Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Казанский национальный исследовательский технический университет
им. А.Н. Туполева – КАИ» (КНИТУ-КАИ)

«УТВЕРЖДАЮ»
Директор Корпоративного института
КНИТУ-КАИ
_____А.А. Лопатин
«02» 03 2015 г.

ПРОГРАММА
дополнительного профессионального образования
(повышения квалификации)
Расследование компьютерных инцидентов
(полное наименование программы ДПО)

Казань, 2015

I. КРАТКАЯ АННОТАЦИЯ ПРОГРАММЫ ДПО

Справочные данные	
Наименование структурного подразделения, реализующего программу	Кафедра Систем информационной безопасности
Название программы ДПО	Расследование компьютерных инцидентов
Научный руководитель рабочей группы по разработке программы ДПО (Ф.И.О., должность)	Аникин Игорь Вячеславович, заведующий кафедрой Систем информационной безопасности
Краткая характеристика образовательной программы	
УГС, направление подготовки	090000 «Информационная безопасность»
Вид профессиональной деятельности, на который ориентирована программа	Информационная безопасность
Краткое описание образовательной программы	В программе переподготовки приобретаются знания, умения, навыки, относящиеся к расследованию компьютерных инцидентов
Объем программы, в час./срок обучения, дней	72 часа / 9 дней
Реализуемые формы обучения	С отрывом от работы

2. УЧЕБНЫЙ ПЛАН

№ п/п	Наименование модулей	Всего часов	В том числе	
			Лекции	Практические (лабораторные) занятия
1	Модуль 1. Основы информационной безопасности	10	6	4
2	Модуль 2. Компьютерные сети и безопасность компьютерных сетей	20	6	14
3	Модуль 3. Противодействие утечкам информации по техническим каналам	12	6	6
4	Модуль 4. Методы и средства расследования компьютерных инцидентов	30	10	20
	ИТОГО:	**72**	**28**	**44**

Форма итоговой аттестации по программе: выпускная квалификационная работа.

Слушателям, успешно завершившим курс обучения (выполнившим все требования учебного плана) выдаются удостоверения о прохождении курсов.

3. ПРОГРАММА ОБУЧЕНИЯ

Основы информационной безопасности

Субъекты и объекты доступа. Санкционированный и несанкционированный доступ. Конфиденциальность, целостность и доступность информации. Угрозы информационной безопасности, уязвимости, риски. Основные источники и пути реализации угроз. Классификация угроз безопасности. Анализ и управление рисками информационной безопасности. Каналы утечки информации и их классификация. Идентификация и аутентификация, разграничение доступа, регистрация и аудит, контроль целостности, криптографические механизмы обеспечения конфиденциальности, целостности и аутентичности информации.

Компьютерные сети и безопасность компьютерных сетей

Типовая IP-сеть организации. Сетевые угрозы, уязвимости и атаки. Средства обнаружения уязвимостей узлов IP-сетей и атак на узлы, протоколы и сетевые службы. Получение оперативной информации о новых уязвимостях и атаках. Способы устранения уязвимостей и противодействия вторжениям нарушителей.

Средства защиты информации в компьютерных сетях. Межсетевые экраны. Виртуальные частные сети. Протоколы аутентификации в компьютерных сетях. Сканеры безопасности и системы обнаружения вторжений.

Противодействие утечкам информации по техническим каналам

Классификация технических каналов утечки информации. Общая характеристика технических каналов утечки информации и их классификация. Каналы утечки речевой информации, информации, обрабатываемой техническими средствами, видовой информации.

Каналы утечки речевой информации: акустический, виброакустический, акустоэлектрический, оптикоэлектронный. Характеристика каждого канала, механизмы возникновения, технические средства и методы получения информации по этим каналам.

Утечка информации по проводным коммуникациям и за счет побочных электромагнитных излучений и наводок (ПЭМИН). Механизмы возникновения каналов утечки информации. Технические средства и методы получения информации с использованием этих каналов.

Общие принципы и методы выявления каналов утечки информации, методы выявления отдельно по каждому из технических каналов. Классификация аппаратуры выявления каналов утечки информации. Обзор моделей каждого вида аппаратуры, краткие технические характеристики.

Методы и средства расследования компьютерных инцидентов

Ответственность за совершение преступлений в сфере компьютерной информации в России.

Особенности образования следов по делам о компьютерных преступлениях

Обнаружение, фиксация и изъятие следов компьютерных преступлений. Сбор информации о ПЭВМ. Особенности проведения компьютерно-технических экспертиз.

Обход парольных систем идентификации и аутентификации в компьютерных системах. Использование и обход систем шифрования данных ПЭВМ. Поиск релевантной информации на носителях информации.

Особенности расследования преступлений: по взломам систем ДБО, игровым автоматам, скиммерам, вредоносному ПО.

Перечень рекомендуемой основной и дополнительной литературы, электронных источников информации.

Основные источники:

1. Аникин, Игорь Вячеславович. Методы и средства защиты компьютерной информации : учеб. пособие для студ. вузов / И. В. Аникин, В. И. Глова ;, 2008. Мин-во образ-я и науки РФ, Фед. агентство по образованию, ГОУ ВПО "КГТУ им. А.Н. Туполева". - Казань : Изд-во КГТУ им. А.Н. Туполева - 262 с.

2. Теория информационной безопасности и методология защиты информации : учеб. пособие / И. В. Аникин, В. И. Глова, Л. И. Нейман, А.Н. Нигматуллина. Мин-во образ-я и науки РФ, Фед. агентство по образованию, ГОУ ВПО "КГТУ им. А.Н. Туполева". - Казань : Изд-во КГТУ им. А.Н. Туполева, 2008. - 280 с.

3. Малюк, Анатолий Александрович. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов / А.А. Малюк, М. : Горячая линия – Телеком, 2004. - 280 с.

Дополнительные источники:

1. Хорев, Павел Борисович. Методы и средства защиты информации в компьютерных системах : учеб. пособие для вузов / П.Б. Хорев. - М. : Академия, 2005.

2. Общесистемные вопросы защиты информации : коллективная монография. Кн. 1 / А. В. Бердышев [и др.] ; под ред. Е. М. Сухарева. - М. : Радиотехника, 2003. - 296 с.

Электронные источники информации:

1. Макаренко С.И. Информационная безопасность: Учебное пособие для студентов вузов. - Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. - 371 с. [Электронный ресурс] // http://window.edu.ru/resource /775/77775/ files/Книга %20ИБ%20_МГГУ_%20- %201.5.3%20_full-print_5_A5.pdf

2. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. - СПб.: СПбГУ ИТМО, 2010. - 98 с. [Электронный ресурс] // http://window.edu.ru/ resource/984/71984 /files/itmo477.pdf