ДЕПАРТАМЕНТ СМОЛЕНСКОЙ ОБЛАСТИ ПО ОБРАЗОВАНИЮ И НАУКЕ
областное государственное бюджетное профессиональное образовательное учреждение
«Смоленская академия профессионального образования»
(ОГБПОУ СмолАПО)

УТВЕРЖДАЮ
Директор ОГБПОУ СмолАПО
_____ М. В. Белокопытов

ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.17 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Смоленск
2019 г.

Рабочая программа учебной дисциплины ОП.17 Основы информационной безопасности разработана с учетом требований Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) **09.02.06 Сетевое и системное администрирование**

Организация разработчик: ОГБПОУ СмолАПО

Разработчик:

Ромашкова И. А. – преподаватель ОГБПОУ СмолАПО

Рассмотрено на заседании кафедры Информационных технологий

Протокол № 1 от 30.08.2019 г.

Рекомендовано к утверждению научно-методическим советом ОГБПОУ СмолАПО

Протокол № 1 от 31.08.2019 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Область применения рабочей программы учебной дисциплины

Рабочая программа учебной дисциплины ОП.17 Основы информационной безопасности является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

1.2Место учебной дисциплины в структуре основной образовательной программы

Учебная дисциплина ОП.17 Основы информационной безопасности относится кобщепрофессиональному циклу дисциплин по специальности, является дисциплиной,устанавливающей базовые знания для освоенияПМ.01 Выполнение работ по проектированию сетевой инфраструктуры, ПМ.03 Эксплуатация объектов сетевой инфраструктуры.

1.3 Цель и планируемые результаты освоения рабочей программы учебной дисциплины

В результате освоения учебной дисциплины обучающийся ***должен уметь:***

- классифицировать основные угрозы безопасности информации;
- применять организационные, правовые, программно-аппаратные, методы и средства защиты информации.

В результате освоения учебной дисциплины обучающийся ***должен знать:***

- сущность и понятия информационной безопасности;
- основные угрозы, методы и средства обеспечения информационной безопасности;
- принципы защиты информации от несанкционированного доступа.

В результате освоения учебной дисциплины обучающийся осваивает элементы компетенций.

Перечень общих компетенций, элементы которых формируются в рамках учебной дисциплины:

Код	Наименование общих компетенций

ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке

Перечень профессиональных компетенций, элементы которых формируются в рамках учебной дисциплины:

Код	**Наименование профессиональных компетенций**
ПК 1.3	Обеспечивать защиту информации в сети с использованием программно-аппаратных средств
ПК 3.4	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации

2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы	**46**
в том числе:	
теоретическое обучение	32
практические занятия	10
контрольная работа	1
самостоятельная работа	2
зачетное занятие	1
Промежуточная аттестация проводится в форме *зачета*	

2.2 Тематический план и содержание рабочей программы учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем часов	Коды компетенций, формированию которых способствует элемент программы
Тема 1. Сущность и понятие информационной безопасности	**Содержание учебного материала**	**Уровень освоения**	**2**	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 09 ОК 10 ПК 1.3 ПК 3.4
	1.1Национальные интересы в информационной сфере. Информационные ресурсы. Информационные войны	2		
	1.2 Доктрина информационной безопасности РФ	2		
	Тематика практических занятий		**2**	
	Практическое занятие «Анализ Доктрины информационной безопасности Российской Федерации»			
Тема 2. Правовые основы защиты информации	**Содержание учебного материала**	**Уровень освоения**	**4**	ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 9 ОК 10 ПК 1.3 ПК 3.4
	2.1 Основные законодательные акты РФ в области защиты информации. Стандарты и нормативно-методические документы в области обеспечения ИБ	2		
	2.2 Ответственность за нарушение законодательства в информационной сфере	2		
	Тематика практических занятий		**2**	
	Практическое занятие «Анализ стандартов информационной безопасности и их применение в организационно-правовой деятельности по защите информации»			
Тема 3. Основные угрозы информационной безопасности	**Содержание учебного материала**	**Уровень освоения**	**6**	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 09
	3.1Цели и задачи защиты информации. Источники и носители защищаемой информации. Понятие конфиденциальной информации	2		
	3.2 Угрозы безопасности информации. Системная классификация угроз безопасности информации. Методы оценки уязвимости информации	3		

	3.3Виды утечки информации. Источники рисков и формы атак на информацию	2		ОК 10 ПК 1.3 ПК 3.4
	Тематика практических занятий			
	Практическое занятие «Классификация угроз безопасности информации на типовом объекте информатизации»		**2**	
Тема 4. Методы и средства обеспечения информационной безопасности	**Содержание учебного материала**	**Уровень освоения**		ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 9 ОК 10 ПК 1.3 ПК 3.4
	4.1Методы обеспечения информационной безопасности компьютерных сетей	2	**7**	
	4.2 Требования по защите средств ВТ и АС от НСД. Классы и показатели защищенности от НСД	2		
	4.3Принципы защиты информации от несанкционированного доступа Разграничение доступ. Идентификация и аутентификации информационной безопасности. Парольные системы для защиты от несанкционированного доступа к информации	3		
	4.4 Криптографические методы защиты информации	2		
	Тематика практических занятий			
	Практическое занятие «Средства защиты информации: идентификация, аутентификация и разграничение доступа. Криптографические средства защиты информации»		**2**	
	Самостоятельная работа обучающихся Выполнение упражнений на шифрование и дешифрование информационных сообщений различными криптографическими методами		**1**	
Тема 5. Программно-аппаратная защита информации	**Содержание учебного материала**	**Уровень освоения**		ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 9 ОК 10 ПК 1.3 ПК 3.4
	5.1Программно-аппаратные угрозы информационной безопасности компьютерных систем	2	**10**	
	5.2 Виды вредоносных программ. Классификация вирусов. Структура современных вирусов	2		
	5.3 Классификация антивирусных программ	2		
	5.4 Защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты	2		
	5.5 Программно-аппаратные комплексы защиты информации	2		
	5.6 Резервное копирование информации	2		
	Тематика практических занятий		**2**	

	Практическое занятие «Применение программно-аппаратных средств защиты информации»			
Тема 6. Обеспечение информационной безопасности	**Содержание учебного материала**	**Уровень освоения**	**3**	ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 9 ОК 10 ПК 1.3 ПК 3.4
	6.1Управление безопасностью. Управление правами пользователей. Привилегии	2		
	6.2 Система аудита. Локальная политика безопасности	2		
	Самостоятельная работа обучающихся Анализ локальной политики безопасности персонального компьютера		**1**	
	Контрольная работа		**1**	
	Зачетное занятие		**1**	

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

3.УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Материально-техническое обеспечение реализации рабочей программы учебной дисциплины

Для реализации рабочей программы учебной дисциплины ОП.17Основы информационной безопасности предусмотрена мастерская «Кибер-безопасности», оснащенная следующим оборудованием и программным обеспечением:

- Персональный компьютер в сборе: Processor - AMD Ryzen X8 R7-1700, DDR4 DIMM 32Гб, Видеокарта - ASUS GeForce GTX 1650 PHOENIX OC [PH-GTX1650-04G], SD накопитель A-DATA S11 Pro AGAMMIXS11P-512GT-C 512 Гб;
- Компьютерный монитор AOC 24" G2460VQ6;
- Клавиатура USB CBR KB 107;
- Компьютерная мышь USB CBR CM-302;
- Источник бесперебойного питания Powercom UPS RPT-800A EURO;
- Сервер [2U / 2 x Intel Xeon Silver 4210R (2.4GHz,10C) / 8 x 32Gb DDR4 2933, ECC R(24up) / 4x960Gb SSD SATA / 4 x 10GE / 2 x 800w;
- Управляемый Коммутатор Cisco WS-C2960L-48;
- Коммутатор L3 WS-C3650-24;
- Телевизор 50” LED Haier LE50K5500TF;
- Флипчат электронный SMART kapp 42;
- Интерактивная доска ScreenMedia;
- Проектор CASIO XJ-V110W с потолочным креплением и коммутацией;
- МФУ Canon i-SENSYS MF426dw;
- USB-токен JaCarta-2 PKI/ГОСТ (XL) JC-MediaKit-4 - "ПКJaCarta – MediaKit,
- РутокенЭЦП 2.0 64 кб;
- RDS-01 USB считывательключей Dallas Touch Memory (iButton);
- DS1996 сизогнутымбрелоком - электронныйключDallasTouchMemory (IButton);
- FindkeyHamster III (HFDU06S) - настольный биометрический считыватель;
- Установочный комплект. Средство защиты информации SecretNetStudio 8;
- Установочный комплект. Средство защиты информации vGate R2;
- Дистрибутив СКЗИ КриптоПро CSP версии 5.0 КС1 и КС2 на DVD;
- Формуляры DallasLock 8.0-К. Право на использование** (СЗИ НСД.СКН); Бессрочная лицензия DallasLock 8.0. Сертифицированный комплект для установки;
- Программное обеспечение клиентского доступа к виртуальным машинам AcademicVMwareWorkstation 15 ProforLinuxandWindows;
- СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;
- ПО операционная система Windows 10 с интегрированной программной платформой .NET Framework, 4.8;
- ПО для просмотра документов в формате PDF AdobeReader DC;
- ПО для архивации 7-Zip;
- ПО офисный пакет MicrosoftOffice 2019;
- СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;
- Антивирусное программное обеспечение KasperskyEndpointSecurity.

Каждое рабочее место, оснащено персональным компьютером с высокоскоростным доступом к сети Интернет.

3.2 Информационное обеспечение реализации рабочей программы учебной дисциплины

Для реализации рабочей программы учебной дисциплины ОП.17Основы информационной безопасности используются следующие печатные издания и дополнительные информационные ресурсы:

Основные источники (печатные издания):

1. Бубнов А.А. Основы информационной безопасности (2-е изд., стер.) учеб. Пособие. - М.: Академия, 2016

Дополнительные источники:

1. Мельников В.П. Информационная безопасность: учеб.пособие для СПО / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М.: Академия, 2014.

2. Защита информации в персональном компьютере: учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – М.: ФОРУМ, 2013. – 368с.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Используемые формы и методы оценки, а также применяемые критерии при реализации рабочей программы учебной дисциплины ОП.17 Основы информационной безопасности:

Результаты обучения	Критерии оценки	Формы и методы оценки
Перечень знаний, осваиваемых в рамках дисциплины: – сущность и понятия информационной безопасности; – основные угрозы, методы и средства обеспечения информационной безопасности; – принципы защиты информации от несанкционированного доступа.	– полно раскрывает сущность информационной безопасности; – правильность формулировок понятий информационной безопасности; – четко описывает основные угрозы, методы и средства обеспечения информационной безопасности; – полно раскрывает принципы защиты информации от несанкционированного доступа	- устный опрос; - индивидуальная беседа; - тестирование; - оценка ответов в ходе эвристической беседы; - защита практических работ; - контрольная работа
Перечень умений, осваиваемых в рамках дисциплины: – классифицировать основные угрозы безопасности информации; – применять организационные, правовые, программно-аппаратные методы и средства защиты информации.	– правильно распознает основные угрозы безопасности информации; – правильность выбора метода защиты информации объекта; – соответствие выбранных организационных, программно-аппаратных средств защиты информации степени конфиденциальности информации.	- выполнение практических работ; - тестирование, - демонстрация умения распознавать основные угрозы безопасности информации; - демонстрация умения применять организационные, правовые, программно-аппаратные методы и средства защиты информации.

5. ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ В ДРУГИХ ООП

Рабочая программа учебной дисциплины ОП.17Основы информационной безопасности может быть использована в ООП укрупненной группы специальностей 09.00.00 Информатика и вычислительная техника.