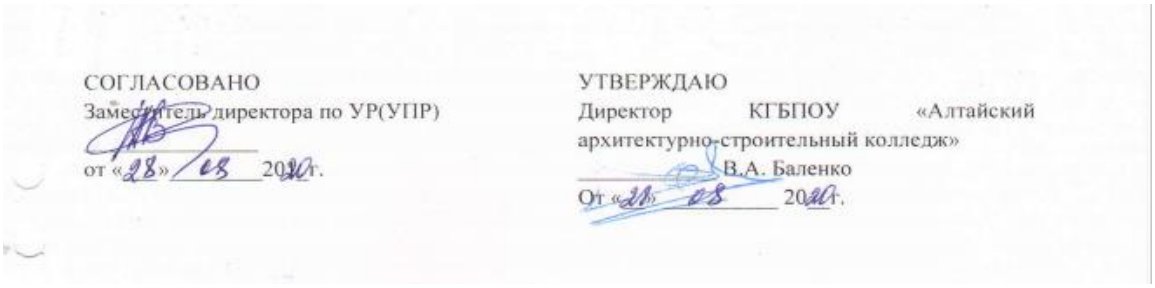
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ АЛТАЙСКОГО КРАЯ

Краевое государственное бюджетное профессиональное образовательное учреждение «Алтайский архитектурно-строительный колледж»



Программа дополнительного профессионального образования

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Защита персональных данных

Уровень квалификации _____ _____

Срок обучения: 6 недель

Форма обучения: очная, заочная

Барнаул -2020

Аннотация программы повышения квалификации

«Защита персональных данных»

Программа дополнительного профессионального образования повышения квалификации «Защита персональных данных» разработана на основе:

Профессионального стандарта "Специалист по технической поддержке информационно-коммуникационных систем", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 5 октября 2015 г. № 688н (зарегистрирован Министерством юстиции Российской Федерации 22 октября 2015 г., регистрационный № 39412)

Федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности 11.02.15 «Инфокоммуникационные сети и системы связи», утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1547 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44945) (далее – ФГОС СПО).

Рабочая программа дополнительного профессионального образования повышения квалификации «Защита персональных данных» предусматривает использование электронного обучения и дистанционных образовательных технологий.

Организация-разработчик:

Краевое государственное бюджетное профессиональное образовательное учреждение «Алтайский архитектурно-строительный колледж».

Составители:

Захарова А.В., преподаватель специальных дисциплин КГБПОУ «Алтайский архитектурно-строительный колледж»

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативно-правовую основу разработки образовательной программы дополнительного профессионального образования – программы повышения квалификации «Защита персональных данных» составляют:

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Приказа Министерства образования и науки РФ от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

Порядок применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ, утвержденный приказом Минобрнауки России от 23.08.2017 № 816 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

Профессионального стандарта "Специалист по технической поддержке информационно-коммуникационных систем", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 5 октября 2015 г. № 688н (зарегистрирован Министерством юстиции Российской Федерации 22 октября 2015 г., регистрационный № 39412)

Федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности 11.02.15 «Инфокоммуникационные сети и системы связи», утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1547 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44945) (далее – ФГОС СПО).

Методическую основу разработки образовательной программы составляют:

-Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов, утвержденные министром образования и науки Российской Федерации 22.01.2015 № ДЛ-1/05вн;

-Письмо от 22 апреля 2015 г. №ВК-1032/06 «О направлении методических рекомендаций».

Содержание программы представлено пояснительной запиской, учебным планом, рабочими программами учебных предметов, планируемыми результатами освоения программы, условиями реализации программы, системой оценки результатов освоения программы, учебно-методическими материалами, обеспечивающими реализацию программы.

Учебный план содержит перечень разделов и тем с указанием времени, отводимого на

освоение тем, включая время, отводимое на теоретические и практические занятия.

Объем программы составляет 72 академических часа.

При реализации дополнительной профессиональной программы могут быть применены дистанционные образовательные технологии, электронное обучение и традиционное обучение.

Образовательная деятельность слушателей при освоении программы предусматривает следующие виды учебных занятий: лекционные и практические занятия, итоговую аттестацию. При реализации программы академический час устанавливается продолжительностью 45 минут.

Программа повышения квалификации имеет модульную структуру. Программа состоит из модулей, которые могут быть впоследствии зачтены при освоении дополнительных профессиональных программ профессиональной переподготовки, имеющих в учебном плане модули аналогичного содержания и трудоемкости. При поступлении на обучение по программе повышения квалификации обучающемуся могут быть зачтены изученные ранее модули аналогичного содержания и трудоемкости, при условии предоставления документа о квалификации, содержащего сведения об освоении данных модулей в составе программ повышения квалификации или программ профессиональной переподготовки.

Условия реализации программы содержат организационно-педагогические, кадровые, информационно-методические и материально- технические требования. Учебно-методические материалы обеспечивают реализацию программы.

Программа предусматривает достаточный для формирования, закрепления и развития практических навыков и компетенций объем практик.

Данная программа может быть использована для разработки адаптированной образовательной программы профессионального обучения - программы повышения квалификации лиц с ограниченными возможностями здоровья.

Освоение программы повышения квалификации завершается итоговой аттестацией слушателей в форме зачета. При освоении дополнительной профессиональной программы параллельно с получением среднего профессионального образования и (или) высшего образования удостоверение установленного образца о повышении квалификации выдаются одновременно с получением соответствующего документа об образовании и о квалификации.

Рабочая программа дополнительного профессионального образования повышения квалификации «Защита персональных данных» предусматривает использование электронного обучения и дистанционных образовательных технологий.

Программа разработана с учетом требований профессиональных стандартов.

2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

2.1. Цель реализации программы

Целью реализации программы является формирование общих и профессиональных компетенций, предусмотренных Федеральным государственным образовательным стандартом среднего профессионального образования (ФГОС СПО) по специальности 11.02.15 «Инфокоммуникационные сети и системы связи», утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1547 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44945) и совершенствование профессиональных знаний, умений и навыков, по уже имеющейся специальности «Инфокоммуникационные сети и системы связи», вида профессиональной деятельности «Техническая эксплуатация инфокоммуникационных сетей связей», предусмотренного профессиональным стандартом "Специалист по технической поддержке информационно-коммуникационных систем", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 5 октября 2015 г. № 688н (зарегистрирован Министерством юстиции Российской Федерации 22 октября 2015 г., регистрационный № 39412)

2.2. Планируемые результаты обучения

Виды деятельности	Профессиональные компетенции или трудовые функции	Практический опыт	Умения	Знания
Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи	ПК 3.1 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2 Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.	- выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности; - разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; - осуществления	классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей,	принципы построения информационно-коммуникационных сетей; международные стандарты информационной безопасности для проводных и беспроводных сетей; нормативно - правовые и законодательные акты в области

	ПК 3.3 Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования..	текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	корпоративных сетей; определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи; осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выполнять тестирование систем с целью определения уровня защищенности; определять оптимальные способы обеспечения информационной безопасности; проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;	информационной безопасности; акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия; технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия; способы и методы обнаружения средств съёма информации в радиоканале; классификацию угроз сетевой безопасности; характерные особенности сетевых атак; возможные способы несанкционированного доступа к системам связи; правила проведения возможных проверок согласно нормативных документов ФСТЭК; этапы определения

			проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации; разрабатывать политику безопасности сетевых элементов и логических сетей; выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи; конфигурировать автоматизированные системы и информационно-	конфиденциальности документов объекта защиты; назначение, классификацию и принципы работы специализированного оборудования; методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2; методы и средства защиты информации в телекоммуникациях от вредоносных программ; технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов; методы и способы защиты информации, передаваемой по кабельным направляющим системам; конфигурации защищаемых сетей; алгоритмы работы тестовых программ; средства защиты различных операционных

			коммуникационные сети в соответствии с политикой информационной безопасности; защищать базы данных при помощи специализированных программных продуктов; защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.	систем и среды передачи информации; способы и методы шифрования (кодирование и декодирование) информации.

2.3. Категория обучающихся

К освоению дополнительных профессиональных программ допускаются: лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование.

2.4. Срок обучения

Трудоемкость обучения по данной программе - 72 часа, включая все виды аудиторной работы, практической работы и итоговую аттестацию. Общий срок обучения - 6 недель.

2.5. Форма обучения

Форма обучения – очная, заочная с использованием электронного обучения и дистанционных образовательных технологий

2.6. Режим занятий

По 4 часа в день, 3 раза в неделю.

3. СОДЕРЖАНИЕ ПРОГРАММЫ

3.1. Учебный план

Основным документом программы является учебный план. Учебный план определяет перечень, трудоемкость, последовательность и распределение учебных предметов, курсов, дисциплин (модулей), практик и иных видов учебной деятельности обучающихся, а также указание видов аттестации.

При реализации программы перечисленные модули могут изучаться как в традиционной, так и дистанционной форме.

Наименование модуля	Объем модуля, час			Форма контроля (устный опрос, КР, тесты и т.д.)
	Всего	В том числе,		
		Лекции	Практические занятия	
1	*2*	*3*	*4*	*6*
Модуль 1. Правовое, нормативное и методическое обеспечение безопасности персональных данных.	12	12	-	модульное тестирование
Модуль 2. Угрозы безопасности персональных данных, уязвимости информационных систем персональных данных.	6	6	-	модульное тестирование
Модуль 3. Организация обработки персональных данных.	26	4	22	выполнение практических заданий
Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	18	10	8	выполнение практических заданий
Модуль 5. Особенности обработки персональных данных без использования средств автоматизации.	6	4	2	выполнение практических заданий
Итоговая аттестация	4	-	-	зачет
Итого	**72**	**36**	**32**	

3.2. Календарный учебный график

№ п/п	Наименование модуля	Учебные недели и нагрузка, в часах					
		1 неделя	**2 неделя**	**3 неделя**	**4 неделя**	**5 неделя**	**6 неделя**
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Модуль 1. Правовое, нормативное и методическое обеспечение безопасности персональных данных.	12					
2	Модуль 2. Угрозы безопасности персональных данных, уязвимости информационных систем персональных данных.		6				

3	Модуль 3. Организация обработки персональных данных.		6	12	8		
4	Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.				4	12	2
5	Модуль 5. Особенности обработки персональных данных без использования средств автоматизации.						6
6	*Итоговая аттестация*						4
	Недельная нагрузка	**12**	**12**	**12**	**12**	**12**	**12**
Всего часов: 72 часа.							
Количество недель обучения: 6 недель.							

3.3. Учебная программа дисциплины

Наименование модулей, разделов (дисциплин) и тем	**Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, учебной практики, используемых образовательных технологий и рекомендуемой литературы**	**Количество часов**
Модуль 1. Правовое, нормативное и методическое обеспечение безопасности персональных данных.	***Содержание***	**12**
	Вводная лекция. Структура и содержание курса. Актуальность проблемы обеспечения безопасности персональных данных, обрабатываемых в информационных системах организации.	
	Основные понятия термины и определения. Правовое, нормативное и методическое регулирование деятельности в области обеспечения безопасности персональных данных.	
	Содержание и основные положения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».	
	Специальные нормативные документы по технической защите информации ограниченного доступа и обеспечению безопасности персональных данных.	
	Правовое, нормативное и методическое регулирование использования средств криптографической защиты информации.	
	Ответственность за нарушение требований по обеспечению безопасности персональных данных. Модульное тестирование	
Модуль 2. Угрозы	***Содержание***	**6**

безопасности персональных данных, уязвимости информационных систем персональных данных.	Общие положения и классификация угроз безопасности персональных данных.	
	Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации.	
	Угрозы программно-математических воздействий и нетрадиционных информационных каналов. Модульное тестирование	
Модуль 3. Организация обработки персональных данных.	***Содержание***	**26**
	Общий порядок организации обработки персональных данных.	
	Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных.	
	В том числе практических занятий	**22**
	№1 Разработка проекта Приказа о назначении сотрудника ответственного за организацию обработки персональных данных.	
	№2 Разработка Должностной инструкции ответственного за организацию обработки персональных данных.	
	№3 Разработка типовой формы ответа оператора на запрос субъекта персональных данных.	
	№4 Разработка проекта Приказа о назначении комиссии по приведению деятельности Организации в соответствие с требованиями Федерального закона «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.	
	№5 Разработка Плана приведения процесса обработки персональных данных, обрабатываемых в ИС организации в соответствии с требованиями 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.	
	№6 Разработка Анкеты для определения перечня, категории и объёма обрабатываемых персональных данных.	
	№7 Разработка Перечня персональных данных, обрабатываемых в информационных системах оператора.	
	№8 Разработка Перечня должностей сотрудников, допущенных к обработке персональных данных в организации.	
	№9 Разработка Положения об обработке персональных данных в организации.	
	№10 Разработка Типовой формы согласия на обработку персональных данных иных субъектов персональных данных.	
	№11 Разработка проекта Приказа о вводе в действие комплекта документов, регламентирующих обработку персональных данных в организации.	
	№12 Разработка Протокола оценки вреда, который может быть причинён субъектам персональных данных.	
	№13 Разработка уведомления об обработке персональных данных.	

Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.доступа.	***Содержание***	**18**
	Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных.	
	Разработка Частной модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных организации.	
	Определение уровня защищённости персональных данных.	
	Состав и содержание мер по обеспечению безопасности персональных данных.	
	Особенности использования средств криптографической защиты информации в рамках построения системы защиты персональных данных в организации.	
	В том числе практических занятий	**8**
	№14 Разработка Частной модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных организации.	
	№15 Определение уровня защищённости персональных данных, обрабатываемых в информационных системах персональных данных организации.	
	№16 Определению базового набора мер по обеспечению безопасности персональных данных для заданного уровня защищённости персональных данных.	
	№17 Практические реализации типовых моделей защищенных информационных систем обработки персональных данных.	
Модуль 5. Особенности обработки персональных данных без использования средств автоматизации.	***Содержание***	**6**
	Особенности обработки персональных данных без использования средств автоматизации.	
	Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне информационных систем персональных данных.	
	В том числе практических занятий	**2**
	№18 Разработка ОРД, необходимых для организации обработки персональных данных без использования средств автоматизации.	
Итоговая аттестация	зачет	**4**
	Всего:	**72 ч.**

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Организационно-педагогические условия реализации программы обеспечивают реализацию программы в полном объеме, соответствие качества подготовки обучающихся установленным требованиям, соответствие применяемых форм, средств, методов обучения и воспитания возрастным, психофизическим особенностям, склонностям, способностям, интересам и потребностям обучающихся.

Программа реализуется с использованием электронного обучения и дистанционных образовательных технологий

Наполняемость учебной группы не превышает 12 человек.

Продолжительность учебного часа теоретических и практических занятий, практического обучения составляет 1 академический час (45 минут).

Максимальная учебная нагрузка в неделю при реализуемой форме обучения не превышает 36 часов.

Педагогические работники, реализующие программу дополнительного профессионального образования, в том числе преподаватели учебных предметов, мастера производственного обучения, удовлетворяют квалификационным требованиям, указанным в квалификационных справочниках по соответствующим должностям и/или профессиональных стандартах.

Учебно-методические условия реализации программы: рабочая программа курса; учебный план; календарный учебный график; расписание занятий, методические материалы и разработки.

Материально-технические условия реализации программы.

Мастерская "Сетевое и системное администрирование"

№ п/п	Наименование учебного оборудования	Единица измерения	Количество
1	2	3	4
Учебно-производственное оборудование			
1.	Кресло компьютерное	Шт.	12
Программное и методическое обеспечение			
1.	10-Strike базовый набор программ системного администрирования/ неисключительное право (лицензия) на использование программного обеспечения 10-Strike "Базовый набор программ администратра Максимальный"	Шт.	1

2.	Коплект антивирусного ПО/ неисключительное право на программу для ЭВМ: Kaspersky EndpointSecurity для бизнеса - Стандартный Russian Edition	Шт.	1
3.	ОС Windows Server 2016/ неисключительное право (лицензия) на использование программного обеспечения WinSvrSTDCore 2019 RUS OLV 16Lic NL Each Acdmc AP CoreLic	Шт.	3

Информация об имеющейся для реализации образовательной программы учебно-материальной базе размещается на официальном сайте учреждения в информационно-коммуникационной сети «Интернет».

Информационное обеспечение обучения.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:

Основные источники

1. Партыка Т.Л. Вычислительная техника : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 3-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 445 с. : ил. — (Среднее профессиональное образование). ISBN: 978-5-91134-646-1
2. Арутюнов, В. В. Защита информации : учебно-методическое пособие / В. В. Арутюнов. - Москва : Либерея-Бибинформ, 2008. - 55, [1] с. : рис. ; 21 см. - (Библиотекарь и время. XXI век ; № 99). - ISBN 5-85129-175-3
3. 3. Васильков А. В., Васильков А. А., Васильков И. А. Информационные системы и их безопасность: Учебное пособие. - М.: Форум, 2015. - 528 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-289-0
4. 4. Мельников, В.П. Информационная безопасность [Текст] : учебное пособие для студентов образовательных учреждений среднего профессионального образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 7-е изд., стер. - Москва : Академия, 2013. - 331, [1] с. : ил., табл.; - (Среднее профессиональное образование. Информатика и вычислительная техника).; ISBN 978-5-7695-9954-5
5. Эксплуатация объектов сетевой инфраструктуры: учебник/А.В.Назаров.- М.: Академия, 2014.- 368с. ISBN 978-5-44680347-7

Дополнительные источники

Научно-технические и реферативные журналы:

1. Электросвязь
2. Вестник связи
3. Сети и системы связи
4. Мобильные системы

5. Цифровая обработка сигналов

6. Сводный реферативный журнал "Связь".

5. СИСТЕМА ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Индивидуальный учет результатов освоения обучающимися образовательных программ, а также хранение в архивах информации об этих результатах, осуществляются образовательной организацией на бумажных и/или электронных носителях.

Основной целью оценки освоения учебной дисциплины является оценка освоенных умений и усвоенных знаний.

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий.

Промежуточная аттестация

Критерии оценки практических работ.

Работа считается зачтенной если: правильно выполнено 60% и более практической работы, правильно даны ответы на 60% и более контрольных вопросов, предоставлен отчет о выполнении работы.

Работа считается не зачтённой если: выполнено менее 50% практической работы, не даны ответы на контрольные вопросы, имеются грубые ошибки в выполнении практических заданий и/или ответах на контрольные вопросы, противоречащие или искажающие основные понятия дисциплины, отчет о выполнении работы не предоставлен.

Допуском к итоговой аттестации является выполнение всех практических работ.

Итоговая аттестация

Повышение квалификации завершается итоговой аттестацией в виде зачета. Зачет проводится в форме защиты индивидуального проекта. Индивидуальный проект выполняется каждым обучающимся в рамках изучаемой программы. Основные требования к оформлению и защите индивидуального проекта приведены в контрольно-оценочных средствах по данной программе.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения	
классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей; определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи; осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выполнять тестирование систем с целью определения уровня защищенности;	оценка выполненных практических заданий, тестирование

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
определять оптимальные способы обеспечения информационной безопасности; проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях; проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации; разрабатывать политику безопасности сетевых элементов и логических сетей; выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи; конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; защищать базы данных при помощи специализированных программных продуктов; защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.	
принципы построения информационно-коммуникационных сетей; международные стандарты информационной безопасности для проводных и беспроводных сетей; нормативно - правовые и законодательные акты в области информационной безопасности; акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия; технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия; способы и методы обнаружения средств съёма информации в радиоканале; классификацию угроз сетевой безопасности; характерные особенности сетевых атак; возможные способы несанкционированного доступа к системам связи; правила проведения возможных проверок согласно нормативных документов ФСТЭК; этапы определения конфиденциальности документов объекта защиты; назначение, классификацию и принципы работы специализированного оборудования; методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2; методы и средства защиты информации в телекоммуникациях от вредоносных программ; технологии применения программных продуктов;	оценка выполненных практических заданий, тестирование

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
возможные способы, места установки и настройки программных продуктов; методы и способы защиты информации, передаваемой по кабельным направляющим системам; конфигурации защищаемых сетей; алгоритмы работы тестовых программ; средства защиты различных операционных систем и среды передачи информации; способы и методы шифрования (кодирование и декодирование) информации.	

6. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОБЕСПЕЧИВАЮЩИЕ РЕАЛИЗАЦИЮ ПРОГРАММЫ

Учебно-методические материалы представлены:

1. Программой повышения квалификации «Защита персональных данных».
2. Положением об Учебно-производственном центре по подготовке, переподготовке и повышению квалификации строителей краевого государственного бюджетного профессионального образовательного учреждения «Алтайский архитектурно-строительный колледж»;
3. Положением о профессиональном обучении в краевом государственном бюджетном профессиональном образовательном учреждении «Алтайский архитектурно-строительный колледж» (КГБПОУ «Алтайский архитектурно-строительный колледж»);
4. Положением о формах обучения по дополнительным профессиональным образовательным программам и программам профессионального обучения в краевом государственном бюджетном профессиональном образовательном учреждении «Алтайский архитектурно строительный колледж»;
5. Правилами приема обучающихся на обучение по программам дополнительного профессионального образования и основным программам профессионального обучения в КГБПОУ «Алтайский архитектурно-строительный колледж»;
6. Электронными учебными материалами.
7. Материалами для проведения промежуточной и итоговой аттестации обучающихся.