Аннотация

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

Наименование: «Информационная безопасность. Безопасность компьютерных систем и защита информации»

1.	Наименование образовательной организации	ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Информационная безопасность. Безопасность компьютерных систем и защита информации»
3.	Объем часов	72
4.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.04.01 Информационная безопасность. 10.05.02 Информационная безопасность телекоммуникационных систем
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	ООП магистратуры 10.04.01 Информационная безопасность, профиль «Безопасность компьютерных систем»; ООП специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Защита информации в радиосвязи и телерадиовещании».
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.034. «Специалист по технической защите информации»
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: • Законодательство Российской Федерации в области технической защиты конфиденциальной информации; • Порядок создания, развития, ввода в эксплуатацию и вывода из эксплуатации информационных (автоматизированных) систем; • Порядок реализации требований по технической защите конфиденциальной информации на всех этапах жизненного цикла информационной системы; • Порядок разработки модели угроз безопасности информации и технического задания на создание системы защиты информации; • Порядок проведения оценки соответствия требованиям по технической защите конфиденциальной информации; • Порядок эксплуатации информационных (автоматизированных) систем; • Порядок проведения анализа защищенности информационных (автоматизированных) систем. **Уметь:** • Применять законодательство Российской Федерации в области технической защиты конфиденциальной информации**;** • Реализовывать требования по технической защите конфиденциальной информации на всех этапах жизненного цикла информационной (автоматизированной) системы; • Разрабатывать модели угроз безопасности информации и технического задания на создание системы защиты информации;	

	• Проводить оценку соответствия требованиям по технической защите конфиденциальной информации; • Проводить анализ защищенности информационных систем (объектов информатизации).	
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	Модуль 1. Требования законодательства РФ по защите компьютерных систем (КС) и информации Модуль 2. ФСТЭК РФ: Методика оценки способов реализации (возникновения) угроз безопасности информации и КС (Утвержден ФСТЭК России 5 февраля 2021 г.) Модуль 3. Реализация системного подхода как комплекс взаимосвязанных мер для предотвращения и раннего обнаружения атак Модуль 4.Методы и средства информационной безопасности, защита информации в компьютерных сетях	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, методрекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Информационная безопасность. Безопасность компьютерных систем и защита информации» 2. Учебные пособия по программе «Информационная безопасность. Безопасность компьютерных систем и защита информации» **(**методические рекомендации для выполнения лабораторных и практических работ; 3. Оценочные средства ДПО в виде тестирующего комплекса.
10.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Системный интегратор ПО Softline ООО «Код Безопасности» Компания «Информзащита» ООО «ИТЛИС» ФГУП РТРС АО «Воентелеком»
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	Модули ПО АО «Лаборатория Касперского» Модули ПО ООО «КРИПТО-ПРО» Модули ПО АО «ИнфоТеКС»

Аннотация

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

Наименование: «Кибербезопасность автоматизированных систем»

	Наименование образовательной организации	ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Кибербезопасность автоматизированных систем»
	Объем часов	72
	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.04.01 Информационная безопасность. 10.05.02 Информационная безопасность телекоммуникационных систем
	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	ООП магистратуры 10.04.01 Информационная безопасность, профиль «Безопасность компьютерных систем»; ООП специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Защита информации в радиосвязи и телерадиовещании»
	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.032 «Специалист по безопасности компьютерных систем и сетей»; 06.033 «Специалист по защите информации в автоматизированных системах»; 06.034 «Специалист по технической защите информации»
	Ключевые результаты обучения: (знать, уметь)	
	Знать: • Методику оценки угроз безопасности инфорации(разработка ФСТЭК РФ,05.02.2021г) • Виды киберугроз, их действия, риски и противодействие • Действия по защите компьютерных сетей от различных угроз, целевых атак и вредоносных программ • Средства защиты уровня приложений • Методы и средства защиты обеспечения целостности и конфиденциальности данных при хранения и при передаче по сети • Средства защиты информационных активов и управление разрешениями для доступа к сети и правила хранения данных • Процессы аварийного восстановления и непрерывность бизнеса - реагирование на инцидент безопасности	

- Набор правил о ликвидации последствий атаки и восстанавления рабочих процессов
- План действий при потере доступа к определенным ресурсам организации из-за атаки злоумышленников.
- Средства повышения осведомленности для снижения влияния человеческого фактора в области кибербезопасности
- Методы сбора информации
- Средства анализа уязвимостей приложений на уровне ОС
- Методы обнаружения вредоносного ПО, инструменты сниффинга и меры его противодействия
- Инструменты для перехвата сеанса Атаки Man-in-the-Middle («человек посередине»)
- Меры противодействия DOS-атак
- Специфика и особенности «Программ-вымогателей»
- Типы SQL-инъекций
- Уязвимости интернета вещей и операционных технологий

Уметь:

- Использовать разработку модели угроз безопасности и ее этапы(ФСТЭК РФ, 05.02.2021г)
- Применять техники по сбору информации
- Сканировать и идентифицировать сервисы ПК
- Применять техники снифинга при DOS-атаке
- Использовать инструмент NESSUS для инвентаризации уязвимостей компьютеров
- Применять техники по взлому паролей и повышению привилегий в ОС
- Использовать защитные инструменты для изоляции потенциального вредоносного ПО(вирусы и троянцы) в специальной виртуальной среде
- Применять техники перехвата сеанса для получения доступа к ресурсам учебных серверов
- Исследовать возможности уклонения от систем обнаружения
- Выполнять отражение и сохранение XSS-атаки
- Применять средства для выполнения SQL инъекции
- Применять меры противодействия атакам на беспроводные сети

Дидактика программы (наименования модулей (дисциплин), разделов (тем).

Модуль 1.Требования законодательства РФ по защите информационных компьютерных систем;
Модуль 2.Анализ защищенности информационных компьютеных систем:методика оценки угроз безопасности инфорации(разработка ФСТЭК РФ,05.02.2021г)
Модуль 3. Анализ уязвимостей:системы и инструменты оценки
Модуль 4. Снифферы и меры противодействия сниффингу
Модуль 5. Социальная инженерия и меры противодействия социальной инженерии
Модуль 6. Отказ в обслуживании и меры противодействия Dos-атакам
Модуль 7. Перехват сеанса и меры противодействия перехвата сеанса
Модуль 8.Обход систем обнаружения вторжений, фаерволлов и меры противодействия
Модуль 9. Кибер-атаки

Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, методрекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Кибербезопасность автоматизированных систем» 2. Учебные пособия по программе «Кибербезопасность автоматизированных систем»; методические рекомендации для

		выполнения лабораторных и практических работ; 3. Оценочные средства ДПО в виде тестирующего комплекса
	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Системный интегратор ПО Softline АО «ИнфоТеКС» ООО «Код Безопасности» Компания «Информзащита» ООО «ИТЛИС» АО «Воентелеком»
	Используемые отечественные ПО и средства защиты информации (при наличии)	Модули ПО АО «Лаборатория Касперского» Модули ПО ООО «КРИПТО-ПРО» Модули ПО АО «ИнфоТеКС»

Аннотация

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

Наименование: «Социально-психологические и правовые аспекты информационной безопасности»

1	Наименование образовательной организации	ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
2	Наименование программы ДПО (в т.ч. повышение квалификации/профессиональная переподготовка)	Программа повышения квалификации «Социально-психологические и правовые аспекты информационной безопасности»
3	Объем часов	72
4	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.04.01 Информационная безопасность. 10.05.02 Информационная безопасность телекоммуникационных систем
5	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	ООП магистратуры 10.04.01 Информационная безопасность, профиль «Безопасность компьютерных систем»; ООП специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Защита информации в радиосвязи и телерадиовещании»
6	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.030 «Специалист по защите информации в телекоммуникационных системах и сетях»
7	Ключевые результаты обучения: (знать, уметь)	
	Знать: • сущность технологий конструирования социальной реальности в виртуальном пространстве; • особенности формирования и влияния угроз и рисков, связанных с Интернет-средой; • типы и модели информационных кампаний в новых социально-экономических условиях; • модели информационного противоборства. • принципы и инструментарий пропагандистской кампании и психологической войны; • основные методы оценки поражающих факторов информационного оружия, надежных средствах констатации его применения; • алгоритмы различения информационной войны, контрпропаганды, антирекламы; • основные технологии создания информационных фреймов и манипуляций в информационном пространстве; • методы анализа социальных сетей и массовых коммуникаций; • особенности управления репутационным риском в информационном пространстве; • нормативные правовые акты, регламентирующие содержание информационного контента и информационные отношения.	

	Уметь: • анализировать тенденции и противоречия современного информационное пространства; • планировать проведение информационных кампаний по противодействию негативному информационному влиянию; • учитывать в практической деятельности особенности информационных кампаний в новых социально-экономических условиях; • выявлять и распознавать фейки и манипуляции; • выявлять скрытый смысл пропагандистской кампании; • подготавливать комплекс мер по нейтрализации деструктивного информационного влияния на определённые группы пользователей сети Интернет • готовить ряд информационных материалов, снижающих эффект негативного информационного влияния; • оценивать репутационные риски в информационном пространстве; • применять законодательство Российской Федерации в области СМИ в интересах противодействия негативному информационному влиянию.	
8	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	Модуль 1. Информационное противоборство как способ достижения целей и удовлетворения групповых интересов. Модуль 2. Практики противодействия негативному информационному влиянию. Модуль 3. Законодательное регулирование информационной безопасности.	
9	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, методрекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Социально-психологические и правовые аспекты информационной безопасности» 2. Учебные пособия по программе «Социально-психологические и правовые аспекты информационной безопасности» **(**методические рекомендации для выполнения лабораторных и практических работ; 3. Оценочные средства ДПО в виде тестирующего комплекса.
10	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	ФГУП РТРС Компания «Информзащита» ООО «ИТЛИС»
11	Используемые отечественные ПО и средства защиты информации (при наличии)	Модули ПО АО «Лаборатория Касперского»

Аннотация

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

Наименование: «Тестирование уязвимостей»

33.	Наименование образовательной организации	Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
34.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Тестирование уязвимостей»
35.	Объем часов	72
36.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.03.01 Информационная безопасность. 10.04.01 Информационная безопасность. 10.05.02 Информационная безопасность телекоммуникационных систем.
37.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	ООП бакалавриата 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем»; ООП магистратуры 10.04.01 Информационная безопасность, профиль «Безопасность компьютерных систем»; ООП специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Управление безопасностью телекоммуникационных систем и сетей».
38.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.030 «Специалист по защите информации в телекоммуникационных системах и сетях»; 06.032 «Специалист по безопасности компьютерных систем и сетей»; 06.033 «Специалист по защите информации в автоматизированных системах»; 06.034 «Специалист по технической защите информации».
39.	Ключевые результаты обучения: (знать, уметь)	
	Знать: • Требования законодательства РФ в части анализа защищенности информационных телекоммуникационных и компьютерных систем; • Методы, способы и средства анализа защищенности информационных систем; • Современные угрозы и векторы атак; • Процессы управления информационной безопасностью; • Методы сбора информации; • Техники сканирования сетей; • Меры противодействия перечислению; • Средства анализа уязвимостей; • Слабые точки архитектуры ОС; • Возможности Linux ОС и Windows ОС; • Основы работы в Cisco IOS; • Скриптовые языки программирования: Python, Powershell. Основы скриптинга;	

	• Сетевые подсистемы Windows /Linux. **Уметь:** • Управлять групповыми политиками, работать с сервисами DNS & DHCP; • Управлять Active Directory, Windows Server & Доменными сервисами; • Применять основы работы в Cisco IOS, модификации пакетов и работы с их структурой; • Проводить сканирование сетей и анализ трафика; • Применять OSINT & Киберразведку; • Производить защиту от атаки на Wi -fi и взлом паролей; • Выполнять поднятие привилегий в Linux, Windows; • Производить атаки на сервисы и порты; • Владеть реверс-инжиниринг и анализом вредоносного ПО.	
40.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	Модуль 1. Требования законодательства Российской Федерации в части анализа защищенности информационных (телекоммуникационных и компьютерных) систем; Модуль 2. Основы: криптографии, управление сервисами, сетью и менеджеры пакетов, пользователями, группами и правами, введение в Linux ОС; Модуль 3. Windows Server: управление групповыми политиками, работа с сервисами DNS & DHCP, управление Active Directory, Windows Server & Доменные сервисы; Модуль 4. Сети (Cisco): Основы сетевой инфраструктуры и базовая сегментация сети (VLANs и Trunk , основы сетевой инфраструктуры, безопасность коммутаторов), основы работы в Cisco IOS, модификация пакетов и работа с их структурой, сетевые подсистемы Windows /Linux; Модуль 5. Программирование: скриптовые языки программирования (Python, Powershell), Bash; Модуль 6. Кибер-инфраструктура для пентестинга: сканирование сетей и анализ трафика, OSINT & Киберразведка, MITM, атаки на Wi -fi и взлом паролей; Модуль 7. Повышение кроссплатформенных привилегий: Windows "Unquoted Service" и подмена DLL, поднятие привилегий в Linux и постэксплуатация, Windows постэксплуатация и дампинг паролей, поднятие привилегий в Windows; Модуль 8. Атаки на сетевую инфраструктуру: PowerShell - инструмент атак, эксплуатация ПО Office, атака на сервисы и порты, реверс - шелл и туннели, Kerberoasting & Pass the Ticket; Модуль 9. Реверс-инжиниринг и анализ вредоносного ПО: IDA & Ghidra, отладка с ollyDBG & x64dbg, GDB.	
41.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, методрекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Тестирование уязвимостей»; 2. Учебные пособия по программе «Тестирование уязвимостей»; методические рекомендации для выполнения лабораторных и практических работ; 3. Оценочные средства ДПО в виде тестирующего комплекса.
42.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Системный интегратор ПО Softline АО «ИнфоТеКС» ООО «Код Безопасности» Компания «Информзащита» ООО «ИТЛИС» АО «Воентелеком» ФСТЭК России
43.	Используемые отечественные ПО и средства защиты информации (при наличии)	Модули ПО АО «Лаборатория Касперского» Модули ПО ООО «КРИПТО-ПРО» Модули ПО АО «ИнфоТеКС»

Аннотация

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

Наименование: «Управление информационной безопасностью»

44.	Наименование образовательной организации	ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
45.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа повышения квалификации «Управление информационной безопасностью»
46.	Объем часов	72
47.	Специальность/направление (ФГОС 3++), по которым реализуется ППК «УИБ»	10.03.01 Информационная безопасность. 10.04.01 Информационная безопасность. 10.05.02 Информационная безопасность телекоммуникационных систем. 10.05.03 Информационная безопасность автоматизированных
48.	Учебная дисциплина (ПООП, ООП), ассоциированная с ППК «УИБ»	ООП бакалавриата 10.03.012 Информационная безопасность, дисциплина «Основы управления информационной безопасностью». ООП магистратуры 10.04.01 Информационная безопасность, дисциплина «Управление информационной безопасностью». ООП специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, дисциплина «Управление информационной безопасностью». ООП специалитета 10.05.03 Информационная безопасность автоматизированных систем».
49.	Профессиональный стандарт, ассоциированный с ППК «УИБ» (ТФ, ОТФ при необходимости)	06.030. «Специалист по защите информации в телекоммуникационных системах и сетях». 06.033. «Специалист по защите информации в автоматизированных системах»
50.	Ключевые результаты обучения: (знать, уметь)	
	Знать: • Терминологию в области ИБ; • Правовую и нормативную базу управления ИБ (УИБ); • Виды объектов обеспечения ИБ (ОИБ); • Особенности управленческого подхода при ОИБ; • Особенности процессного подхода при ОИБ; • Особенности риск-ориентированного подхода при ОИБ; • Особенности контроля ИБ; • Особенности обеспечения непрерывности ИБ. **Уметь:** • Использовать терминологию в области ИБ; • Применять нормативную базу УИБ; • Проводить анализ объектов ОИБ и идентификацию их активов; • Проводить оценку угроз ИБ;	

	• Осуществлять выбор процессов и мер защиты информации, процессов и мер обеспечения ИБ; • Разрабатывать политики обеспечения ИБ.	
51.	Дидактика ППК «УИБ» (наименования модулей (дисциплин), разделов (тем).	
	Модуль 1. Введение: 1.1.Введенние (для ППК «УИБ» 1.2.Введение (для дисциплин, относящихся к УИБ) Модуль 2. Теоретические основы УИБ: 2.1.Систематика понятий в области ИБ 2.2.Объекты обеспечения ИБ (ОИБ). 2.3.Концептуальные основы обеспечения ИБ. 2.4.Нормативная база УИБ. 2.5.Системотехника ИБ. Модуль 3.Процессы управления ИБ: 3.1.Процесс управления рисками ИБ. 3.2.Процесс управления инцидентами ИБ. 3.3.Процесс управления контролем ИБ. 3.4.Процесс управления обеспечения непрерывности ИБ Модуль 4. Практические вопросы управления ИБ. 4.1.Описание объектов ОИБ. 4.2.Идентификация активов объектов ОИБ. 4.3.Анализ угроз ИБ. 4.4.Выбор процессов и мер защиты информации, процессов управления и мер ОИБ. 4.5.Разработка политик обеспечения ИБ. Модуль 5.Особенности реализации дисциплин, относящихся к УИБ. Модуль 6.Оценка результатов проведения занятий по ППК «УИБ».	
52.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, методрекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Управление информационной безопсностью»; 2. Учебные пособия по программе «Управление информационной безопсностью»; методические рекомендации для выполнения лабораторных и практических работ; 3. Оценочные средства ДПО в виде тестирующего комплекса.
53.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Системный интегратор ПО Softline АО «ИнфоТеКС» ФГУП «НПП «Гамма» ООО «Код Безопасности» Компания «Информзащита»
54.	Используемые отечественные ПО и средства защиты информации (при наличии)	Модули ПО АО «Лаборатория Касперского» Модули ПО ООО «КРИПТО-ПРО» Модули ПО АО «ИнфоТеКС»

Аннотация

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

Наименование: «Информационная безопасность»

55.	Наименование образовательной организации-разработчика программы	ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
56.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа профессиональной переподготовки «Информационная безопасность»
57.	Объем часов	360
58.	Специальность/направление (ФГОС 3++), по которым реализуется программа	10.04.01 Информационная безопасность. 10.05.02 Информационная безопасность телекоммуникационных систем
59.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	ООП магистратуры 10.04.01 Информационная безопасность, профиль «Безопасность компьютерных систем»; ООП специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Защита информации в радиосвязи и телерадиовещании»
60.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.032 «Специалист по безопасности компьютерных систем и сетей»; 06.033 «Специалист по защите информации в автоматизированных системах»; 06.034 «Специалист по технической защите информации»
61.	Ключевые результаты обучения: (знать, уметь)	
	Знать: • Нормативные правовые акты, методические документы и национальные стандарты в области обеспечения информационной безопасности; • Виды конфиденциальной информации, перечни сведений конфиденциального характера; • Средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; • Требования по ТЗКИ; • Организацию и содержание проведения работ по контролю (мониторингу) защищенности конфиденциальной информации, состав и содержание необходимых документов; • Принципы построения и функционирования систем и сетей передачи информации; • Особенности защиты информации в автоматизированных системах управления технологическими процессами; • Принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем; • Методы и методики контроля (мониторинга) защищенности конфиденциальной информации; • Порядок проведения контроля (мониторинга) информационной безопасности средств и систем информатизации. **Уметь:**	

	• Применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области информационной безопасности; • Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; • Классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; • Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; • Выбирать меры защиты информации; • Определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий; • Формировать требования по ТЗКИ; • Организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации.	
62.	Дидактика программы (наименования модулей (дисциплин), разделов (тем).	
	Раздел 1. Правовое регулирование защиты информации в Российской Федерации. Раздел 2. Комплексная система защиты информации в организации. Раздел 3. Защита конфиденциальной информации от утечки по техническим каналам. Раздел 4. Защита конфиденциальной информации от несанкционированного доступа. Раздел 5. Перспективные технологии защиты информации для педагогических кадров Раздел 6. Криптографическая (с помощью шифровальных средств) защита конфиденциальной информации.	
63.	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 по программе «Информационная безопасность»; методические рекомендации для выполнения лабораторных и практических работ; 3. Оценочные средства ДПО в виде тестирующего комплекса.
64.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	АО «ИнфоТеКС» ООО «Код Безопасности» Компания «Информзащита» ООО «ИТЛИС» ФГУП «НПП «Гамма»
65.	Используемые отечественные ПО и средства защиты информации (при наличии)	Модуль шифрования «Квазар» Модули ПО АО «Лаборатория Касперского»

Аннотация

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

Наименование: «Информационная безопасность. Техническая защита конфиденциальной информации»

1.	Наименование образовательной организации	Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
2.	Наименование программы ДПО (в т.ч. повышение квалификации / профессиональная переподготовка)	Программа профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации»
3.	Объем часов	390
4.	Специальность / направление (ФГОС 3++), по которым реализуется программа	10.03.01 Информационная безопасность. 10.04.01 Информационная безопасность. 10.05.02 Информационная безопасность телекоммуникационных систем.
5.	Учебная дисциплина (ПООП, ООП), ассоциированная с программой	ООП бакалавриата 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем»; ООП бакалавриата 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»; ООП магистратуры 10.04.01 Информационная безопасность, программа «Безопасность компьютерных систем»; ООП специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей».
6.	Профессиональный стандарт, ассоциированный с программой (ТФ, ОТФ при необходимости)	06.030 «Специалист по защите информации в телекоммуникационных системах и сетях»; 06.032 «Специалист по безопасности компьютерных систем и сетей»; 06.033 «Специалист по защите информации в автоматизированных системах»; 06.034 «Специалист по технической защите информации».
7.	Ключевые результаты обучения: (знать, уметь)	
	Знать: • нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ; • основы функционирования государственной системы противодействия (ПД) иностранным техническим разведкам (ИТР) и ТЗИ, цели и задачи ТЗКИ; • виды конфиденциальной информации, перечни сведений конфиденциального характера; • возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий; • действующую систему сертификации средств защиты информации по требованиям безопасности информации;	

	• основы лицензирования деятельности по ТЗКИ; • требования по ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения); • организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов; • организацию и содержание проведения работ по контролю (мониторингу) защищенности конфиденциальной информации, состав и содержание необходимых документов; • правила разработки, утверждения, обновления и отмены документов в области ТЗКИ; • типовую структуру, задачи и полномочия подразделения по ТЗИ; • принципы работы основных узлов современных технических средств информатизации; • основы построения информационных систем и формирования информационных ресурсов, принципы построения и функционирования операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основные протоколы компьютерных сетей; • типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащенности техническими средствами; • технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами; • способы (методы) и требования по ТЗКИ; • 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; • методы и методики контроля (мониторинга) защищенности конфиденциальной информации; • порядок проведения контроля (мониторинга) информационной безопасности средств и систем информатизации; • требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации; • средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации, порядок их применения, перспективы развития; • порядок проведения аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации; • 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; • программы и методики аттестационных испытаний и аттестации объекта информатизации на соответствие требованиям по защите информации; • порядок установки, монтажа, испытаний средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации; • порядок устранения неисправностей и проведения ремонта (технического обслуживания) ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации. **Уметь:** • применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ; • разрабатывать необходимые документы в интересах проведения работ по ТЗКИ; • определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий; формировать требования по ТЗКИ; • определять требования к средствам ТЗКИ на объектах информатизации; организовывать и проводить работы по ТЗКИ; • организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля; • применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;

	• проводить аттестационные испытания и аттестацию объектов информатизации на соответствие требованиям по защите информации, оформлять материалы аттестационных испытаний; • разрабатывать программы и методики аттестационных испытаний и аттестации объектов информатизации; • осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных; • проводить установку, монтаж, испытания и техническое обслуживание средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации; • устранять неисправности и проводить ремонт (техническое обслуживание) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации; • разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ТЗКИ для их представления в лицензирующий орган.	
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем)).	
	Раздел 1. Нормативно-правовые основы обеспечения информационной безопасности в Российской Федерации Раздел 2. Средства и системы передачи, обработки и хранения информации Раздел 3. Техническая защита информации от утечки по техническим каналам Раздел 4. Меры и средства технической защиты конфиденциальной информации от НСД Раздел 5. Обеспечение безопасности персональных данных при их обработке в ИСПДн Раздел 6. Программно-аппаратная защита информации Раздел 7. Защита информации ограниченного доступа с использованием криптографических средств Раздел 8. Организационно-технические и правовые основы использования в информационных системах электронного документооборота и электронной подписи	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, методрекомендации по лаб.работам, фонд оценочных средств.	1. Курс лекций программы ДПО «Информационная безопасность. Техническая защита конфиденциальной информации»; 2. Учебные пособия по программе «Информационная безопасность. Техническая защита конфиденциальной информации»; методические рекомендации для выполнения лабораторных и практических работ; 3. Оценочные средства ДПО в виде тестирующего комплекса.
10.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	ООО «Код Безопасности» НИУ МИЭТ Компания «Информзащита» ФСТЭК России ФГУП «НПП «Гамма»
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	Средства защиты информации: - центр управления сетью АПКШ «Континент»; - криптошлюз + сервер доступа АПКШ «Континент»; - детектор атак АПКШ «Континент»; - программно-аппаратный комплекс «Соболь»; - центр управления сетью + сервер доступа АПКШ «Континент»; - криптокоммутатор АПКШ «Континент»; - детектор атак АПКШ «Континент». Программное обеспечение: - ПАК Соболь управление шаблонами КЦ; - Континент АП.