ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ
КОЛЛЕДЖ СВЯЗИ № 54
ИМЕНИ П.М. ВОСТРУХИНА

РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Москва

2017

РЕКОМЕНДОВАНА	УТВЕРЖДАЮ
Методической цикловой комиссией	Зам. директора по УМР
Протокол №__ от «__»_____ 2017 г.	ГБПОУ КС № 54
Председатель ПЦК	_____ И.Г. Бозрова
_____ В.П. Шаманин	«___»_____2017 г.

Разработчики:
Пешкина О.В., преподаватель спецдисциплин

Ф.И.О., должность

Рецензенты:

Ф.И.О., должность

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

Информационная безопасность телекоммуникационных систем

1.1. Область применения программы

Программа междисциплинарного курса(далее примерная программа) – является частью примерной основной профессиональной образовательной программы в соответствии с ФГОС по специальности **090303 Информационная безопасность телекоммуникационных систем** (базовой подготовки) в части освоения основного вида профессиональной деятельности (ВПД): **Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем** и соответствующих профессиональных компетенций (ПК):

1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно - аппаратных и инженерно - технических средств обеспечения информационной безопасности телекоммуникационных систем.

2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно - аппаратных и инженерно - технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению.

3. Формулировать предложения по применению программно- аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем.

4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей.

Примерная программа междисциплинарного курсаможет быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области защиты информации в телекоммуникационных сетях и конвергентных системах при наличии среднего (полного) общего образования. Опыт работы не требуется.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- применения инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем;

- применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
- выявления технических каналов утечки информации;

уметь:

– выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;
– определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
– проводить типовые операции настройки средств защиты операционных систем;
– применять технические методы и средства защиты информации на выделенных объектах;
– использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов;
– организовывать безопасный доступ к информационным ресурсам информационно- телекоммуникационной системы;
– производить установку и настройку типовых программно-аппаратных средств защиты информации;
– пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
– осуществлять установку, настройку и обслуживание технических средств защиты информации и средств охраны объектов;
– решать частные технические задачи при аттестации объектов, помещений, технических средств;
– обнаруживать и обезвреживать разрушающие программные воздействия с использованием программных средств;
– осуществлять настройку, регулировку и ремонт оборудования средств защиты;

знать:

- основные положения системного подхода к технической защите информации;
- основные технические каналы утечки защищаемой информации в автоматизированных и телекоммуникационных системах, физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности;
- порядок проведения работ по технической защите информации;
- типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
- основные протоколы идентификации и аутентификации в телекоммуникационных системах;
- состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;

- особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;
- основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;
- основные понятия криптографии и типовые криптографические методы защиты информации;
- основные технические методы и средства защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам, средств охраны и безопасности объектов;
- назначение, принципы работы и правила эксплуатации технических средств и систем, аппаратуры контроля, защиты и другого оборудования, используемого при проведении работ по защите информации;
- правила применения, эксплуатации и обслуживания технических средств защиты информации.

1.3. Рекомендуемое количество часов на освоение программы междисциплинарного курса:

максимальной учебной нагрузки обучающегося 171 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося 114часов;

самостоятельной работы обучающегося 57 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МЕЖДИСЦИПЛИНАРНОГО КУРСА

Результатом освоения программы междисциплинарного курса является овладение обучающимися видом профессиональной деятельности (ВПД) **Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 1.	Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем
ПК 2.	Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению
ПК 3.	Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем
ПК 4.	Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности
ОК 2.	Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3.	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях
ОК 4.	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития
ОК 5.	Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности
ОК 6.	Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями

ОК 7.	Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9.	Быть готовым к смене технологий в профессиональной деятельности
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)
ОК 11.	Формулировать задачи логического характера и применять средства математической логики для их решения
ОК 12.	Понимать физическую сущность задач, возникающих в ходе профессиональной деятельности, и применять соответствующий физический аппарат для их решения
ОК 13.	Использовать вычислительную технику и прикладные программные пакеты для решения профессиональных задач
ОК 14.	Ориентироваться в элементной базе устройств телекоммуникационных систем и обеспечения их информационной безопасности

3. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

3.1. Тематический план междисциплинарного курса

Коды профессиональных компетенций	**Наименования разделов МЕЖДИСЦИПЛИНАРНОГО КУРСА***	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов *(если предусмотрена рассредоточенная практика)*
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., курсовая работа (проект),** часов		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ПК 1-3	Криптографическая защита информации	**171**	**114**	**60**	**-**	**57**	**-**	**-**	**-**

* Раздел профессионального модуля – часть примерной программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

** Производственная практика (по профилю специальности) может проводиться параллельно с теоретическими занятиями междисциплинарного курса (рассредоточено) или в специально выделенный период (концентрированно).

3.2. Содержание обучения по междисциплинарного курса (МДК)

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работ обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
МДК 01. Криптографическая защита информации			**171**	
Тема 1.1 Основные понятия и определения современной криптографии	**Содержание учебного материала**		4	1
	1	**Базовые криптографические понятия.** Основные понятия и определения современной криптографии		
	2	**Классическая и математическая криптография.** Стойкость криптографических схем. Правило Керкхоффса. Расстояние единственности. Криптографические задачи		
	Самостоятельная работа		6	
	1	Сравнительный анализ классической и математической криптографии. Решение задач по оценки стойкости современного шифра. Исследование многоразового шифроблокнота.		
Тема 1.2 История криптографии	**Содержание учебного материала**		4	1
	1	**Эпоха донаучной криптографии.** Шифр Гай Юлия Цезаря. Шифр перестановки Сцитала. Диск Энея. Квадрат Полибия. Шифр Чейза. Тюремный шифр. Магические квадраты. Шифр Аве Мария. Таблица Тритемия. Шифр Бэкона. Шифровальный диск Альберти. Шифры Порта. Шифр Кордано и Решелье. Шифр Фальконера. Шифр Кеплера и Галилея.		
	2	**Криптография XX века.** Роторные шифровальные машины(Lorenz, Энигма). Шифр Lucifer. Шифр DES, RSA.		
	Практические занятия		2	
	1	Использование криптографических средств шифрование древних времен		

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
	Самостоятельная работа обучающихся		4	
	1	Подготовить эссе по истории криптографии. Составление хронологической таблицы.		
Тема 1.3 Симметричные криптосистемы	**Содержание учебного материала**		**52**	**2**
	1	**Шифрование методом замены (подстановки)** Область применения метода шифрования заменой. Порядок шифрования и расшифрования методом замены. Схема шифрования Вижинера. Порядок и последовательность шифрования и расшифровки по таблице Вижинера. Метод шифрования монофонической заменой. Методы одноалфавитной и многоалфавитной подстановки. Одноразовые блокноты.	12	
	2	**Шифрование методом перестановки** Основные принципы шифрования методом перестановки. Разновидности шифрования методом перестановки, используемые в автоматизированных системах. Применение метода перестановки с ключом. Применение метода шифрования перестановки колонок с пропусками. Шифрование перестановкой по маршрутам Гамильтона.		
	3	**Шифрование методом гаммирования** Суть шифрования методом гаммирования, область его применения. Порядок применения методов шифрования гаммированием с конечной и бесконечной гаммами. Метод гаммирования двоичного текста.		**2**

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
	4	**Алгоритм симметричного шифрования DES, AES** Криптографический стандарт DES. Принцип работы алгоритма DES. Режимы работы алгоритма DES. Тройной DES. Криптографический стандарт AES. Принцип работы алгоритма AES. Режимы работы алгоритма AES. Расширенный стандарт шифрования Rijndael.		**2**
	5	**Блочные и поточные криптосистемы.** Режим электронной шифровальной книги Режим сцепления блоков шифра Биграммный шифр Плейфера. Поточные криптосистемы		**2**
	6	**Отечественный стандарт шифрования** Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования		**2**
	Лабораторные работы		18	
	1	Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации.		
	2	Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей		
	3	Изучение устройства и принципы работы шифровальной машины «Энигма»		
	4	Сеть Фейстеля.		

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
	5	Генерация псевдослучайных чисел		
	6	Изучение стандарта симметричного шифрования AESRIJNDAEL		
	7	Шифрование методом скользящей перестановки		
	8	Дешифрование шифра простой перестановки при помощи метода Биграмм.		
	9	Шифр Плейфера.		
	Практические работы		10	
	2	Решение криптографических задач методами замены и перестановки и блочным шифром		
	3	Решение криптографических задач методом гаммирования		
	4	Использование стандартов криптосистемы DES		
	5	Использование стандартов криптосистемы AES		
	6	Использование стандартов криптосистемы ГОСТ		
	Самостоятельная работа		12	
	1	Оценка и сравнение различных методов шифрования по криптологической стойкости (составить сводную таблицу)		
	2	Решение задач по шифрованию и дешифрованию с применением различных алгоритмов.		
	3	Выполнение заданий по лабораторным работам, оформление отчетной документации		
Тема 1.4 Ассиметричные криптосистемы	**Содержание учебного материала**		**22**	
	1	**Алгоритм Диффи-Хеллмана.** Реализация процедуры шифрования с открытым ключом. Использование алгоритмов криптосистемы с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана.	4	**2**

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
	2	**Алгоритм RSA** Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.		**2**
	Лабораторные работы		6	
	10	Генерация простых чисел, используемых в ассиметричных системах шифрования		
	11	Реализация криптосистемы RSA		
	12	Реализация криптосистемы Эль-Гамаля		
	Практические работы		6	
	7	Решение криптографических задач по алгоритму Диффи-Хеллмана		
	8	Решение криптографических задач по алгоритму Эль-Гамаля		
	9	Решение криптографических задач по алгоритму RSA		
	Самостоятельная работа		6	
	1	Решение криптографических задач по ассиметричным криптосистемам		
	2	Выполнение заданий по лабораторным и практическим работам, оформление отчетной документации		
Тема 1.5. Схема электронной подписи	**Содержание учебного материала**		**18**	
	1	**Алгоритм цифровой подписи DSA. Новые стандарты ЭЦП** Параметры схемы цифровой подписи Реализация алгоритма DSA Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи	8	**2**
	2	**Инфраструктура открытых ключей PKI** Основные компоненты PKI Архитектуры PKI Примеры использования PKI		**2**

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
	3	**ЭЦП.** Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты.		**2**
	4	**Отечественный стандарт цифровой подписи.**		**2**
	Практические работы		4	
	10	Реализация цифровой подписи на основе криптосистемы Эль-Гамаля, RSA, Шамира		
	11	Реализация цифровой подписи на основе ГОСТ 334.10-2012		
	Самостоятельная работа		6	
	1	Решение задач по ЭЦП		
	2	Подготовка к тестированию по теме 2.3.		
	3	Выполнение заданий по лабораторным и практическим работам, оформление отчетной документации		
Тема 1.6 Стеганография	**Содержание**		**16**	
	1	**Основные методы стеганографии.** Введение в стеганографию.	4	
	2	**Принципы компьютерной стеганографии.** Простейшие примеры стеганографии. Недостатки и проблемы компьютерной стеганографии.		**2**
	Лабораторные работы		6	
	13	Защита программного обеспечения методами стеганографии		
	14	Защита электронных документов с использованием цифровых водяных знаков		
	15	Стегокомплексы, допускающие использование аудиоконтейнеров, на примере программы InvisibleSecrets		

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
	Самостоятельная работа		6	
	1	Подготовка докладов по современным методам компьютерной стеганографии		
	2	Выполнение заданий по лабораторным работам, оформление отчетной документации		
	3	Подготовка к тестированию по теме 2.4.		
Тема 1.7 Криптографические протоколы	**Содержание учебного материала**		**10**	
	1	Основы криптографических протоколов **Протоколы аутентификации.** **Протоколы распределения ключей.** Протоколы образования защищенных каналов передачи данных.	10	**2**
	2	**Протоколы электронной подписи** Протокол конфиденциальной подписи. Протокол мультиподписи. Протокол групповой подписи. Протокол подписи вида онлайн/офлайн Протокол подписи с ограниченным жизненным циклом Протокол затемненной подписи		**2**
	3	**Банковские криптографические протоколы** Электронные платежи Электронные монеты Электронные бумажники		
	4	**Протоколы конфиденциальных вычислений** Общие модели конфиденциальности Пример протокола конфиденциального вычисления		

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
	Практические работы		8	
	12	Использование криптографических протоколов аутентификации и распределения ключей		
	13	Использование криптографических протоколов электронной подписи		
	14	Использование криптографических протоколов электронных платежей		
	15	Использование криптографических протоколов конфиденциальных вычислений		
	Самостоятельная работа		10	
	1	Анализ достоинств и недостатков криптографических протоколов		
	2	Выполнение заданий по лабораторным и практическим работам, оформление отчетной документации		
Тема 1.8 Документация и инновации в сфере криптографической защиты данных	**Содержание**		15	2
	1	**Нормативное обеспечение в области криптографической защиты информации** Законодательство Российской Федерации о нормативном регулировании криптографической защиты информации. Нормативные правовые акты и документы, определяющие технические требования в криптографической сфере.	8	
	2	**Отечественные программные продукты криптографической защиты информации** Организации, осуществляющие разработку средств криптографической защиты информации. Линейка продуктов «КриптоПро». Средства криптографической защиты информации «Крипто БД». Продукция ОАО «ИнфоТеКС». Продукция ФГУП «НТЦ «Атлас».		

Наименование разделов междисциплинарного курса(ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
	3	**Квантовая криптография.** Квантовые коммуникационные технологии. Технологии квантовой обработки информации. Технологии квантовых вычислений. Постквантовая криптография. Современные этапы развития прикладной квантовой криптографии.		
	4	**Нелинейные системы на службе защиты данных.** Практическая составляющая нелинейной системы защиты информации.		
	Самостоятельная работа		7	
	1	Анализ достоинств и недостатков криптографических продуктов		
	2	Подготовка к тестированию по теме 4.1.		
Итого- 171 час (114-аудиторных, 57 – самостоятельных)				

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)

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

4 . 1 . Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие учебной лаборатории «Информационной безопасности».

Оборудование лаборатории и рабочих мест лаборатории «Информационной безопасности»:

программно-аппаратные средства защиты информации в открытых системах, криптографические средства защиты информации, технические средства защиты от НСД по техническим каналам утечки информации, устройства обнаружения и подавления средств негласного съёма информации в телекоммуникационных сетях, комплект учебно-методической документации.

Реализация программы модуля предполагает обязательную производственную практику, которую рекомендуется проводить концентрированно.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

Учебники:

1. Васильева И.Н. Криптографические методы защиты информации М.: Юрайт, 2016
2. Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации М.: Юрайт,2015
3. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность: учебное пособие, 6-е издание – М.: Академия, 2011.
4. Партыка Т.Л., Попов И.И. Информационная безопасность – М.: Форум, 2011.
5. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. – М.: Телеком, 2005.
6. Арутюнов В. В. Защита информации. – М.: Либерея, 2008.
7. Корнеев И. К., Степанов Е. А. Защита информации в офисе. – М.: Проспект, 2010.
8. Кузнецов А. А. Защита деловой информации. – М.: Экзамен, 2008.
9. Куприянов А. И., Шевцов В. А., Сахаров А. В. Основы защиты информации. – М.: Академия, 2008.
10. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие. – М.: Форум, 2009.

Дополнительные источники:

Учебники и учебные пособия:

1. Ярочкин В.И. Информационная безопасность - Гаудеамус, 2004.
2. Гришина Н. В. Комплексная система защиты информации на предприятии. – М.: Форум, 2009.
3. Галатенко В.А. Основы информационной безопасности: учебное пособие - Интернет-Университет Информационных Технологий, www.intuit.ru, 2004.
4. Байбурин В.Б. Введение в защиту информации: учебное пособие. – М.: Форум, 2004.
5. Емельянова Н.З., Партыка Т. Л., Попов И. И. Защита информации в персональном компьютере: учебное пособие. – М.: Форум, 2009.
6. Шепитько Г., Гудов Г., Локтев А. Комплексная система защиты информации на предприятии. – М.: МФА, 2008.
7. Шумский А. А., Шелупанов А. А. Системный анализ в защите информации. – М.: Гелиос АРВ, 2005.
8. Доминик Байер. Microsoft ASP .NET. Обеспечение безопасности. – СПб.: Русская Редакция, 2008.

Интернет ресурсы:

http://window.edu.ru/
http://arhidelo.ru/
http://www.winline.ru/
http://www.mirash.ru/
http://www.fstec.ru/
http://www.gtk.lissi.ru/
http://otdel-k-tula.ru/
http://bre.ru/
http://iso27000.ru/
http://ru.wikipedia.org

4.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках междисциплинарного курса«Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем» является освоение учебной практики для получения первичных профессиональных навыков в рамках междисциплинарного курса«Выполнение работ по профессии техник по защите информации», а так же предварительное изучение дисциплины «Компьютерное моделирование» и дисциплин общепрофессионального цикла: «Цепи и сигналы электросвязи», «Теория электрических цепей», «Электронная техника», «Теория электросвязи», «Основы телекоммуникаций». При работе над курсовой работой (проектом) обучающимся оказываются консультации.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по

междисциплинарному курсу (курсам): наличие высшего профессионального образования, соответствующего профилю модуля «Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем» и специальности «Информационная безопасность телекоммуникационных систем».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин: «Теория электрических цепей»; «Электронная техника»; «Теория электросвязи»; «Вычислительная техника»; «Электрорадиоизмерения»; «Основы телекоммуникаций».

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МЕЖДИСЦИПЛИНАРНОГО КУРСА(ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем	- установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов; - установка и настройка типовых программно-аппаратных средств защиты информации; - обоснованность использования программно-аппаратных и инженерно-технических средств в соответствии с рекомендациями ФСТЭК и РОСКОМНАДЗОРа.	*Текущий контроль в форме:* *- защита лабораторных и практических работ;* *- тестирование с использованием дифференцированного метода.* *Комплексный экзамен по модулю.* *Зачеты по производственной практике и по каждому из разделов МЕЖДИСЦИПЛИНАРНОГО КУРСА.* *Защита курсового проекта.*
Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению	- настройка, регулировка и ремонт оборудования средств защиты; - целесообразный выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой; - проведение типовых операции настройки средств защиты операционных систем; - знание особенностей применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах.	

Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем	- точность и грамотность проведения аттестации объектов защиты; - точность определения источников несанкционированного доступа, исходя из модели угроз; - точность в определении типа сигнала и технического средства в соответствии с алгоритмом программного продукта; - целесообразность использования программно-аппаратных и инженерно-технических средств в соответствии с рекомендациями ФСТЭК РОССИИ и РОСКОМНАДЗОРа; - обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств; - защищённость телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК; - защищённость информации организационными методами в соответствии с инструкциями на объекте; - соблюдение нормативно-правовых аспектов по защите информации в создании модели угроз объекта защиты.	

Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей	- знание номенклатуры применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам, средств охраны и безопасности объектов; - правильное применение, эксплуатация и обслуживание технических средств защиты информации; - правильное ведение и своевременное заполнение рабочей технической документации по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем.	

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности	– демонстрация интереса к будущей профессии; – участие в работе научного студенческого общества, конкурсах профессионального мастерства; – стремление к развитию в профессиональной деятельности.	*Наблюдение*

Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	– выбор и применение методов и способов решения профессиональных задач в области защиты информации в телекоммуникационных сетях; – оценка эффективности и качества выполнения мероприятий по защите информации.	*Наблюдение, экспертная оценка*
Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях	– решение стандартных и нестандартных профессиональных задач в области защиты информации; – своевременность и эффективность принятых решений; – скорость и правильность принятия решения в нестандартной ситуации.	*Наблюдение, экспертная оценка*
Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития	– эффективный поиск необходимой информации для эффективного выполнения профессиональных задач использование различных источников, включая электронные; – анализ инноваций, используемых при решении профессиональных задач; – стремление к профессиональному росту; – эффективный анализ информации и своевременная постановка и решение задачи.	*Анализ отчетов по самостоятельной работе. Практические работы.*
Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности	– работа с программно-аппаратными средствами защиты информации; – работа с инженерно-техническими средствами защиты информации; – работа с криптологическими средствами защиты информации; – оценка эффективности использования информационно-коммуникационных технологий в профессиональной деятельности	*Практические работы*
Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями	– взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения; – соблюдение норм культуры делового общения;	*Наблюдение, экспертная оценка*

	– понимание технического языка.	
Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий	– самоанализ и коррекция результатов собственной работы; – самосовершенствование; – рефлексия.	*Наблюдение, экспертная оценка. Анализ отчетов по самостоятельной работе*
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	– организация самостоятельных занятий при изучении МЕЖДИСЦИПЛИНАРНОГО КУРСА; – составление траектории собственного развития; – стремление к саморазвитию и росту в профессиональной деятельности.	*Анализ отчетов по самостоятельной работе, наблюдение*
Быть готовым к смене технологий в профессиональной деятельности	– анализ инноваций в области технических средств защиты от НСД; – выбор наиболее эффективных технологий для решения профессиональных задач.	*Анализ отчетов по самостоятельной работе*
Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)	– соблюдение техники безопасности – применение профессиональных умений и навыков для решения поставленных задач.	*Наблюдение, экспертная оценка*
Формулировать задачи логического характера и применять средства математической логики для их решения	– организация самостоятельной подготовки по совершенствованию логического мышления; – применение средств математической логики для решения задач; – решение частных задач в области информационной безопасности.	*Анализ отчетов по самостоятельной работе*
Понимать физическую сущность задач, возникающих в ходе профессиональной деятельности, и применять соответствующий физический аппарат для их решения	– понимание физических процессов, происходящих при реализации задач информационной безопасности; – эффективный анализ физических полей, несущих информацию.	*Наблюдение, экспертная оценка*
Использовать вычислительную технику и прикладные программные пакеты для решения профессиональных задач	– анализ инноваций в области компьютерных технологий; – эффективное применение программно-аппаратных средств для решения задач по информационной безопасности;	*Наблюдение, практические работы*

	– стремление к профессиональному росту и совершенствованию знаний.	
Ориентироваться в элементной базе устройств телекоммуникационных систем и обеспечения их информационной безопасности	– организация самостоятельных дополнительных занятий по углубленному изучению элементной базы; – профессиональный интерес к структуре и элементному наполнению технических средств защиты информации.	*Наблюдение, экспертная оценка*