Аннотация программы ДПО в области ИБ для обучения ППС

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 «Криптоанализ в комплексных системах обеспечения информационной безопасности на проникновение»
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)	06.032 «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: • 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, • Методы обнаружения вредоносного • ПО, инструменты сниффинга и меры его противодействия • Социальной инженерии, • Меры противодействия DDOS-атак, • Инструменты для перехвата сеанса, • Инструменты обхода фаерволлов, • Инструменты взлома веб-серверов и меры противодействия • Инструменты защиты веб-приложений, • Типы SQL-инъекций, • Методы взлома беспроводных сетей и меры противодействия • Инструменты по защите мобильных устройств, • Инструменты атак на ИВ(Интернет Вещей) и меры противодействия, **Уметь:** • Применять техники по сбору информации • Сканировать и идентифицировать сервисы ПК • Применять техники перечисления • Использовать инструмент NESSUS для инвентаризации уязвимостей компьютеров • Применять техники по взлому паролей и повышению привилегий в ОС • Тестировать работы шелл- трояна,реверсного трояна,скрытого трояна • Применять техники активного сниффинга для получения передаваемых по сети данных и	

	подмены запросов • Применять наборы средств социальной инженерии SET из состава KALI LINUX • Применять техники DOS-атаки для вывода из строя сервисов учебных серверов • Применять техники перехвата сеанса для получения доступа к ресурсам учебных серверов • Исследовать возможности уклонения от систем обнаружения • Использовать Дефейс учебного веб-сервера посредством эксплуатации уязвимости с помощью MetasPloit FrameWork • Выполнять отражение и сохранение XSS-атаки • Взламывать учебный сервер с помощью SQL- инъекций • Находить точки доступа,сниффинг, де-аутентификация,взлом ключей WEP,WPA,WPA-2 и расшифровывание Wi-Fi трафика • Изучить уязвимости Интернета Вещей и операционных технологий • Изучить атаки на облака и инструменты защиты облачных вычислений • Изучить алгоритмы шифрования и средства стеганографии	
8.	Дидактика программы (наименования модулей (дисциплин), разделов (тем). Модуль 1. Введение в криптоанализ Модуль 2. Сбор информации Модуль 3. Сканирование Модуль 4. Перечисление Модуль 5. Анализ уязвимостей Модуль 6. Криптоанализ системы Модуль 7. Трояны и другое вредоносное ПО Модуль 8. Снифферы Модуль 9. Социальная инженерия Модуль 10. Отказ в обслуживании Модуль 11. Перехват сеанса Модуль 12. Обход систем обнаружения вторжений, фаерволлов и систем ловушек Модуль 13. Криптоанализ веб-серверов Модуль 14. Криптоанализ веб- приложений Модуль 15. SQL- инъекции Модуль 16. Криптоанализ беспроводных сетей Модуль 17. Взлом мобильных платформ Модуль 18. Криптоанализ интернета вещей и операционных технологий Модуль 19. Облачные вычисления Модуль 20. Криптография и инфраструктура современных шифров	
9.	Планируемое обеспечение программы (УМК), перечислить: курс лекций, учебное пособие, методрекомендации по лаб.работам, фонд оценочных средств.	Курс лекций в формате презентаций. Курс лекций в формате On line/remote трансляция и Вебинар- записи Основная литература : 1. Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом: учебное пособие / Ю. А. Котов. — Новосибирск: Новосибирский государственный технический университет, 2017. — 67 с. — ISBN 978-5- 7782-3411-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91227.html 2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с. 3. Зегжда Д.П. Основы безопасности информационных систем - М.: Горячая линия - Телеком, 2000. 4. Прохорова О.В. Информационная безопасность и

		защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с. 5. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: учеб, пособие. - М.: ИТК «Дашков и К», 2006. -336 с. 6. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф. — Электрон. текстовые данные. — М.: ДМК Пресс, 2017. — 702 с. 7. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации / составители А.Э. Смирнов, Ю.А. Пономарёва. — Москва: Московский технический университет связи и информатики, 2015. — 67 с. — ISBN 2227- 8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/61738.html Методические рекомендации для выполнения лабораторных и практичеких работ. ФОС: промежуточная аттестация- защита лабораторных и практических работ/тестирование
10.	Фирмы-производители средств защиты информации, внешние образовательные организации, которые будут привлечены к реализации программы или отдельные представители организаций.	Системный интегратор ПО Microsoft Системный интегратор ПО Softline ООО «Код Безопасности» Компания «Информзащита» ООО «ИТЛИС»
11.	Используемые отечественные ПО и средства защиты информации (при наличии)	Модули ПО АО «Лаборатория Касперского» Модули ПО ООО «КРИПТО-ПРО»

Руководитель проекта

Директор ИПК МТУСИ Воскобович В.В.