Dr. Web, Avast, Avira.
3. Среда комплексного управления безопасностью сетей Kaspersky Security Center, WSUS, Nagios, Cacti, Checkpoint Security System.
4. Система пакетного анализа tcp-dump, Wireshark (свободно-распространяемое ПО);
5. Системы обеспечения защиты межсетевого взаимодействия iptables, shorewall, Microsoft firewall (свободно-распространяемое ПО).

Приложение №1.

Методические указания для обучающегося по освоению дисциплины:

Курс «Безопасность программно-информационных систем» является базовым для студентов по направлению подготовки 09.03.04 «Программная инженерия», профиль «Разработка программно-информационных систем».

Целью курса является изучение основных технологий обеспечения информационной безопасности программно-информационных систем, которые понадобятся для дальнейшего обучения и работы.

В ходе изучения дисциплины студенты приобретают практические навыки и умения: по принципам построения и обеспечения безопасности станций и узлов с программным управлением; принципам построения защищенных систем и сетей передачи дискретных сообщений; средствам обеспечения защиты операционных систем, информационных прикладных систем; принципам построения подсистем управления безопасностью в локальных информационных и вычислительных сетях; проводить системный анализ и инжиниринг современных конвергентных инфокоммуникационных систем обеспечения безопасности; производить оценку эффективности и качества функционирования инфокоммуникационных систем; владения инструментами обеспечения информационной безопасности в рамках современной структуры предприятия, навыками настройки и развертывания программно-аппаратных комплексов обеспечения защиты информационных систем.

Занятия проводятся в виде лекций и лабораторных работ в соответствии с рабочей программой. Для изучения курса большое значение имеет самостоятельная работа студентов.

Формы контроля знаний студентов предполагают текущий и итоговый контроль. Текущий контроль знаний проводится в устный опрос. Формой итогового контроля является дифференцированный зачет.

Перед итоговым контролем рекомендуется проводить консультации, в том числе, по необходимости — индивидуальные.

Самостоятельная работа является главным условием успешного освоения изучаемой учебной дисциплины.

Исходный этап изучения курса 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 практическим занятиям, а также методических указаниях для студентов заочного обучения.

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.

Изучение каждой темы следует завершать выполнением лабораторных заданий, ответами на тесты, решением задач, содержащихся в соответствующих

разделах учебников и методических пособий. 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 практическим занятиям и методическим указаниях для студентов заочного отделения. 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.

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. В. С. Горбатов, О. Ю. Полянская - Основы технологии PKI - 2-е изд. - Телеком, 2011 1 + 1
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб.: Питер, 2011.
3. Пакин А.И. Информационная безопасность информационных систем управления предприятием [Электронный ресурс]: учебное пособие. — М.: Московская государственная академия водного транспорта, 2009. — 41 с. — — Режим доступа: http://www.iprbookshop.ru/46462.html
4. Лиманова Н.И. Архитектура вычислительных систем и компьютерных сетей [Электронный ресурс]: учебное пособие. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 197 с. — Режим доступа: http://www.iprbookshop.ru/75368.html
5. Катунин Г.П. Основы инфокоммуникационных технологий [Электронный ресурс]: учебник. — Саратов: Ай Пи Эр Медиа, 2018. — 797 с. — Режим доступа: http://www.iprbookshop.ru/74561.html

6.2. Перечень дополнительной литературы

1. Голицына, О. Л. Программное обеспечение: учеб. пособие / О. Л. Голицына, Т. Л. Партыка, И. И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2010.
2. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004.
3. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
4. Кравченко, Т. К. Инфокоммуникационные технологии управления предприятием: учеб. пособие / Т. К. Кравченко, В. Ф. Пресняков. - М. : ГУ ВШЭ, 2003.
5. Fuzzing: исследование уязвимостей методом грубой силы - ("High Tech") /Саттон М., Амини П., Грин А., Саттон М., Александр Грин, Амини П. Символ-Плюс, 2009.
6. Берлин А.Н. Основные протоколы Интернет [Электронный ресурс]. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 602 с. — Режим доступа: http://www.iprbookshop.ru/52181.html
7. Привалов И.М. Основы аппаратного и программного обеспечения [Электронный ресурс]: учебное пособие. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 145 с. — Режим доступа: http://www.iprbookshop.ru/63113.html
8. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]. — Саратов: Профобразование, 2017. — 446 с. — Режим доступа: http://www.iprbookshop.ru/63800.html
9. Персова М.Г. Современные компьютерные технологии [Электронный ресурс]: конспект лекций / М.Г. Персова, Ю.Г. Соловейчик, П.А. Домников. — Новосибирск: Новосибирский государственный технический университет, 2014. — 80 с. — Режим доступа: http://www.iprbookshop.ru/45025.htm
10. Д.П. Зегжда, А.М. Ивашко. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.

7. **МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ**

Компьютерные классы, оснащённые компьютерами с несколькими установленными программными продуктами:

1. Операционная система Microsoft Windows, Ubuntu, Linux Mandriva. Cisco IOS, GNS, CISCO Packet Tracer (свободно-распространяемое ПО).
2. Комплексные средства обеспечения антивирусной защиты Kaspersky Antivirus, Dr. Web, Avast, Avira.
3. Среда комплексного управления безопасностью сетей Kaspersky Security Center, WSUS, Nagios, Cacti, Checkpoint Security System.
4. Система пакетного анализа tcp-dump, Wireshark (свободно-распространяемое ПО);
5. Системы обеспечения защиты межсетевого взаимодействия iptables, shorewall, Microsoft firewall (свободно-распространяемое ПО).
6. СОТСБИ-guard.
7. Positive Technologies Application Firewall Educstion.

Рабочая программа и ГРС без изменений утверждена на 2016 / 2017 учебный год

Протокол № 10 заседания кафедры от « 9 » 06 2016 г.

Заведующий кафедрой _____
(подпись, Ф.И.О.)

Директор института _____
(подпись, Ф.И.О.)

Рабочая программа и ГРС без изменений утверждена на 2017 / 2018 учебный год

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

Заведующий кафедрой _____
(подпись, Ф.И.О.)

Директор института _____
(подпись, Ф.И.О.)

Рабочая программа и ГРС с изменениями, дополнениями утверждена на 2018 / 2019 учебный год

Протокол № 10 заседания кафедры от « 21 » 05 2018 г.

Заведующий кафедрой _____
(подпись, Ф.И.О.)

Директор института _____
(подпись, Ф.И.О.)

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

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ[3]

Рабочая программа утверждена на 2020 /2021 учебный год без изменений / с изменениями, дополнениями[4]

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

Заведующий кафедрой _____ (Поляков В.М.)
подпись, ФИО

Директор института _____ (Белоусов А.В.)
подпись, ФИО

[3] Заполняется каждый учебный год на отдельных листах
[4] Нужное подчеркнуть

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