ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

АРХАНГЕЛЬСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ
ИМ. Б.Л. РОЗИНГА (ФИЛИАЛ) СПбГУТ
(АКТ (ф) СПбГУТ)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 7EDEC31CD7768B9DAE1B249DD415B9F5
Владелец: Топанов Александр Павлович
Действителен: с 02.05.2023 до 25.07.2024

УТВЕРЖДАЮ
Зам. директора по учебной работе
_____ М.А. Цыганкова
_____ 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.13. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

по специальности:

09.02.01 - Компьютерные системы и комплексы

г. Архангельск
2024

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы и в соответствии с учебным планом по специальности 09.02.01 Компьютерные системы и комплексы.

Рабочая программа рассмотрена и одобрена цикловой комиссией Информационной безопасности инфокоммуникационных систем
Протокол № 7 от 28.05 2024 г.
Председатель _____ А.А. Садков

Автор:
А.А. Садков, преподаватель первой квалификационной категории АКТ (ф) СПбГУТ.

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1 Область применения программы

Рабочая программа учебной дисциплины (далее рабочая программа) – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.01 Компьютерные системы и комплексы.

1.2 Место учебной дисциплины в структуре программы подготовки специалистов среднего звена

Дисциплина входит в профессиональный цикл

1.3 Цель и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины

В результате освоения учебной дисциплины обучающийся должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации.

В результате освоения учебной дисциплины обучающийся должен знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- современные средства и способы обеспечения информационной безопасности.

1.4 Перечень формируемых компетенций

Общие компетенции (ОК):

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

Профессиональные компетенции (ПК):

ПК 1.5. Выполнять требования нормативно-технической документации.

ПК 3.1. Проводить контроль параметров, диагностику и восстановление работоспособности компьютерных систем и комплексов

ПК 3.2. Проводить системотехническое обслуживание компьютерных систем и комплексов

ПК 3.3. Принимать участие в отладке и технических испытаниях компьютерных систем и комплексов; инсталляции, конфигурировании программного обеспечения

Личностные результаты (ЛР): ЛР1-ЛР22

1.5 Количество часов на освоение рабочей программы учебной дисциплины

максимальной учебной нагрузки обучающегося 96 часов, в том числе:
- обязательной аудиторной учебной нагрузки обучающегося 64 часов,
- самостоятельной работы обучающегося 32 часа.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**96**
Обязательная аудиторная учебная нагрузка (всего)	**64**
в том числе:	
практические занятия	32
Самостоятельная работа обучающегося (всего)	**32**
в том числе:	
работа с учебной литературой, конспектами лекций, решение задач и выполнения упражнений	16
подготовка к практическим занятиям	16
Промежуточная аттестация в форме дифференцированного зачёта	

2.2 ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа студентов		Объем часов	Уровень освоения
Раздел 1 Теоретические основы информационной безопасности			**48**	
Тема 1.1 Основы информационной безопасности и свойства информации	**Содержание учебного материала**		16	1,2
	1	Информация, ее источники, носители и основные характеристики информации		
	2	Основные проблемы защиты информации и системный подход к решению проблемы защиты информации		
	3	Функции подсистемы обеспечения информационной безопасности (ИБ) в структуре предприятия		
	4	Телекоммуникационные сети, протоколы сетей и методы защиты информации в сетях.		
	5	Источники конфиденциальной информации и структура правового обеспечения ИБ РФ		
	6	Стандарты в области обеспечения ИБ и их применение		
	7	Виды уязвимостей и угроз информационной безопасности.		
	8	Риски и оценка рисков в области ИБ		
	Практические занятия		16	
	1	Работа с информационно-правовой системой Консультант плюс		
	2	Работа с документами по информационной безопасности РФ		
	3	Работа с требования к безопасности информационных систем в Российской Федерации		
	4	Работа с правовыми документами, определяющими функции регулирующих органов в области обеспечения защиты информации в РФ		

	5	Работа с требованиями к безопасности каналов передачи информации		
	6	Работа с правовыми документами, определяющих принципы сокрытия информации в целях обеспечения информационной безопасности предприятия.		
	7	Работа с механизмами анализа степени серьезности угроз		
	8	Применение программных средств операционных систем (ОС) для аудита информационной безопасности		
	Самостоятельная работа обучающихся			
	Работа с учебной литературой, конспектами лекций, решение задач и выполнения упражнений		8	
	Подготовка к практическим занятиям № 1-8		8	
Раздел 2 Практические основы реализации информационной безопасности предприятия			**48**	
Тема 2.1 Угрозы информационной безопасности и меры их устранения	**Содержание учебного материала**			
	1	Модели и архитектура систем защиты в системе информационной безопасности предприятия		
	2	Типовые сценарии несанкционированного доступа к конфиденциальной информации		
	3	Криптографические механизмы обеспечения информационной безопасности		
	4	Технические средства и методы защиты информации и их применение		
	5	Программные средства и методы защиты информации и их применение	16	2, 3
	6	Организационно-административные меры защиты и их применение		
	7	Обеспечение конфиденциальности, целостности и доступности информации при организации защиты информации в персональных компьютерах.		
	8	Обеспечение конфиденциальности, целостности и доступности информации в процессе организации защиты информации при ее передаче по каналам связи		

	Практические занятия		16	
	9	Проведение тестирования состояния защищенности компьютерных систем		
	10	Применение методов криптографической защиты информации и простейших алгоритмов шифрования.		
	11	Реализация процесса защиты документов в LibreOffice и информации в архивах.		
	12	Работа с механизмами контроля целостности при передаче данных с использованием сетевых протоколов		
	13	Работа со средствами контроля целостности файлов		
	14	Работа с подсистемой парольной идентификации пользователей.		
	15	Работа с персональным межсетевым экраном компьютера		
	16	Работа с механизмами обеспечения безопасности каналов передачи информации		
	Самостоятельная работа обучающихся		8	
	Работа с учебной литературой, конспектами лекций, решение задач и выполнения упражнений			
	Подготовка к практическим занятиям № 9-16		8	
		Всего	**96**	

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 УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета, лаборатории компьютерных сетей и телекоммуникаций.

Оборудование учебного кабинета:

доска классная – 1 шт., стол письм.1-тумб. с подвесн тумб – 1 шт., стол ученический на металлокаркасе– 15 шт., стул «Изо» – 1 шт., стул ученич. на металлокаркасе– 30 шт., шкаф 2-х створчатый – 1 шт., шкаф для документов– 2 шт.

Оборудование лаборатории компьютерных сетей и телекоммуникаций и рабочих мест лабораторий:

стол преподавателя на металлокаркасе – 1 шт., кресло «Юпитер» – 2 шт., стол компьютерный на металлокаркасе левый – 4 шт., стол компьютерный на металлокаркасе правый – 10 шт., стол на металлокаркасе – 1 шт., стул СМ-9ГП – 14 шт., табурет СМ-31 – 14 шт., тележка под системный блок – 1 шт., ПК - 1 шт.: монитор 19” TFT LG Flatron L1942SE-BF, системный блок (Foxconn TSAA-700/ASRock H67DE3/Intel Core i3 2120 3.3GHz/DDR III 8Gb/WD 500Gb SATA III/D-Link DGE-528T/Gigabit Lan), ПК - 14 шт.: монитор 19” TFT LG Flatron L1942SE-BF, системный блок (Foxconn TSAA-700/ASRock H67DE3/Intel Core i3 2120 3.3GHz/DDR III 8Gb/WD 500Gb SATA III/D-Link DGE-528T/Gigabit Lan), мультимедиа-проектор Epson EB-X12, экран Screen Media GoldView MW 4*3, учебная доска, маршрутизатор D-Link Dir-320, маршрутизатор D-Link DSR-500N, маршрутизатор D-link DFL-800, маршрутизатор TP-link TL-WR743ND, коммутатор D-Link DGS-3312SR – 2шт., коммутатор D-Link DES-3528 – 8шт., LAN-тестер – 2шт., модем D-link DSL-2540u – 2шт., маршрутизатор D-link DSL-2640U – 10 шт., стойка для монтажа сетевого оборудования – 2 шт., патч-панель – 2шт., клещи обжимные – 8шт., оптические передатчики D-link – 4шт., GPON терминал Huawei Echolife HG850a – 2шт., розетки распределительные под RJ-45 – 4шт., конекторы RJ-45 – 50шт., экран сетевой анализатор – 2шт., программное обеспечение: MS Windows Server 2008 R2, MS Windows Server 2012 R2, MS Windows Server 2016, OpenVAS 8, LibreOffice 6, ОС Ubuntu Linux 14.04, VirtualBox 5, OpenSSL 1, OpenVPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2.0.2, Ossec 3.2, IredMail 0.9.9, FreeBSD 7, Asterisk 13, PhpMyAdmin 5, Wireshark 2.2.6, Zenmap 7.70, Denver 3, MySQL Workbench 6.3, Joomla 2, Notepade++ 4.0.2, GNU PG 2.

3.2 Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ. [Электронный ресурс]/Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/. - свободный.

2. Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 N 28375) [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_146520/.— свободный.

3. Баранова, Е. К. Основы информационной безопасности : учебник / Е. К. Баранова, А. В. Бабаш. — Москва : РИОР : ИНФРА-М, 2022. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - URL: https://znanium.com/catalog/product/1860126. – Режим доступа: по подписке. — Текст : электронный.

4. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А. В. Васильков, И. А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2022. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - URL: https://znanium.com/catalog/product/1836631. – Режим доступа: по подписке.— Текст : электронный.

5. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - URL: https://znanium.com/catalog/product/1189328 – Режим доступа: по подписке. Текст : электронный.

6. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2023. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - URL: https://znanium.com/catalog/product/1910870 – Режим доступа: по подписке. - Текст : электронный.

Дополнительные источники:

1. Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ФОРУМ : ИНФРА-М, 2021. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - URL: https://znanium.com/catalog/product/1189337 – Режим доступа: по подписке. - Текст : электронный.

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, устных и письменных опросов, тестирования.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Освоенные умения	
классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	**Текущий контроль:** Практические работы №№1-3,6, 12 Наблюдение Анализ Экспертная оценка
применять основные правила и документы системы сертификации Российской Федерации	**Текущий контроль:** Практические работы №№1-5 Наблюдение Анализ Экспертная оценка
классифицировать основные угрозы безопасности информации	**Текущий контроль:** Практические работы №№4,5, 7-11, 13 - 16 Наблюдение Анализ Экспертная оценка
Усвоенные знания	
сущность и понятие информационной безопасности, характеристику ее составляющих;	**Текущий контроль:** Внеаудиторная самостоятельная работа №1-9 Тестовое задание №1 (вопросы с 1 по 16) Устный и письменный вопрос
место информационной безопасности в системе национальной безопасности страны;	**Текущий контроль:** Тестовое задание №1 (вопросы с 1по 16) Внеаудиторная самостоятельная работа №1-9 Устный и письменный опрос
источники угроз информационной безопасности и меры по их предотвращению;	**Текущий контроль:** Тестовое задание №2 (вопросы с 1 по 27) Внеаудиторная самостоятельная работа №10-18 Устный и письменный опрос
современные средства и	**Текущий контроль:**

способы обеспечения информационной безопасности.	Тестовое задание №2 (вопросы с 1 по 27) Внеаудиторная самостоятельная работа №10-18 Устный и письменный опрос
	Промежуточная аттестация в форме дифференцированного зачёта