Частное образовательное учреждение высшего образования
«Санкт-Петербургский университет технологий управления и экономики»

УТВЕРЖДАЮ
Первый проректор
_____ С.В. Авдашкевич
«29» 08 2017 г.

РАБОЧАЯ ПРОГРАММА

учебной дисциплины

ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность СПО:	*09.02.05 Прикладная информатика (по отраслям)*
Программа подготовки:	*базовая*
Форма обучения:	*очная*
Уровень образования, необходимый для приема на обучение по ППССЗ:	*основное общее образование*
Профиль получаемого профессионального образования:	*технический*

Санкт-Петербург
2017

Разработчик (и) __Смирнова С.Л.___ ____преподаватель___
(ФИО) степень, должность

ОБСУЖДЕНО

на заседании ПЦК _Прикладная информатика_

«29» августа 2017 г., протокол № 1

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.05 Прикладная информатика (по отраслям).

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы:

учебная дисциплина входит в учебный цикл: профессиональный учебный цикл.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины[1]:

Процесс изучения дисциплины способствует формированию следующих компетенций:

Код	*Содержание компетенции*
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ПК 2.2	Разрабатывать и публиковать программное обеспечение и информационные ресурсы отраслевой направленности со статическим и динамическим контентом на основе готовых спецификаций и стандартов.
ПК 2.3	Проводить отладку и тестирование программного обеспечения отраслевой направленности.
ПК 2.4	Проводить адаптацию отраслевого программного обеспечения.
ПК 2.5	Разрабатывать и вести проектную и техническую документацию.
ПК 2.6	Участвовать в измерении и контроле качества продуктов.

[1] Требования к результатам освоения учебной дисциплины (умения, знания, ОК и ПК) указываются в соответствии с ФГОС. Требования к результатам освоения учебной дисциплины (умения, знания, ОК и ПК), добавленные за счет часов вариативной части ППССЗ, отмечаются символом «*».

ПК 3.1	Разрешать проблемы совместимости программного обеспечения отраслевой направленности.
ПК 3.2	Осуществлять продвижение и презентацию программного обеспечения отраслевой направленности.
ПК 3.3	Проводить обслуживание, тестовые проверки, настройку программного обеспечения отраслевой направленности.
ПК 3.4	Работать с системами управления взаимоотношениями с клиентами.

В результате освоения учебной дисциплины обучающийся должен
У меть:

- проверить компьютер на предмет наличия уязвимостей и угроз доступности
- разработать политику информационной безопасности
- выявлять вредоносный код программными средствами
- подбирать и оптимизировать антивирусный комплекс под определенную систему
- управлять политикой безопасности и доступом в Оспользователей и групп пользователей
- диагностировать работу и безопасность сети
- управлять системными службами целью повышения безопасности системы и контроля ее безопасности.

Знать:

- составляющие информационной безопасности
- системы формирования режима информационной безопасности
- общие критерии ИБ
- стандарты информационной безопасности распределенных систем.

В рамках рабочей программы используются следующие активные и интерактивные формы проведения занятий: метод «мозгового штурма», мультимедиа-презентация, проблемная лекция, учебная дискуссия.

1.4. Количество часов на освоение рабочей программы учебной дисциплины:
максимальной учебной нагрузки обучающегося 94 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 68 часов;
самостоятельной работы обучающегося 26 часов.

Учебная дисциплина введена за счет часов вариативной части ППССЗ.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

2.1.1. Очная форма обучения

Вид учебной работы	***Объем часов***	**Семестр**	
		7	**8**
Максимальная учебная нагрузка обучающегося (всего)	**94**	46	48
Обязательная аудиторная учебная нагрузка обучающегося (всего)	**68**	32	36
В том числе:			
Лекционные занятия (ЛЗ)	40	16	24
Практические занятия, семинары (ПЗ)	28	16	12
Контрольные работы (КР)		+	
Самостоятельная работа обучающегося (СР)	**26**	14	12
Форма промежуточной аттестации[2]	**ДЗ**		ДЗ

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)**	**Объем часов**				**Уровень освоения**[3]
		Очная форма				
		Всего	**в том числе**			
			ЛЗ	**ПЗ + ЛР + КР**	**СР**	
Раздел 1. Информационная безопасность и уровни ее обеспечения		**24**	**14**	**4**	**6**	

[2] Формы промежуточной аттестации (ДЗ – дифференцированный зачет, З – зачет, Э – экзамен) указываются в соответствии с учебным планом. Если в семестре не предусмотрена промежуточная аттестация, в соответствующей ячейке таблицы указывается «–» (другие формы контроля в таблице не указываются).

[3] 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)

Тема 1.1. Понятие "информационная безопасность"	**Содержание учебного материала**	10	6	2	2	***2***
	Составляющие информационной безопасности Система формирования режима информационной безопасности		6			
	Практические занятия Права на использование директории для определенного пользователя			2		
	Самостоятельная работа Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации				2	
Тема 1.2. Стандарты ИБ	**Содержание учебного материала**	14	8	2	4	***3***
	Общие критерии ИБ Стандарты информационной безопасности распределенных систем Административный уровень обеспечения информационной безопасности Каналы несанкционированного доступа к информации		8			
	Практические занятия Проверка компьютера на предмет наличия уязвимостей Исследование угроз доступности Разработка политики информационной безопасности			2		
	Контрольная работа					
	Самостоятельная работа Классификация угроз "информационной безопасности»				4	
Раздел 2. Компьютерные вирусы и защита от них		**12**	**4**	**2**	**6**	
Тема 2.1. Вирусы как угроза информационной безопасности Классификация компьютерных вирусов	**Содержание учебного материала**	12	4	2	6	****3***
	Классификация компьютерных вирусов и характеристика "вирусоподобных" программ		4			
	Практические занятия Исследование реестра, на предмет возможных уязвимостей для вирусов Дизассамблирование кода поиск и лечение вредоносного кода			2		
	Контрольная работа					
	Самостоятельная работа Оптимизация антивирусной программы под определенную систему				6	
Раздел 3. Безопасность операционных систем		**22**	**10**	**10**	**2**	

Тема 3.1. Основы информационной безопасности ОС	**Содержание учебного материала**	6	2	4	-	2
	Политика безопасности Управление доступом Аутентификация и авторизация		2			
	Практические занятия Вход в систему и завершение сеанса Изучение базовых прав доступа			4		
	Контрольная работа					
Тема 3.2. Концепции безопасности UNIX	**Содержание учебного материала**	6	2	4	-	3
	Пользователи и группы Права доступа Суперпользователь Аутентификация пользователей		2			
	Практические занятия Переход в режим суперпользователя Изучение базы данных пользователей			4		
Тема 3.3. Настройка системы безопасности	**Содержание учебного материала**	10	6	2	2	3
	База данных пользователей системы Изменение базы данных пользователей Изменение прав доступа Ограничения сеанса пользователя		6			
	Практические занятия Добавление и удаление пользователей			2		
	Контрольная работа					
	Самостоятельная работа команды управления правами. Команды управления пользователями.				2	
Раздел 4. Безопасность в КС		**32**	**8**	**12**	**12**	
Тема 4.1. Сетевой интерфейс в ОС	**Содержание учебного материала**	8	2	2	4	3
	Конфигурация IP-сетей		2			
	Практические занятия Настройка сетевого интерфейса			2		
	Контрольная работа					
	Самостоятельная работа Команды по конфигурированию сети Команды по диагностике сети				4	
Тема 4.2. Сервисы Internet	**Содержание учебного материала**	12	2	6	4	3

	Служба доменных имён Удалённый терминал Прокси-серверы		2			
	Практические занятия Настройка таблицы маршрутизации Изучение службы доменных имён Простая диагностика работы сети Работа по удалённому терминалу			6		
	Контрольная работа					
	Самостоятельная работа Команды удалённого терминала				4	
Тема 4.3. Межсетевой экран	**Содержание учебного материала**	8		4	4	3
	Практические занятия Сканирование локальной сети Сканирование удалённых хостов Настройка сетевого экрана			4		
	Контрольная работа					
	Самостоятельная работа Команды по управлению сетевым экраном Расширенная диагностика и настройка сети				4	
Раздел 5. Управление службами ОС		8	4	4		
Тема 5.1. Загрузка операционной системы	**Содержание учебного материала**					2
	Этапы загрузки системы Процесс init Конфигурация запуска init Какие бывают службы Служба планирования заданий Сетевые службы Мониторинг и журналирование		4			
	Практические занятия Управление сетевыми слкжбами и службами журналирования			4		
Дифференцированный зачет		2	2			
Всего:		**94**	**40**	**28**	**26**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия

Кабинет теории информации;

Кабинет архитектуры электронно-вычислительных машин и вычислительных систем № 502 СПБ, Рижский пр., д. 26, Лит.Б

Оборудование:

Персональные компьютеры, проектор плакаты, столы, стулья, программное обеспечение: Microsoft Office, Консультант-Плюс, Гарант.

3.2. Учебно-методическое и информационное обеспечение

Основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М. : Издательство Юрайт, 2017. — 325 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-00843-2.
2. Проектирование информационных систем : учебник и практикум для СПО / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук ; под общ. ред. Д. В. Чистова. — М. : Издательство Юрайт, 2016. — 258 с.
3. Новожилов, О. П. Информатика : учебник для СПО / О. П. Новожилов. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017. — 620 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-04436-2.

Дополнительная литература:

1. Мельников Д.А. Информационная безопасность открытых систем. — Москва: Флинта 2014 г.— 448 с. — Электронное издание. — ISBN 978-5-9765-1613-7
2. Гаврилов, М. В. Информатика и информационные технологии : учебник для СПО / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017. — 383 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-03051-8.
3. Чусавитина Г.Н., Давлеткириева Л.З., Чернова Е.В., ред. Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. — Москва: Флинта 2014 г.— 161 с. — Электронное издание. — ISBN 978-5-9765-2038-7

Периодические издания

1. Бизнес-информатика [Электронный ресурс] : журнал. – Режим доступа: elibrary.ru.
2. Вестник АГТУ. Серия: Управление, вычислительная техника и информатика [Электронный ресурс] : журнал. – Режим доступа: cyberleninka.ru.
3. Интернет-маркетинг [Электронный ресурс] : журнал. – Режим доступа: grebennikon.ru.
4. Информатика и системы управления [Электронный ресурс] : журнал. – Режим доступа: elibrary.ru.
5. Информационные системы и технологии [Электронный ресурс] : журнал. – Режим доступа: elibrary.ru.
6. Прикладная информатика [Электронный ресурс] : журнал. – Режим доступа: elibrary.ru.
7. Программные продукты и системы [Электронный ресурс] : журнал. – Режим доступа: e.lanbook.com.
8. Системы и средства информатики [Электронный ресурс] : журнал. – Режим доступа: elibrary.ru.

Современные профессиональные базы данных и информационные ресурсы:

1. ЭБС «Юрайт» (http://biblio-online.ru)
2. ЭБД «Издательский дом «Гребенников» (http://grebennikon.ru/)
3. ЭБС «Айбукс.ру» (www.ibooks.ru)
4. ЭБС «Лань» (http://e.lanbook.com/)
5. ЭБС «Университетская библиотека онлайн» (http://biblioclub.ru)
6. Архив научных журналов НЭИКОН (http://arch.neicon.ru)

7. ЭБС СПбУТУиЭ (http://libume.ru/jirbis/)
8. Информационно-справочная правовая система Консультант Плюс (http://www.consultant.ru)
9. Научная электронная библиотека elibrary.ru (elibrary.ru)
10. Научная электронная библиотека «Киберленинка» (cyberleninka.ru)
11. Справочная правовая система Гарант (http://www.garant.ru)

Информационные ресурсы в сети «Интернет»:

1. ALGLIB: кросс-платформенная библиотека численного анализа (http://alglib.sources.ru)
2. Algolist.manual.ru: алгоритмы, методы, исходники (http://algolist.manual.ru)
3. Codenet.ru: все для программиста (http://www.codenet.ru)
4. DATBAZE: база полезных знаний (https://datbaze.ru)
5. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)
6. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru)
7. Информационно-коммуникационные технологии в образовании: портал (http://www.ict.edu.ru)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
У меют: • проверить компьютер на предмет наличия уязвимостей и угроз доступности • разработать политику информационной безопасности • выявлять вредоносный код программными средствами • подбирать и оптимизировать антивирусный комплекс под определенную систему • управлять политикой безопасности и доступом в Оспользователей и групп пользователей • диагностировать работу и безопасность сети • управлять системными службами целью повышения безопасности системы и контроля ее безопасности. Знают: • составляющие информационной безопасности • системы формирования режима информационной безопасности • общие критерии ИБ	Оценка результатов практических занятий Устный фронтальный и индивидуальный опрос Оценка результатов тестирования Оценка рефератов, других творческих работ обучающихся, в том числе компьютерных презентаций по темам Выполнение дополнительных заданий по собственной инициативе обучающихся

Приложение 1

Распределение часов вариативной части

Дисциплина введена за счет часов вариативной части ППССЗ.