ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт – Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»
Санкт-Петербургский колледж телекоммуникации

«УТВЕРЖДАЮ»

Зам. директора по УВР
колледжа СПб ГУТ

_____ Т.Н Сиротская

“ 2 ” сентября 2016 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
модуля сопряжения «Информационные технологии»

ОСНОВЫ ИНФОРМАЦИОНОЙ БЕЗОПАСНОСТИ

для специальности СПО:
09.02.03 Программирование в компьютерных системах

Направление подготовки ВО: 09.03.02 Информационные системы и технологии

Санкт - Петербург
2016

Рабочая программа составлена в соответствии с Федеральным государственным образовательным (ФГОС) стандартом высшего образования.

Составитель: Н.В.Кривоносова

Рассмотрена и одобрена на заседании цикловой комиссии № 5 (цикловая комиссия информатики и программирования в компьютерных системах)

Утверждена на заседании методического совета

«23» марта 2016 г. Протокол № 3

Председатель цикловой (предметной) комиссии:

Н.В.Кривоносова

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Область применения программы

Рабочая программа учебной дисциплины «Программирование в компьютерных сетях» (Б2.В.ДВ.2.2) является частью профессиональной образовательной программы для специальности СПО: **09.02.03 «**Программирование в компьютерных системах**»,** составлена в соответствии с ФГОС и учебным планом подготовки бакалавров по направлению подготовки **09.03.02** «Информационные системы и технологии».

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: дисциплина входит в Математический и естественнонаучный цикл.

Освоение дисциплины «Основы информационной безопасности» способствует формированию у студентов общих компетенций: умение анализировать и оценивать исторические события и процессы владением культурой мышления; способность к восприятию, обобщению и анализу информации, постановке цели и выбору путей ее достижения; готовность к кооперации с коллегами, работе в коллективе; способность анализировать социально значимые проблемы и процессы; умение логически верно, аргументированно и ясно строить устную и письменную речь; осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен:

иметь представление:

- об основных угрозах безопасности информации в сетях связи.

знать:

- политики и модели безопасности;
- требования международных стандартов и требования руководящих документов в области защиты информации от НСД;
- стандарты криптографической защиты информации;
- методы и средства защиты информации в компьютерных системах;
- основы построения защищенных сетей;
- основные протоколы, используемые для защиты информации в компьютерных системах;
- принципы построения и применения межсетевых экранов;
- основы управления средствами обеспечения безопасности информации в компьютерных сетях;
- организационно-технические мероприятия обеспечения безопасности информации в компьютерных сетях.

уметь:

- применять стандартные программно-аппаратные и технические средства защиты информации;
- планировать организацию работы по обеспечению безопасности информации компьютерной сети.

1.4. Количество часов на освоение программы дисциплины:

Максимальная учебная нагрузки обучающегося - **36** часов, в том числе:

обязательная аудиторная учебная нагрузка обучающегося **26** часов;

самостоятельная работа обучающегося - **10** часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	**36**
Обязательная аудиторная учебная нагрузка (всего)	**26**
Лекции (комбинированные уроки)	20
Лабораторные работы	6
Самостоятельная работа обучающегося (всего)	**10**
Итоговая аттестация в форме дифференцированного зачёта	

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся		Объем часов	Уровень освоения
Тема 1. Основы информационной безопасности	**Содержание учебного материала**		26	
	1.	**Политики и модели безопасности компьютерных сетей** Введение в курс. Основные понятия и определения. Угрозы, уязвимости корпоративных сетей и систем. Задачи обеспечения информационной безопасности сетей. Понятие политики безопасности. Основные типы политики безопасности. Модели безопасности. Дискреционные модели распространения прав доступа. Мандатные модели распространения прав доступа. Модели безопасности основных операционных систем.		*2*
	2	**Требования к защите информации в компьютерных сетях** Международные и государственные стандарты безопасности компьютерной информации. Классификация автоматизированных систем и нормативные требования по обеспечению безопасности компьютерной информации. Требования по обеспечению защиты от НСД к средствам вычислительной техники.		*2*
	3	**Методы и средства защиты информации в компьютерных сетях** Классификация методов и средств защиты компьютерной информации. Модель нарушителя и классификация средств криптографической защиты информации. Требования к программным и аппаратным компонентам СКЗИ.		*2*
	4	**Методы и средства защиты информации в компьютерных сетях** Стандарт шифрования данных ГОСТ-28147-89. Назначение, алгоритм шифрования, основные режимы работы. Шифрование в режимах простой замены и гаммирования. Режим формирования и проверки имитовставки. Особенности аппаратной и программной реализации алгоритмов шифрования. Стандарт шифрования данных AES. Построение и использование криптографической хеш-функции. Принцип построение пошаговой хеш-функции. Анализ хеширующего преобразования.		*2*
	5	**Методы и средства защиты информации в компьютерных сетях** Стандарт электронной цифровой подписи. Управление ключами в криптографических системах защиты компьютерной информации. Назначение,		*2*

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся		Объем часов	Уровень освоения
		классификация и требования к ключам. Генерация ключевой информации. Хранение и распределение ключевой информации.		
	6	**Способы и протоколы аутентификации** Способы и протоколы аутентификации. Способы аутентификации, использующие пароли и цифровые сертификаты. Биометрическая аутентификация.		*2*
	7	**Основы построения и защиты компьютерных сетей** Многоуровневая защита компьютерных сетей. Криптографические протоколы, используемые в технологии клиент-сервер. Криптографические протоколы защиты транспортного уровня компьютерной сети. Средства криптографической защиты в компьютерных сетях. Эксплуатационные характеристики СКЗИ. Анализ принципов построения и характеристик СКЗИ типа «Верба», «Шип», «Игла», «Шепот», «Пиранья», «Криптон-М».		*2*
	8	**Основы построения и защиты компьютерных сетей** Криптографические комплексы защиты IP-протоколов. Протокол аутентифицирующего заголовка. Протокол инкапсулирующей защиты. Защита удаленного доступа к ЛВС. Принципы организации удаленного доступа. Протоколы аутентификации удаленного доступа.		*2*
	9	**Основы построения и защиты компьютерных сетей** Защита информации при межсетевом взаимодействии. Защита информации в межсетевых экранах. Назначение и классификация межсетевых экранов. Принципы построения и функционирования межсетевых экранов на различных уровнях ВОС, применение криптографии в межсетевых экранах и фильтрах. Требования к межсетевым экранам.		*2*
	10	**Управление средствами обеспечения безопасности информации в компьютерных сетях** Организационно-технические мероприятия обеспечения безопасности информации в КС. Порядок планирования организационно-технических мероприятий по защите компьютерной информации. Обязанности должностных лиц по обеспечению информационной безопасности в КС. Аттестация объектов автоматизации. Перспективы развития средств и систем защиты информации в		*2*

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся		Объем часов	Уровень освоения
		КС. Проблемы обеспечения безопасности в КС военного назначения. Меры по обеспечению надежности функционирования систем криптографической защиты информации.		
	Лабораторные работы			
	1	**Лабораторная работа № 1** Исследование аппаратно-программных средств защиты (Криптон)		
	2	**Лабораторная работа № 2** Исследование аппаратно-программных средств защиты (Пиранья, Шепот)		
	3	**Лабораторная работа № 3** Управление настройками межсетевых экранов		
Самостоятельная работа обучающихся: Изучение конспектов лекций. Работа с учебником, с дополнительной литературой. Написание рефератов и выполнение индивидуальных заданий. Тематика рефератов и индивидуальных заданий: • Составление схемы подсистема защиты от несанкционированного доступа. • Оформление в виде конспекта основных признаков несанкционированного доступа к информации. • Разработка схемы Парольной аутентификации. • Оформление в виде конспекта основных положений общеметодологических принципов формирования теории защиты. • Составление перечня задач теории защиты. • Принципы построения защиты в сетях • Оформление в виде конспекта вопросов, касающихся понятия стратегии защиты информации и особенностей стратегических решений. • Подготовка перечня требований к сервисам безопасности. • Составление схемы основных составляющих политики безопасности. • Оформление в виде конспекта основных положений Механизма аутентификации. • Разработка структуры процессов технологии управления подсистемой защиты ОС. • Понятие системного анализа: микроскопическое представление системы, иерархическое представление системы.			**10**	

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
	• Разработка классификации моделей защиты. • Оформление в виде конспекта основных требований к Средствам и методам выявления компь-ютерных вирусов. • Подготовка архитектурной модели Управления доступом. • Оформление в виде конспекта основных положений Аутентификации в доменах Windows. • Составление перечня стадий Сетевых атак. • Определение типовой модели системы автоматизированного проектирования защиты информации. • Разработка модели защиты информации. • Оформление в виде конспекта основных положений аппаратных средств защиты информации. • Оформление в виде конспекта основных видов контроля безопасности. • Подготовка плана Аудита. Оформление в виде конспекта основных положений математической защиты информации. • Составление перечня методов кодирования информации. • Разработка алгоритма хеширования. • Подготовка перечня антивирусных программ. • Оформление в виде конспекта основных положений инженерно-технической защиты информации. Составление характеристик подсистем ввода, хранения, регистрации и учета информации.		
	Всего	**36**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие:

Учебных кабинетов, оснащенных персональными компьютерами с выходом в сеть Internet, программами эмуляторов и симуляторов; компьютерных мастерских;

Лаборатории:

- «Информационной безопасности»;
- «Компьютерных сетей»;
- «Информационно-коммуникационных сетей связи»;

Для выполнения лабораторных и практических работ необходимо иметь **оборудование**:

ПК по количеству обучающихся с установленным лицензионным ПО, операционные системы семейств WINDOWS, LINUX, антивирусные программы, текстовый редактор.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К.Баранова, А.В.Бабаш. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2016.
2. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие для вузов. - М.: ФОРУМ, 2015.
3. Шаньгин В.Ф. Информационная безопасность и защита информации. - М.: ДМК Пресс, 2014.
4. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. - М.: ФОРУМ: ИНФРА-М, 2016.

Дополнительные источники:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие для вузов / А. А.Афанасьев, Л.Т.Веденьев, А.А.Воронцов [и др.]. – М.: Горячая Линия–Телеком, 2012.
2. Басалова Г.В. Основы криптографии. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. - М.: Горячая линия-Телеком, 2013.
4. Олифер, В.Г. Безопасность компьютерных сетей/В.Г.Олифер, Н.А.Олифер. - М.: Горячая линия-Телеком, 2014.
5. Основы управления информационной безопасностью: учебное пособие / Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. – М.: Горячая Линия–Телеком, 2013.
6. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов. - М.: Горячая линия-Телеком, 2014.
7. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов/О. И.Шелухин, Д. Ж. Сакалема, А. С. Филинова. - М.: Горячая линия-Телеком, 2013.

Интернет-ресурсы:

1. Comnews. Новости телекоммуникаций, вещания и ИТ: ежедневная Интернет-газета[Электронный ресурс]. - Режим доступа: http://www.comnews.ru/, свободный.
2. Connect! Мир связи: сетевой журнал [Электронный ресурс]. - Режим доступа: http://www.connect.ru/, свободный.
3. Интернет-университет информационных технологий - Интуит (Национальный Открытый университет. Безопасность [Электронный ресурс]: каталог курсов. - Режим доступа: http://old.intuit.ru/catalog/security/, свободный.
4. Компоненты и технологии: сетевой журнал [Электронный ресурс]. - Режим доступа: http://www.kit-e.ru/, свободный.
5. Сайт компании Cisco [Электронный ресурс]. - Режим доступа: http://www.cisco.ru/, свободный.
6. Сайт компании D-Link [Электронный ресурс]. - Режим доступа: http://www.dlink.ru/, свободный.
7. Современные телекоммуникации России: отраслевой информационно-аналитический онлайн-журнал [Электронный ресурс]. - Режим доступа: http://www.telecomru.ru/, свободный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка **результатов освоения дисциплины осуществляется преподавателем в процессе проведения аудиторных занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.**

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Иметь представление: – об основных угрозах безопасности информации в сетях связи.	выполнение индивидуальных проектов; выполнение тестовых заданий, сдача зачёта
знать:	
– политики и модели безопасности; – требования международных стандартов и требования руководящих документов в области защиты информации от НСД; – стандарты криптографической защиты информации; – методы и средства защиты информации в компьютерных системах; – основы построения защищенных сетей; – основные протоколы, используемые для защиты информации в компьютерных системах; – принципы построения и применения межсетевых экранов; – основы управления средствами	выполнение индивидуальных проектов; выполнение тестовых заданий, выполнение домашних заданий, сдача зачёта

обеспечения безопасности информации в компьютерных сетях; – организационно-технические мероприятия обеспечения безопасности информации в компьютерных сетях.	
уметь:	
– применять стандартные программно-аппаратные и технические средства защиты информации; – планировать организации работы по обеспечению безопасности информации компьютерной сети.	выполнение индивидуальных заданий и выступление с докладами; выполнение тестовых заданий, выполнение домашних заданий, сдача дифференцированного зачёта

Приложение

Вопросы и задания к дифференцированному зачёту
по дисциплине
«Основы информационной безопасности»

1. Угрозы, уязвимости корпоративных сетей и систем.
2. Задачи обеспечения информационной безопасности сетей.
3. Понятие политики безопасности. Основные типы политики безопасности.
4. Модели безопасности. Дискреционные модели распространения прав доступа.
5. Мандатные модели распространения прав доступа.
6. Модели безопасности основных операционных систем.
7. Международные и государственные стандарты безопасности компьютерной информации.
8. Требования по обеспечению защиты от НСД к средствам вычислительной техники.
9. Классификация методов и средств защиты компьютерной информации.
10. Модель нарушителя и классификация средств криптографической защиты информации. Требования к программным и аппаратным компонентам СКЗИ.
11. Стандарт шифрования данных ГОСТ-28147-89. Назначение, алгоритм шифрования, основные режимы работы.
12. Шифрование в режимах простой замены и гаммирования.
13. Режим формирования и проверки имитовставки. Особенности аппаратной и программной реализации алгоритмов шифрования.
14. Стандарт шифрования данных AES.
15. Построение и использование криптографической хеш-функции.
16. Принцип построения пошаговой хеш-функции.
17. Стандарт электронной цифровой подписи.
18. Управление ключами в криптографических системах защиты компьютерной информации. Назначение, классификация и требования к ключам.
19. Генерация ключевой информации.
20. Хранение и распределение ключевой информации.
21. Способы и протоколы аутентификации.
22. Способы аутентификации, использующие пароли и цифровые сертификаты.
23. Биометрическая аутентификация.
24. Многоуровневая защита компьютерных сетей.
25. Криптографические протоколы, используемые в технологии клиент-сервер.
26. Криптографические протоколы защиты транспортного уровня компьютерной сети.
27. Средства криптографической защиты в компьютерных сетях.
28. Криптографические комплексы защиты IP-протоколов.
29. Протокол аутентифицирующего заголовка.
30. Протокол инкапсулирующей защиты.
31. Защита удаленного доступа к ЛВС.
32. Протоколы аутентификации удаленного доступа.
33. Защита информации при межсетевом взаимодействии.
34. Защита информации в межсетевых экранах. Назначение и классификация межсетевых экранов.
35. Принципы построения и функционирования межсетевых экранов на различных уровнях ВОС, применение криптографии в межсетевых экранах и фильтрах. Требования к межсетевым экранам.
36. Организационно-технические мероприятия обеспечения безопасности информации в КС. Порядок планирования организационно-технических мероприятий по защите компьютерной информации.

37. Обязанности должностных лиц по обеспечению информационной безопасности в КС. Аттестация объектов автоматизации.
38. Перспективы развития средств и систем защиты информации в КС.
39. Проблемы обеспечения безопасности в КС военного назначения.
40. Меры по обеспечению надежности функционирования систем криптографической защиты информации.