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
28 03 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности:

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

г. Архангельск
2024

Рабочая программа учебной дисциплины составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, примерной основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем и в соответствии с учебным планом по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа рассмотрена и одобрена цикловой комиссией Информационной безопасности инфокоммуникационных систем

Протокол № 7 от 28.03 2024 г.

Председатель _____ А.А. Садков

Составитель:

К.С. Ефремова, преподаватель АКТ (ф) СПбГУТ.

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Место дисциплины в структуре образовательной программы:

Учебная дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла образовательной программы в соответствии с ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2 Планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания:

Код ПК, ОК	Умения	Знания
ОК 03 ОК 06 ОК 09 ОК 10 ПК 2.1	Классифицировать защищаемую информацию по видам тайны и степеням секретности. Классифицировать основные угрозы безопасности информации.	Сущность и понятие информационной безопасности, характеристику ее составляющих. Место информационной безопасности в системе национальной безопасности страны. Виды, источники и носители защищаемой информации. Источники угроз безопасности информации и меры по их предотвращению. Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах. Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи.

		Современные средства и способы обеспечения информационной безопасности. Основные методики анализа угроз и рисков информационной безопасности.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Объем образовательной программы учебной дисциплины	**64**
Самостоятельная работа	**16**
Суммарная учебная нагрузка во взаимодействии с преподавателем	**48**
т.ч. в форме практической подготовки	**18**
в том числе:	
теоретическое обучение	28
практические занятия	18
итоговое занятие	2
Промежуточная аттестация в форме дифференцированного зачета	

2.2 Тематический план и содержание учебной дисциплины ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем часов	Коды компетенций, формированию которых способствует элемент программы
1	2		3	4
Раздел 1. Теоретические основы информационной безопасности			**36**	
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**		**6**	ОК 03, ОК 06, ОК 09, ПК.2.1
	1	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	2	
	2	Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий.	2	
	3	Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности.	2	
Тема 1.2. Основы защиты информации	**Содержание учебного материала**		**6**	ОК 03, ОК 06, ОК 09, ПК 2.1
	1	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.	2	

	2	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации.	2	
	3	Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.	2	
	Практические занятия		**6**	
	1	Работа с документами в области информационной безопасности РФ по определению объектив защиты и классификации тайн	2	
	2	Определение объектов защиты на типовом объекте информатизации.	2	
	3	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	2	
	Самостоятельная работа обучающихся		**6**	
	1	Выполнение поиска информации в документах в области информационной безопасности, связанной с классификацией тайн касательной	2	
	2	Анализ состава типовых объектив информатизации	2	
	3	Анализ устройств для обеспечения определённых классов защищенной информации	2	
Тема 1.3. Угрозы безопасности защищаемой информации.	**Содержание учебного материала**		**4**	ОК 03, ОК 06, ОК 09, ПК.2.1
	1	Понятие угрозы безопасности информации Системная классификация угроз безопасности информации.	2	
	2	Каналы и методы несанкционированного доступа к информации Уязвимости. Методы оценки уязвимости информации	2	

	Практическое занятие		**4**	
	4	Работа с документами классификации угроз и методов определения уязвимостей объектов информатизации	2	
	5	Определение угроз объекта информатизации и их классификация	2	
	Самостоятельная работа обучающихся		**4**	
	4	Работа с системой классификации угроз CVE	2	
	5	Построение вектора атак	2	
Раздел 2. Методология защиты информации			**26**	
Тема 2.1. Методологические подходы к защите информации	**Содержание учебного материала**		**2**	ОК 03, ОК 06, ОК 09, ПК 2.1
	1	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.Виды мер и основные принципы защиты информации.	2	
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание учебного материала**		**4**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1
	1	Организационная структура системы защиты информации Законодательные акты в области защиты информации.	2	
	2	Российские и международные стандарты, определяющие требования к защите информации.Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	2	
	Практическое занятие		**4**	
	6	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности РФ	2	
	7	Работа в справочно-правовой системе с нормативными и	2	

		правовыми документами по информационной безопасности Международных		
	Самостоятельная работа обучающихся		**4**	
	6	Составление требований по защите информации объекта информатизации согласно требований нормативными и правовыми документами по информационной безопасности РФ	2	
	7	Составление требований по защите информации объекта информатизации согласно требований нормативными и правовыми документами по информационной безопасности РФ	2	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала**		**6**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1
	1	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	2	
	2	Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации.	2	
	3	Организационно-распорядительная защита информации. Работа с кадрами и внутри объектовый режим. Принципы построения организационно-распорядительной системы.	2	
	Практическое занятие		**4**	
	8	Выбор мер защиты информации для автоматизированного рабочего места	2	
	9	Составление паспорта защищенного автоматизированного рабочего места	2	

	Самостоятельная работа обучающихся		**2**	
	8	Выбор программно–аппаратных средств для защиты автоматизированного места	2	
Итоговое занятие			**2**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1
Всего			**64**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Кабинет информационной безопасности, оснащенный оборудованием и техническими средствами обучения: доска классная – 1 шт., стол компьютерный– 13 шт., стул – 13 шт., компьютерные кресла – 13 шт., системный блок (CPU AMD Ryzen 7 3700x (8 Cores/32MB/8T/3.6GHz); 16 Гбайт (16 Гбайт) памяти DDR4, 2 666 МГц, без ECC; твердотельный накопитель M.2 PCIe NVMe, 512 Гбайт, класс 35) – 13 шт., монитор (Asus 23”8) – 13 шт., клавиатура (Oklick 530S) – 14 шт., мышь для компьютера (Defender OPTICAL MB-160) – 14 шт., источник бесперебойного питания – 13 шт., проектор – 1 шт., активная колонка - 1шт., офисный пакет Microsoft Office Professional 2016 - 13 шт, виртуальный межсетевой экран следующего поколения Cisco Firepower в составе с FMC- 10 шт., ОС Microsoft Windows Server - 1 шт., ОС Microsoft Windows 10 - 13 шт., сервер SuperMicro CSE-113AC2-R706WB2 2x750W black Intel Xeon Silver 4216 256 ГБ ОЗУ, 960 GB SSD - 1 шт., монитор 23,6 – 1 шт., источник бесперебойного питания для сервера - 1 шт., стойка двухрамная (стк-24.2-9005 цмо) – 1 шт., телевизор на стойке (huawei 55”) – 1 шт., экран для проектора (SAKURA CINEMA WALLSCREEN) – 1 шт., МФУ (Xerox B205) – 1 шт., ПАК Arduino - 3 шт.,Анализатор спектра IFR 2398 - 1 шт.,Электронный осциллограф IBIS-1 — 1шт.,Соболь 3.0 kb-sobol 3.0 k1 v1-SP1Y - 2 шт .,Видео регистратор jassun jsr-H0415mini - 1 шт.,Видео регистратор vesta VDRV-5004M - 1 шт.,Коммутатор Alcatel OmniStack LS 6224 - 5 шт .,Программные межсетевые экраны для маршрутизаторов Cisco 1700 (Cisco 1721) - 2 шт.,Стенд : пульт защиты помещений — 1 шт.,Стенд: исследование утечки информации по звуковым каналам — 1 шт., стойки для монтажа сетевого оборудования - 2 шт. Программное обеспечение: MS Windows Server 2008 R2, OS Debian Linux 9, Audacity 2.3, Zoneminder 1.32, Open VAS 8, LibreOffice 6, OS Ubuntu Linux 14.04, Virtual Box 5, Open SSL 1.0, Open VPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2, Ossec 3.2, IredMail 0.9.9, OS FreeBSD 11,12. Asterisk 13, PHP MyAdmin 5, Wireshark 2.2.6, Zenmap 7.7, Platinum Pack 4.0., Eset Nod32 Fire Wall 5.,Крипто Про.,RedCheck 2.0., DevieeLock 8.

Мастерская, лаборатория информационных технологий, оснащенная оборудованием и техническими средствами обучения: стол на металлокаркасе– 15 шт., стол ученический на мнталлокаркасе– 8 шт., стул ученический на металлокаркасе– 30 шт., сетевой коммутатор D-Link DGS-1016D E-net Switch (16 ports, 10/100/1000Mbps) – 1 шт., ПК - 1 шт.: монитор 19” TFT Hyundai X91D, системный блок (InWin/GA-H87-HD3/Intel Core i3-4330 3.5GHz/DDR III 4Gb/Seagate 500Gb SATA III/Gigabit Lan), ПК 14 шт.: монитор 19” TFT LG Flatron L1953S, системный блок (Foxconn TLA-397/Asus B85M-G/Intel Core i3-4170 3.7GHz/DDR III 4Gb/Seagate 500Gb/Gigabit Lan), мультимедиа-проектор (Epson EMP-821), экран (Lumien Master Picture 4*3), учебная доска,

программное обеспечение: MS Windows 7, MS Office 2007, MS Visio 2007, MS Visual Studio 2010, MS SQL Server 2008, Eset NOD32, LibreOffice 5, Foxit Reader 7, Multisim 10.1, MathCAD 2014, Adobe Flash CS3, Any Logic 7, 7-Zip, набор дистрибутивов для веб-разработки Denwer, Консультант+, RAD Studio Berlin 10.1, браузер Google Chrome, браузер MS Internet Explorer 11, KiCAD 4.0.5, Python 3.6, Free Pascal 3.0.2.Office 2013, SQL Server2012, LibreOffice 6,2, Visual Studio2012, Free Pascal 3.04.Локальная сеть с выходом в сеть Интернет и доступом к ЭБС и СДО.

Документация ФСТЭК:

1. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам, инв. № 2170дсп, экз. № 1828, 1 книга, для служебного пользования.

2. Требования к системам обнаружения вторжений, инв. № 4457дсп, экз. № 1736, 1 книга, для служебного пользования.

3. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВОСП-К), инв. № 4453дсп, экз. № 1630, 1 книга, для служебного пользования.

4. Руководящий документ. Защита информации. Комплектующие помехоподавляющие изделия электронной техники, радиоэкранирующие и помехоподавляющие материалы. Общие технические требования, инв. № 4477дсп, экз. № 409, 1 книга, для служебного пользования.

5. Требования к средствам антивирусной защиты, инв. № 4471дсп, экз. № 790, 1 книга, для служебного пользования.

6. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (с изменениями, внесенными в соответствии с Извещениями о корректировке № 1-2005, № 1-2006, № 1-2008), инв. № 5210дсп, экз. № 778, 1 книга, для служебного пользования.

7. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (Требования к средствам доверенной загрузки), инв. № 5288дсп, экз. № 619, 1 книга, для служебного пользования.

8. Требования к средствам контроля съемных машинных носителей информации, инв. № 5550дсп, экз. № 542, 1 книга, для служебного пользования.

3.2 Информационное обеспечение реализации программы

3.2.1. Основные печатные и электронные издания:

1. 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: для зарегистрир.пользователей. - Текст : электронный.

2. Бубнов, А.А. Основы информационной безопасности (3-е изд.) : учебник / А.А. Бубнов. - Москва: Академия, 2020.

3. Ильин, М.Е. Криптографическая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник. / М.Е. Ильин. - Москва: Академия, 2020.

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.

3.2.2. Дополнительные источники:

1. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - URL: https://znanium.com/catalog/product/1082470 – Режим доступа: для зарегистрир.пользователей. - Текст : электронный.

2. Зверева, В. П. Организация и технология работы с конфиденциальными документами : учебник / В. П. Зверева, А. В. Назаров. — Москва : КУРС : ИНФРА-М, 2020. - 320 с. - (Среднее профессиональное образование). - ISBN 978-5-906818-96-6. - URL: https://znanium.com/catalog/product/1078083 – Режим доступа: для зарегистрир.пользователей. - Текст : электронный.

3. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - URL: https://znanium.com/catalog/product/1898839 – Режим доступа: по подписке. - Текст : электронный.

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
Перечень знаний, осваиваемых в рамках дисциплины: - сущность и понятие информационной безопасности, характеристику ее составляющих; - место информационной безопасности в системе национальной безопасности страны; - виды, источники и носители защищаемой информации; - источники угроз безопасности информации и меры по их предотвращению; - факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; - жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	Характеристики демонстрируемых знаний Оценка знаний осуществляется по пятибалльной шкале.	– тестирование; – письменный опрос; – устный опрос; - устное собеседование по теоретическому материалу; – оценка результатов выполнения практических работ №№1-9; – дифференцированный зачет

- современные средства и способы обеспечения информационной безопасности; - основные методики анализа угроз и рисков информационной безопасности.		
Перечень умений, осваиваемых в рамках дисциплины: - классифицировать защищаемую информацию по видам тайны и степеням секретности; - классифицировать основные угрозы безопасности информации.	Характеристики демонстрируемых умений Оценка умений осуществляется по пятибалльной шкале.	– оценка результатов выполнения практических работ №№1-9; – оценка результатов выполнения самостоятельной работы; – дифференцированный зачет