Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Этика и безопасность искусственного интеллекта»

1.	Наименование образовательной организации-разработчика программы	Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Этика и безопасность искусственного интеллекта»
3.	Объем часов	72
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	– 10.04.01. Информационная безопасность; – 10.05.01. Компьютерная безопасность (специализация 2); – 10.05.03. Информационная безопасность автоматизированных систем (специализации 5,6,7); – 10.05.04. Информационно-аналитические системы безопасности (специализации 1,2,3); – 10.05.05. Безопасность информационных технологий в правоохранительной сфере (специализации 4,5).
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	– Безопасность систем искусственного интеллекта (10.04.01, 10.05.03 специализации 5,6,7); – Безопасность экспертных систем (10.05.01 специализация 2, 10.05.04 специализации 1,2,3); – Доверенный искусственный интеллект (10.04.01); – Этические и правовые проблемы внедрения искусственного интеллекта (10.04.01, 10.05.05 специализации 4,5).
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	– 06.030 Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях»; – 06.031 Профессиональный стандарт «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности»; – 06.032 Профессиональный стандарт "Специалист по безопасности компьютерных систем и сетей"– ОТФ B, B/02.6; – 06.033 Профессиональный стандарт «Специалист по защите информации в автоматизированных системах».
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: - основные концепции искусственного интеллекта, связанные с оценкой устойчивости, управлением рисками, безопасностью, объяснимостью, обнаружением аномалий и компьютерных атак и защитой данных; -основные международные и национальные стандарты в области доверенного искусственного интеллекта;	

	- нормативно правовую базу в области разработки и использования искусственного интеллекта, защиты результатов интеллектуальной деятельности и сведений ограниченного доступа, полученных с целью обучения и тестирования искусственного интеллекта, обеспечения прав человека; - современные этические принципы разработки полезных и социально-приемлемых систем на базе искусственного интеллекта. Уметь: - готовить материалы по тематике доверенного искусственного интеллекта (научные статьи, презентации, доклады и др.); -формулировать и анализировать задачи, связанные с обеспечением доверия к искусственному интеллекту с использованием общепринятых и принятых в данной сфере принципов, методов и подходов; -интерпретировать требования заказчика и применять концепции искусственного интеллекта при формулировании технического задания; - анализировать проблематику различных сфер человеческой деятельности, где применение искусственного интеллекта позволит эффективно решить актуальные проблемы; - анализировать и применять нормы международного и российского законодательства в сфере интеллектуальной собственности, авторских прав и защиты информации для разработки соответствующих систем на базе искусственного интеллекта.	
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем). Учебная дисциплина «Этические проблемы внедрения искусственного интеллекта»: – Принципы искусственного интеллекта; – Социальная ответственность, связанная с внедрение систем на базе искусственного интеллекта; – Создание и использование этичного и социально приемлемого ИИ в современном мире; – Правовые аспекты участия человека в биомедицинских экспериментах для обучения и тестирования систем на базе искусственного интеллекта. Учебная дисциплина «Доверенный искусственный интеллект»: – Проблемы доверия к системам на базе искусственного интеллекта; – Этические аспекты доверия к системам на базе искусственного интеллекта; – Объяснимость работы моделей искусственного интеллекта и машинного обучения; – Обнаружение аномалий в системах искусственного интеллекта; – Оценка устойчивости (робастности) искусственного интеллекта. Учебная дисциплина «Безопасность систем искусственного интеллекта»: – Методы оценки рисков и управление рисками, возникающих из-за внедрения систем на базе искусственного интеллекта; – Компьютерные атаки на системы на базе искусственного интеллекта; – Защита данных при разработке и использовании систем на базе искусственного интеллекта.	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы «Этика и безопасность искусственного интеллекта». 2. Учебные пособия и профильная литература: • Загорулько Ю.А. Искусственный интеллект. [Электронный ресурс]: Учебное пособие для вузов/Загорулько Ю.А., Загорулько Г.Б., 2020.93 с.; • Чио К. Машинное обучение и безопасность. [Электронный ресурс]: руководство/ К. Чио, Д. Фримэн, 2020.388 с.; • Андрей Бурков Машинное обучение без лишних слов. [Электронный ресурс]: Бурков Андрей, 2020. -192 с. 3. Методические рекомендации по практическим,

		лабораторным работам. 4. Оценочные средства в виде тестирующего комплекса
10.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	– ФГОБОУ ВО «Омский Государственный Технический Университет» (ОмГТУ); – ООО «СИБ» https://sib-nsk.net/ ; – ООО НТЦ «КАСИБ» https://kasib.ru/ ;
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	«AIC desktop» http://aiconstructor.ru/

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Методы и средства криптографической защиты информации»

1.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Методы и средства криптографической защиты информации»
3.	Объем часов	40
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	– 10.03.01 Информационная безопасность (профиль 1); – 10.05.01 Компьютерная безопасность (специализации 1-8); – 10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12); – 10.05.03 Информационная безопасность автоматизированных систем (специализации 1-11); – 10.05.04 Информационно-аналитические системы безопасности (специализации 1-4); – 10.04.01 «Информационная безопасность»
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	– Криптографические протоколы (10.03.01 Информационная безопасность (профиль 1), 10.05.01 Компьютерная безопасность (специализации 1-8), – Методы и средства криптографической защиты информации (10.05.01 Компьютерная безопасность (специализации 1-8), 10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12), 10.05.04 Информационно-аналитические системы безопасности (специализации 1-4);10.04.01 «Информационная безопасность»); – Программно-аппаратные средства защиты информации (10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12), 10.05.03 Информационная безопасность автоматизированных систем (специализации 1-4), 10.04.01 «Информационная безопасность»).
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.032 Профессиональный стандарт "Специалист по безопасности компьютерных систем и сетей", утвержденный приказом Министерства труда и

		социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: - криптоалгоритмы, используемые в современных стандартах шифрования данных; - криптоалгоритмы, используемые в современных криптосистемах с открытым ключом; - методы выбора криптографических параметров, обеспечивающих необходимую стойкость криптосистемы; - приложения криптографии к решению различных проблем защиты информации в компьютерных системах, в частности проблемы безопасности электронных банковских систем. Уметь: - применять полученные знания к исследованию простых шифров; - строить и изучать математические модели криптоалгоритмов; - проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;	
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	Учебная дисциплина «Криптографические методы защиты информации»: − Криптосистемы с открытым ключом. Система Диффи-Хэллмана; − Шифр Шамира. Шифр Эль-Гамаля. Односторонняя функция с «лазейкой» и шифр RSA; − Теоретическая стойкость криптосистем; − Современные шифры с секретным ключом; − Электронная или цифровая подпись; − Криптографические протоколы.	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб. работам, фонд оценочных средств.	1.Курс лекций программы «Криптографические методы защиты информации» 2. Учебные пособия и профильная литература: • *Алферов А.П. , Зубов А.Ю. , Кузьмин А.С. , Черемушкин А.В.* «Основы криптографии». — М.: Гелиос АРВ, 2005. • *Белов Е.Б, Лось В.П., Мещеряков Р.В., Шелупанов А.А.* Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2006. • *Панасенко С.* «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009 г. • *ПогореловБ.А., Сачков В.Н.* Словарь криптографических терминов. М.: МЦНМО, 2006 • *Проскурин В.Г.* Защита программ и данных. Учебное пособие для вузов. М.: Академия, 2012. • *Проскурин, В.Г.* Защита в операционных системах. – М.: Академия, 2012. • *Рябко Б.Я., Фионов А.Н.* Основы современной криптографии и стеганографии. – М.: Горячая линия–Телеком, 2010. • *Черёмушкин А.В.* Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009 • *Шнаер Б.* «Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си». — М.: Триумф, 2002. • Удостоверяющий центр ViPNet: курс лекций и

		практикум. • Система защиты информации ViPNet (Курс лекций). • Введение в криптографию / Под общ. ред. В.В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012. - 348 с. • Глухов М.М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В. Введение в теоретико-числовые методы криптографии. – М.: Лань, 2011. • Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации. Учебник для академического бакалавриата. - М.: Юрайт, 2017. • Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - М.: Гелиос АРВ, 2005. • Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. - М.: Горячая линия- Телеком, 2012 . — 141 с. • Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006 3. Оценочные средства в виде тестирующего комплекса
10.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС»),
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС») – ViPNet_Client, ViPNet_PKI_Client

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Противодействие сетевым атакам»

12.	Наименование образовательной организации-разработчика программы	Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)
13.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Противодействие сетевым атакам»
14.	Объем часов	72
15.	Специальность/направление (ФГОС 3++), по которым реализуется программа	– 10.03.01. Информационная безопасность (профили 2,4,5); – 10.04.01. Информационная безопасность; – 10.05.01. Компьютерная безопасность (специализации 1, 5-8); – 10.05.02 Информационная безопасность телекоммуникационных систем (специализации 7-12); – 10.05.05. Безопасность информационных технологий в правоохранительной сфере (специализации 4,5).
16.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	– Проектирование элементов защищенных телекоммуникационных систем (10.05.02 специализации 7-12); – Компьютерные атаки (10.03.01 профили 2,4,5; 10.05.01 специализации 1, 5-8; 10.04.01 Информационная безопасность); – Основы построения систем перехвата информации и управления (10.05.05 специализации 4,5); – Моделирование и предотвращение сетевых атак в локальных сетях (10.05.01 специализации 4,7); – Мониторинг безопасности телекоммуникационных систем (10.05.02 специализации 7,9,10,12).
17.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	– 06.030 Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях»; – 06.032 Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» – ОТФ B, B/03.6; ОТФ C, C/02.7, C/03.7, C/05.7
18.	Ключевые результаты обучения: (знать, уметь)	
	Знать: – основные угрозы безопасности информации в телекоммуникационных системах; – распространенные типы сетевых атак в локальных и глобальных сетях и инструменты, используемые для их реализации; – современные способы виртуализации и моделирования телекоммуникационных систем; – основные подходы к мониторингу и анализу сетевого трафика; – методы противодействия сетевым атакам в телекоммуникационных системах;	

	– принципы построения систем обнаружения атак; – существующие методики оценки безопасности систем и проведения тестов на проникновение. Уметь: – выявлять и оценивать угрозы несанкционированного доступа к телекоммуникационным системам и сетям; – использовать встроенные механизмы защиты от несанкционированного доступа в составе телекоммуникационных систем; – проводить проверку работоспособности и эффективности применяемых средств защиты; – применять методы анализа защищенности компьютерных систем и сетей; – применять инструментальные средства проведения мониторинга защищенности компьютерных систем; – применять программные инструменты с открытым исходным кодом для обнаружения сетевых атак.	
19.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	Учебная дисциплина «Моделирование и предотвращение сетевых атак в локальных сетях»: – Подготовка виртуального стенда для моделирования и предотвращения сетевых атак; – Противодействие сетевым атакам на таблицу коммутации; – Противодействие сетевым атакам на протокол DHCP; – Противодействие сетевым атакам на протокол ARP; – Моделирование разведывательных сетевых атак; – Моделирование атак прослушивания; – Тестирование на проникновение. Учебная дисциплина «Мониторинг безопасности телекоммуникационных систем»: – Подходы к мониторингу и анализу сетевого трафика; – Применение ПО с открытым исходным кодом для обнаружения сетевых атак; – Организация, парсинг и анализ журналов системы обнаружения атак; – Генерация, захват и анализ сетевого трафика; – Применение сценариев для анализа журналов системы обнаружения вторжений; – Создание и использование сигнатур; – Обнаружение сетевых атак в режиме реального времени.	
20.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб. работам, фонд оценочных средств.	1. Курс лекций программы «Противодействие сетевым атакам». 2. Учебные пособия: • Щерба Е.В., Щерба М.В., Магазев А.А. «Противодействие сетевым атакам в локальных сетях»; 3. Методические рекомендации к лабораторным работам и практическим заданиям Практикум: • Щерба Е.В., Ситник В.А. «Мониторинг сетевых вторжений»; 4. Оценочные средства в виде тестирующего комплекса
21.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	– ФГБОУ ВО «Омский государственный технический университет» (ОмГТУ); – АО «Позитив Текнолоджиз».
22.	Используемые отечественные ПО и средства защиты информации (при наличии)	– ОС Astra Linux Special Edition; – Программное обеспечение с открытым исходным кодом: • Kali Linux; • Ubuntu; • Система обнаружения атак Zeek.

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Информационно-аналитические системы безопасности»

1.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа профессиональной переподготовки «Информационно-аналитические системы безопасности»
3.	Объем часов	360
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.05.04 Информационная безопасность автоматизированных систем (специализации 1-4)
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	– Базы данных и экспертные системы (10.05.04 Информационная безопасность автоматизированных систем (специализации 1-11)); – Методы анализа данных (10.05.04 Информационная безопасность автоматизированных систем (специализации 1-4); – Основы обработки данных больших объемов (10.05.04 Информационная безопасность автоматизированных систем (специализации 1-4); – Распределённые информационно-аналитические системы 10.05.04 Информационная безопасность автоматизированных систем (специализации 1); – Моделирование информационно-аналитических систем 10.05.04 Информационная безопасность автоматизированных систем (специализации 3); – Информационная безопасность бизнес-процессов (10.05.04 Информационная безопасность автоматизированных систем (специализации 1-4). – Методология информационно-аналитической работы (10.05.04 Информационная безопасность автоматизированных систем (специализации 1-4). – Технологии, методики и подходы OSINT (10.05.04 Информационная безопасность автоматизированных систем (специализации 1-4). – Анализ инцидентов информационной безопасности (10.05.04 Информационная безопасность автоматизированных систем (специализации 1-4).

6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	Профстандарт 06.031 Специалист по автоматизации информационно-аналитической деятельности в области безопасности Обобщенная трудовая функция: A. Применение ИАС (информационно-аналитических систем) в защищенном исполнении в процессах АИАД (автоматизированной информационно-аналитической деятельности) ТФ-A/01.7, ТФ-A/02.7, ТФ-A/03.7 D. Организационное управление в ИАС в защищенном исполнении Профстандарт 06.001 Программист, ОТФ A, ТФ A/01.3 Профстандарт 08.021 Специалист по финансовому мониторингу (в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма), ОТФ B, ТФ B/01.7 ТФ B/02.7
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: – этапы проектирования и разработки баз данных (БД); – типовую структуру экспертных систем (ЭС), типы задач, решаемых экспертными системами, области применения ЭС; – модели представления знаний; – процесс разработки экспертных систем; – типовую структуру систем управления базами данных (СУБД), основные функции и компоненты СУБД; – структуры данных и ограничения целостности реляционной модели данных, операции реляционной алгебры; – принципы проектирования реляционной БД, отвечающие требованиям нормализации; – операторы языка SQL: CREATE TABLE, CREATE VIEW, SELECT, INSERT, UPDATE, DELETE, CREATE ROLE, GRANT; – принципы интеграции операторов языка SQL с универсальной средой программирования; – типы физической организаций файла и соответствующие им методы доступа; – основные подходы к оптимизации запросов в реляционных СУБД; – проблемы управления транзакциями и подходы к их решению; – методологические основы анализа данных; – методы анализа распределения данных; – методы анализа временных рядов; – методы анализа однородности данных; – методы анализа многомерных данных и снижения размерности; – основы сбора и обработки больших данных; – технологии хранения больших данных; – архитектуру распределённых СУБД; – процедурные расширения языков запросов реляционных СУБД; – современные технологии разработки web-приложений; – методы построения и исследования аналитических и имитационных моделей процессов обработки информации в информационно-аналитических системах; – методы оценки эффективности процессов обработки информации в информационно-аналитических системах на базе математического моделирования; – архитектуру распределённых СУБД;	

	– процедурные расширения языков запросов реляционных СУБД; – современные технологии разработки web-приложений; – методы построения и исследования аналитических и имитационных моделей процессов обработки информации в информационно-аналитических системах; – методы оценки эффективности процессов обработки информации в информационно-аналитических системах на базе математического моделирования; – методы управления и выявления инцидентов ИБ; – методы оценки эффективности принимаемых решений и действий в процессном подходе управления и анализа инцидентов ИБ; – – задачи аналитической работы в области ИБ и ее ограничения; – – методы работы с малыми группами исполнителей в задачах обеспечения информационной безопасности; Уметь: – - разрабатывать ER-модель предметной области; – реализовывать схему реляционной БД с использованием языка SQL; – формализовывать предметную область с целью создания баз данных и экспертных систем; – осуществлять выбор средств обеспечения информационной безопасности распределённых СУБД; – разрабатывать программные единицы с использованием процедурных расширений языков запросов распределённых СУБД; – строить и исследовать аналитические и имитационные модели процессов обработки информации в информационно-аналитических системах; – решать методами моделирования задачи исследования эффективности процессов обработки информации в информационно-аналитических системах; – выявлять инциденты ИБ на основе анализа разносторонней информации о функционировании АС; – формализовывать и реализовывать предложения по совершенствованию системы управления ИБ организации и инцидентами в частности; – использовать процессный подход и рекомендации нормативных документов для организации процесса управления инцидентами на предприятии; осуществлять выбор средств обеспечения информационной безопасности распределённых СУБД; – разрабатывать программные единицы с использованием процедурных расширений языков запросов распределённых СУБД; – строить и исследовать аналитические и имитационные модели процессов обработки информации в информационно-аналитических системах; – решать методами моделирования задачи исследования эффективности процессов обработки информации в информационно-аналитических системах; – рассчитать на основе типовых методик экономические и финансовые показатели, необходимые для обоснования организационно-управленческих решений в области создания и эксплуатации ИАС в ИБ; – оценивать стоимость внедрения и стоимость владения ИАС в ИБ.
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).
	Учебная дисциплина «Базы данных и экспертные системы»: – Концепция баз данных.; – Системы управления базами данных (СУБД); – Проектирование баз данных; – Концептуальное проектирование;

	− Реляционная модель данных; − Проектирование реляционной БД на основе принципов нормализации; − Язык SQL; − Дореляционные базы данных; − Постреляционные базы данных; − SQL в среде программирования; − Физическая организация файла и методы доступа. Индексы; − Выполнение запросов. Оптимизация запросов; − Управление транзакциями; − Системы искусственного интеллекта; − Модели представления и манипулирования знаниями; − Разработка экспертных систем. Учебная дисциплина «Методы анализа данных»: − Методология анализа данных.; − Моделирование данных; − Анализ распределения данных; − Анализ зависимостей элементов последовательности; − Анализ однородности данных; − Анализ зависимостей в многомерных данных; − Снижение размерности данных. Учебная дисциплина «Основы обработки данных больших объемов»: − Основы обработки больших данных; − Сбор больших данных; − Анализ потоков данных и поиск нечетких дубликатов; − Полнотекстовое индексирование больших данных; − Рекомендательные системы; − Технологии хранения больших данных; − Модель вычислений MapReduce; − Колоночные СУБД; − Документо-ориентированные распределенные СУБД; − Графовые СУБД; − Анализ графов социальных сетей; − Мониторинг процессов обработки больших данных. Учебная дисциплина «Моделирование информационно-аналитических систем»: − Моделирование. Основные понятия и принципы. − Аналитическое моделирование. Математическое моделирование; − Показатели и критерии эффективности функционирования систем; − Введение в имитационное моделирование; − Системы имитационного моделирования; − Планирование эксперимента. Учебная дисциплина «Распределенные системы»: − Архитектура масштабируемых параллельных систем; − Параллельное программирование; − Распределенное хранение и обработка данных; − Разработка web-приложений: язык разметки; − Высоконагруженные системы; − Облачные вычисления и виртуализация. Учебная дисциплина «Информационная безопасность бизнес-процессов» − Моделирование систем управления ИБ; − Процессный подход в управлении ИБ; − Ситуационный подход. Особенности и применение. Приоретизация и оптимизация инвестиций в ИБ; − Метрики процессов ИБ;

	− Активы ИБ. Инвентаризация и анализ; − Процессы аутсорсинга ИБ. Управление аутсорсингом Учебная дисциплина «Методология информационно-аналитической работы» - Методология работы с источниками информации - Инструменты для поиска информации в интернете. Правила составления информационного документа. - Методы аналитической работы. Учебная дисциплина «Анализ инцидентов информационной безопасности» − Системный подход к управлению инцидентами ИБ, нормативное регулирование процесса; − Организационное управление инцидентами ИБ, методы оценки эффективности и организации деятельности группы реагирования, политика и планы реагирования, способы составления и отработки; − Средства управления инцидентами ИБ, источники сведений и системы анализа данных, стратегии распределения ресурсов; Учебная дисциплина «Технологии, методики и подходы OSINT» − Правовые и этические аспекты OSINT − Работа с источниками, сбор и анализ информации из подключенных цифровых устройств, использование мобильных приложений, GPS-трекеров, умных камер и других IoT − Методы сбора Больших данных, методы анализа с использованием искусственного интеллекта (машинное обучение, нейронные сети), работа с отчетами на основе проведенного анализа для принятия управленческих решений − Обзор современных инструментов OSINT	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб.работам, фонд оценочных средств.	1.Курс лекций программы ДПО «Информационная безопасность» 2. Учебные пособия и профильная литература: • Дейт, К.Дж. Введение в системы баз данных. 8-е издание. : / К.Дж. Дейт — М.: Диалектика, 2019. — 1327 с. • Коннолли, Т. Базы данных: проектирование, реализация и сопровождение. 8-е изд.: / Т. Коннолли — М.: Вильямс, 2018. — 1439 с. • Джарратано, Дж Экспертные системы: принципы разработки и программирование, 4-е издание.: / Дж Джарратано, Г. Райли — М.: Вильямс, 2007. — 1152 с. • Смирнов, С.Н. Практикум по работе с базами данных. : / С.Н. Смирнов, А.В. Киселев — М.: Гелиос АРВ, 2012. — 160 с. • Мхитарян, В.С. Анализ данных: учебник / В.С. Мхитарян, М.Ю. Архипова, Т.А. Дуброва, Ю.Н. Миронкина, В.П. Сиротин — М.: Юрайт, 2017. — 490 с. • Кеннет, Су Теоретический минимум по Big Data. Всё что нужно знать о больших данных: / Су Кеннет, Ын. Анналин — СПб: Питер, 2019. — 208 с. • Лесковец, Ю. Анализ больших наборов данных: / Ю. Лесковец, Дж.Д. Ульман — М.: ДМК Пресс, 2016. — 498 с. • Клеппман, М. Высоконагруженные приложения. Программирование, масштабирование, поддержка: / М. Клеппман — СПб: Питер, 2018. — 740 с. • Уилсон, Д.Р. Семь баз данных за семь недель. Введение в современные базы данных и идеологию NoSQL: / Д.Р. Уилсон, Э. Редмонд — М.: ДМК Пресс, 2018. — 384 с. • Фаулер, М. NoSQL. Методология разработки

		нереляционных баз данных: / М. Фаулер, П.Дж. Садаладж — М.: Диалектика-Вильямс, 2020. — 192 с. • Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина; Министерство образования и науки РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2017. - 86 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=467139; • Дарл, К. Oracle для профессионалов. Архитектура, методики программирования и основные особенности версий 9i, 10g, 11g и 12c: / К. Дарл, Т. Кайт — М.: Диалектика-Вильямс, 2019. — 336 с. • 2. Ткачев, О.А. Основы программирования в СУБД Oracle. SQL+PL/SQL: / О.А. Ткачев — М.: Litres, 2021. — 456 с. • 3. Форта, Б. Oracle PL/SQL за 10 минут: / Б. Форта — М.: Диалектика-Вильямс, 2019. — 336 с. • 4. Смирнов, С.Н. Безопасность систем баз данных: учебное пособие / С.Н. Смирнов — М: Гелиос АРВ, 2007. — 351 с. • 5. Кайт, Т. Oracle для профессионалов. Архитектура, методики программирования и особенности версий 9i,10g и 11g: учебное пособие / Т. Кайт — М: Вильямс, 2012. — 848 с. • Петухов, О.А. Моделирование: системное, имитационное, аналитическое: Учебное пособие / О.А. Петухов, А.В. Морозов, Е.О. Петухова — Спб.: СЗТУ, 2008. — 288 с. • 2. Финаев, В.И. Аналитические и имитационные модели: Учебное пособие / В.И. Финаев, Е.Н. Павленко, Е.В. Заргарян — Таганрог: Издательствово Технологического института ЮФУ, 2007. — 310 с. • 3. Эльберг, М.С. Имитационное моделирование: Учебное пособие / М.С. Эльберг, Н.С. Цыганков — Красноярск: Сибирский федеральный университет (СФУ), 2017. — 128 с. • 4. Салмина, Н.Ю. Имитационное моделирование: Учебное пособие / Н.Ю. Салмина — Томск: Эль Контент, 2012. — 90 с. • 5. Варжапетян, А.Г. Имитационное моделирование на GPSS/H: Учебное пособие / А.Г. Варжапетян — Спб.: ГУАП, 2007. — 384 с. • 6. Каталевский, Д.Ю. Основы имитационного моделирования и системного анализа в управлении: Учебное пособие / Д.Ю. Каталевский — М.: Издательский дом «Дело», 2015. — 496 с. 3. Метод рекомендации по лаб. работам. 4. Оценочные средства в виде тестирующего комплекса
10.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные	– ООО «Атом Безопасность»; – ЗАО «НПО «Эшелон».

	представители организаций.	
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	– Astra Linux 1.6 Common Edition – Elma – ScanOVAL

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Разработка автоматизированных систем в защищенном исполнении»

12.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)
13.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа профессиональной переподготовки «Разработка автоматизированных систем в защищенном исполнении»
14.	Объем часов	360
15.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.05.03 Информационная безопасность автоматизированных систем (специализации 1-11)
16.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	– Организационное и правовое обеспечение информационной безопасности (10.05.03 Информационная безопасность автоматизированных систем (специализации 1-11)); – Анализ рисков информационной безопасности (10.05.03 Информационная безопасность автоматизированных систем (специализации 1-11); – Анализ безопасности информационных систем (10.05.03 Информационная безопасность автоматизированных систем (специализации 1-11); – Организация проектной деятельности 10.05.03 Информационная безопасность автоматизированных систем (специализации 1-11); – Разработка и эксплуатация автоматизированных систем в защищенном исполнении); – Нормативная база обеспечения информационной безопасности организаций финансово-кредитной сферы (10.05.03 Информационная безопасность автоматизированных систем (специализации 1-11).
17.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	– 06.030 Профессиональный стандарт "Специалист по защите информации в телекоммуникационных системах и сетях", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н; – 06.032 Профессиональный стандарт "Специалист по безопасности компьютерных систем и сетей", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н.
18.	Ключевые результаты обучения: (знать, уметь)	

	Знать: - нормативные документы ФСТЭК, ФСБ, Роскомнадзор, Минцифры; - обзор международных стандартов; - типовую модель (ФСТЭК). - критерии нарушителя/угроз; - нормативные документы по классификации защищаемых объектов; - ГОСТР 15408 (Оценочный уровень доверия средств защиты); - меры защиты (Организационные, превентивные, технические)- виды, источники и носители защищаемой информации; - технические средства защита информации, их классификация (какие средства есть и порядок применения); - порядок сертификации средств защиты информации. - обзор нормативной базе по проектированию (ГОСТы); - модель угроз; - акты классификации информатизации Уметь: - разрабатывать техническое задания на проектирования ИС (ГОСТР 34.601-603); - проектировать АС в защищенном исполнении (ГОСТР 51.); - разрабатывать эскизный проект; - разрабатывать рабочий проект; - проектировать этапы внедрения системы; - проводить аттестацию на соответствие требований ИБ для ИС; - разрабатывать порядок эксплуатации АС в защищенном исполнении;
19.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).
	Учебная дисциплина «Организационное и правовое обеспечение информационной безопасности»: − Безопасность информационного общества; − Характеристика законодательства РФ в области информационной безопасности; − Перечень нормативных правовых актов по обеспечению безопасности информатизации; − Нормативные документы ФСТЭК, Роскомнадзора, Минцифры; ФСБ; − Обзор международных стандартов. Учебная дисциплина «Информационно-аналитическая и техническая экспертиза компьютерных систем»: − Типовая модель ФСТЭК; − Нормативные документы по классификации защищаемых объектов; − Оценочный уровень защиты средств защиты; − Меры защиты; − Технические средства защиты информации, их классификация; − Порядок сертификации средств защиты информации. Учебная дисциплина «Разработка автоматизированных систем в защищенном исполнении»: − Обзор нормативной базы по проектированию; − Разработка технического задания на проектирование информационных систем; − Проектирование автоматизированных систем в защищенном исполнении; − Этапы проектирования и внедрения ИС; − Аттестация на соответствие требований; − Порядок эксплуатации автоматизированных систем в защищенном исполнении. Учебная дисциплина «Безопасность автоматизированных систем в финансово-кредитной сфере»: − Модель угроз;

	– Акты классификации.	
20.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб.работам, фонд оценочных средств.	1.Курс лекций программы ДПО «Информационная безопасность» 2. Учебные пособия и профильная литература: ● Редько С.Г., Итс Т.А., Цветкова Н.А., Голубев С.А., Сурина А.В. Основы проектной деятельности: учебное пособие. Учебное пособие. Санкт петербург. 2018. 84 с. DOI: 10.18720/SPBPU/2/s18-134. ● 2. Михалкина, Е. В. Организация проектной деятельности : учебное пособие / Е. В. Михалкина, А. Ю. Никитаева, Н. А. Косолапова ; Южный федеральный университет. – Ростов-на-Дону : Издательство Южного федерального университета, 2016. – 146 с. ISBN 978-5-9275-1988-0. ● Семкин С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации.: Учебное пособие.-М.: Гелиос АРВ, 2005.-185 ● Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие - Спнкт-Петребург: Лань, 2017.- 324 с. ● Галатенко В.А. Основы информационной безопасности [Электронный ресурс]: - Электрон. текстовые данные.- Интернет - Университет(ИНТУИТ), 2016, - 266 с.137 ● БД угроз ФСТЭК http://bdu.fstec.ru; ● Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие [Электронный ресурс]: учебное пособие/ Шелухин О.И., САкалема Д.Ж., Филинова А.С.- электрон. дан.- Москва: Горячая линия-Телеком, 2013, - 220 с. ● Милославская Н.Г. Интрасети: обнаружение вторжений: [учебн. пособие для студентов вузов по специальности информ. безоп. авт. систем и ""Компьютерная безопасность""]/ Н.Г. Миорславская , А.И. Толстой .- М.:ЮНИТИ-ДАНА, 2001 г.- 587 с. ● В.Г. Миронова, А.А. Шелупанов. Анализ этапов предпроектного обследования информационной системы персональных данных // Периодический научный журнал «Вестник СибГАУ им.М.Ф.Решетнева».-2011 - №2(35), С. 45-48 ● А. Бирюков ""Информационная безопасность: защита и нападение"" 2-е изд. ДМК(2017) 3. Метод рекомендации по лаб. работам. 4. Оценочные средства в виде тестирующего комплекса
21.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	– ООО «Системы информационной безопасности» – АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС»), Федеральное государственное бюджетное образовательное учреждение высшего образования Новосибирский государственный технический университет, НГТУ

22.	Используемые отечественные ПО и средства защиты информации (при наличии)	Средства ПО и защиты информации компаниями: – АО "Аладдин Р.Д."; – ООО «Код Безопасности», – АО "ОКБ САПР"; – АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС»); – ООО «ЦБИ».

Аннотация

программы дополнительного профессионального образования профессорско-преподавательского состава в области информационной безопасности в рамках реализации федерального проекта «Информационная безопасность»

Наименование: «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»

1.	Наименование образовательной организации	Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ)
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа профессиональной переподготовки «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»
3.	Объем часов	706
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	– 10.03.01 Информационная безопасность (профиль 3); – 10.04.01 Информационная безопасность; – 10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12); – 10.05.03 Информационная безопасность автоматизированных систем (специализации 1-4).
5.	– Учебная дисциплина (ПООП, ООП), ассоциированная с программой	– Организационное и правовое обеспечение информационной безопасности (10.03.01 Информационная безопасность, профиль 3, 10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12), 10.05.03 Информационная безопасность автоматизированных систем (специализации 1-4)); – Комплексное обеспечение защиты информации телекоммуникационных систем (10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12), – Защита информации от утечки по техническим каналам (Информационная безопасность, профиль 3, 10.05.02 Информационная безопасность, специализации 1-12, 10.05.03 Информационная безопасность автоматизированных систем (специализации 1-4); – Системы и сети передачи информации (10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-

		12), – **Аттестация объектов информатизации по требованиям безопасности информации** (10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12), – **Защита информации от утечки по техническим каналам** – (10.05.01 Информационная безопасность, профиль 3,); 10.04.01 Информационная безопасность; – 10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12); – **Мониторинг безопасности телекоммуникационных систем и сетей** (10.05.02 Информационная безопасность телекоммуникационных систем (специализации 1-12), 10.04.01 Информационная безопасность,
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	– 06.030 Профессиональный стандарт "Специалист по защите информации в телекоммуникационных системах и сетях", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н; – 06.032 Профессиональный стандарт "Специалист по безопасности компьютерных систем и сетей", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н.
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: – нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации; – основы построения информационных систем и формирования информационных ресурсов; – виды конфиденциальной информации; – перечни сведений конфиденциального характера, основные требования и рекомендации по их защите; – действующую систему сертификации средств защиты информации по требованиям безопасности информации; – основы лицензирования деятельности по ТЗКИ и (или) деятельности по разработке и производству средств защиты конфиденциальной информации; – физические основы возникновения, классификацию и характеристики ТКУИ; – угрозы безопасности информации; – цели, задачи, основы организации, основные способы и средства ТЗКИ и контроля защищенности информации; – правила разработки, утверждения, обновления и отмены документов в области ТЗКИ; – типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащенности техническими средствами; – порядок проведения аттестации объектов информатизации по требованиям безопасности информации; – организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (в том числе по защите информации от утечки по техническим каналам, защиты информации от несанкционированного доступа (НСД) и по защите	

	информации от специальных воздействий); – общие требования по ТЗКИ (в том числе по защите информации от утечки по техническим каналам, защиты информации от НСД и по защите информации от специальных воздействий), нормы, требования и рекомендации – по защите объектов информатизации от различных угроз безопасности информации, методы и методики контроля их выполнения; – требования к средствам ТЗКИ и контроля защищенности информации; средства ТЗКИ и контроля защищенности информации, порядок их применения; – принципы построения и функционирования, примеры реализации современных операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основные протоколы компьютерных сетей; – программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей; – подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты информации от утечки по техническим каналам, несанкционированных, непреднамеренных воздействий, контроля целостности информации; – порядок осуществления аутентификации взаимодействующих объектов, проверки подлинности отправителя и целостности передаваемых данных; – порядок организации и проведения контроля защищенности информации; типовую структуру, задачи и полномочия подразделения по ТЗКИ; требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объекта информатизации; – порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемую в этих целях контрольную аппаратуру и тестовые средства. Уметь: – работать с действующей нормативной правовой и методической базой в области защиты информации; – определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий; – определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации; – разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации; – разрабатывать технические задания на проведение научно- исследовательских и опытно-конструкторских работ в области ТЗКИ; – проводить работы по классификации защищенности – автоматизированных систем от НСД к информации, аттестации объектов информатизации; – применять подсистемы разграничения доступа, подсистемы обнаружения атак, методы анализа результатов проверок, учета нарушений требований по ТЗКИ; – осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных; – применять штатные средства ТЗКИ и контроля защищенности информации, осуществлять контроль защищенности информации; – проводить организационные и технические мероприятия по ТЗКИ;
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).
	Учебная дисциплина «Организационно-правовые основы технической защиты конфиденциальной информации»: – Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам; – Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа;

- Техническая защита конфиденциальной информации от специальных воздействий;
- Организация защиты конфиденциальной информации на объектах информатизации;
- Аттестация объектов информатизации по требованиям безопасности информации;
- Контроль состояния технической защиты конфиденциальной информации.

Учебная дисциплина «Аппаратные средства вычислительной техники»:

- Представление данных в ЭВМ;
- Системное и прикладное программное обеспечение;
- Способы представления информации в компьютере и методы их реализации;
- Организация взаимодействия периферийных устройств и процессора;
- Типы компьютерных устройств хранения информации и их носители;
- Использование компьютеров в системе обработки информации;
- Модель взаимодействия открытых систем (OSI);
- Сопряжение ЭВМ с каналами связи.

Учебная дисциплина «Системы и сети передачи информации»:

- Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам;
- Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа;
- Техническая защита конфиденциальной информации от специальных воздействий;
- Организация защиты конфиденциальной информации на объектах информатизации;
- Аттестация объектов информатизации по требованиям безопасности информации;
- Контроль состояния технической защиты конфиденциальной информации.

Учебная дисциплина «Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам»:

- Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа;
- Техническая защита конфиденциальной информации от специальных воздействий;
- Организация защиты конфиденциальной информации на объектах информатизации;
- Аттестация объектов информатизации по требованиям безопасности информации;
- Контроль состояния технической защиты конфиденциальной информации.

Учебная дисциплина «Меры и средства технической защиты конфиденциальной информации от несанкционированного доступа»:

- Техническая защита конфиденциальной информации от специальных воздействий;
- Организация защиты конфиденциальной информации на объектах информатизации;
- Аттестация объектов информатизации по требованиям безопасности информации;
- Контроль состояния технической защиты конфиденциальной информации.

Учебная дисциплина «Техническая защита конфиденциальной информации от специальных воздействий»:

- Физические процессы, возникающие при воздействии мощными электрическими и магнитными полями и токами на технические средства обработки информации;
- Угрозы безопасности информации от специальных электромагнитных воздействий;
- Организация и содержание работ по защите информации от преднамеренных силовых

	электромагнитных воздействий; – Меры и средства защиты конфиденциальной информации от специальных электромагнитных и электрических воздействий; – Экранирующие материалы и покрытия; – Экранирование электростатических, электродинамических полей и низкочастотных магнитных полей; – Конструкции экранирующих корпусов и их элементы; – Экранирующие системы зданий и помещений. Вводно-защитные устройства для зданий и помещений; – Фильтры, разрядники и поглощающие устройства для защиты технических средств обработки информации от электрических воздействий. Учебная дисциплина «Организация защиты конфиденциальной информации на объектах информатизации»: – Порядок планирования и организации работ в интересах обеспечения ТЗИ на защищаемых объектах информатизации; – Стадии создания системы защиты информации объекта информатизации; – Разработка руководства по защите информации; – Разработка аналитического обоснования необходимости создания системы защиты информации; – Разработка технического (частного технического) задания на создание системы защиты информации; – Особенности реализации требований по защите информации от НСД на эксплуатируемом (функционирующем) объекте информатизации; – Особенности реализации требований по защите информации от НСД при создании нового объекта информатизации в защищенном исполнении; – Особенности реализации требований по защите персональных данных. Учебная дисциплина «Аттестация объектов информатизации по требованиям безопасности информации»: – Нормативная правовая и методическая база системы аттестации объектов информатизации по требованиям безопасности информации; – Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации; – Организация аттестации защищаемого помещения по требованиям безопасности информации; – Организация аттестации автоматизированных систем по требованиям безопасности информации в части защиты от НСД; – Методы аттестационных испытаний; – Проверка подсистем защиты информации от НСД; – Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации и объекта информатизации. Программа и методики аттестационных испытаний объектов информатизации. Аттестат соответствия. Учебная дисциплина «Контроль состояния технической защиты конфиденциальной информации»: – Организация и порядок проведения контроля состояния ТЗКИ; – Методики оценки защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН; – Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН; – Проведение контроля защищенности конфиденциальной информации от утечки за счет

	ПЭМИН с использованием программно-аппаратных комплексов; − Проведение контроля защищенности речевой конфиденциальной информации от утечки по техническим каналам с использованием программно-аппаратных комплексов; − Методика инструментального контроля выполнения норм показателя защищенности акустической речевой конфиденциальной информации; − Методы и средства контроля защищенности акустической речевой конфиденциальной информации от утечки по техническим каналам.	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, метод рекомендации по лаб.работам, фонд оценочных средств.	1.Курс лекций программы ДПО «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» 2. Учебные пособия и профильная литература: • Новиков С.Н. «Методы защиты информации»; • Иванов А. В. «Оценка защищенности информации от утечки по виброакустическим каналам»; • Иванов А. В. «Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок»; • Иванов А. В. «Защита речевой информации от утечки по акустоэлектрическим каналам»; • Гончаров С.А. «Проектирование систем информационной безопасности»; • Крук Б.И. «Телекоммуникационные системы и сети»; • Величко В.В., Субботин Е.А., Шувалов В.П., Ярославцев А.Ф. «Телекоммуникационные системы и сети»; • Хорошевский В.Г. Архитектура вычислительных систем. • Хорев А.А. Техническая защита информации: учеб, пособие для студентов вузов. В 3 т. Т. 3. Контроль эффективности защиты информации. - М.: НПЦ «Аналитика», 2008. • Хорев А.А. Организация контроля эффективности противодействия техническим средствам разведки и защиты информации: учебное пособие. -М.: Министерство обороны Российской Федерации, 2006. • Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. - М.: «Горячая линия - Телеком», 2011. • Меньшаков Ю.К. Теоретические основы технических разведок.- М.: МГТУ им. Н.Э.Баумана, 2008. • Тупота В.И., Петигин А.Ф. Контроль защищенности средств вычислительной техники от утечки информации за счет побочных электромагнитных излучений. Учебное пособие. - Воронеж, 2010. 3. Методические рекомендации по лабораторным

		работам и практическим заданиям. 4. Оценочные средства в виде тестирующего комплекса
10.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	– АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС»), – Федеральное государственное бюджетное образовательное учреждение высшего образования Новосибирский государственный технический университет, НГТУ.
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	– АО «Информационные Технологии и Коммуникационные Системы» («ИнфоТеКС»); – АО «Позитив Текнолоджиз»