ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»

ЧУ ДПО "ЦИТ БИС"

Подписано цифровой подписью: ЧУ ДПО "ЦИТ БИС"
DN: email=edu@astralnalog.ru, 1.2.643.3.131.1.1=120C303034303237303936363335, 1.2.643.100.3=120B303038393331313 5313432, 1.2.643.100.1=120D313039343030303 03031313530, street=ул Циолковского 4 212, c=RU, st=40 Калужская область, l=г Калуга, o=ЧУ ДПО "ЦИТ БИС", title=Директор, givenName=Игорь Ильич, sn=Чернин, cn=ЧУ ДПО "ЦИТ БИС"
Дата: 2022.01.20 10:40:29 +03'00'

УТВЕРЖДАЮ

Директор ЧУ ДПО
«ЦИТ БИС»

_____ И.И. Чернин
«___»_____2017г

Дополнительная профессиональная программа повышения квалификации
специалистов по защите информации по направлению «Информационная безопасность»

«Комплексное обеспечение информационной безопасности автоматизированных систем. Криптографические средства и методы защиты информации»

(108 академических часов)

г.Калуга
2017

1.Общие положения.

Программа «Комплексное обеспечение информационной безопасности автоматизированных систем. Криптографические средства и методы защиты информации» разработана в соответствии со статьями 12, 13 и главой 10 Федерального закона от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации" и «Порядком организации и осуществления образовательной деятельности по дополнительным профессиональным программам» утвержденным приказом Минобрнауки России от 01.07.2013 № 499, с учетом федеральнах государственных образовательных стандартов, утвержденных приказами Минобрнауки России от 23.06.2010 № 681, от 28.10.2009 №497 и №496. При разработке программы выполнены требования по разработке дополнительных профессиональных программ, утвержденные приказом Минобразования России от 05.12.2013 № 1310.

2.Цель реализации дополнительной профессиональной программы.

Целью реализации дополнительной профессиональной программы является формирование и (или) совершенствование у слушателей компетенций в области информационной безопасности, а именно освоение руководителями подразделений и специалистами по информационной безопасности знаний и актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ в области технической защиты информации, в соответствии с современными требованиями.

Задачи профессиональной деятельности: работа по документационному и организационно-технологическому обеспечению защиты информации в организациях различных структур и отраслевой направленности.

3.Планируемые результаты обучения

Процесс освоения дополнительной профессиональной программы профессиональной переподготовки направлен на совершенствование и (или) формирование у обучающихся профессиональных навыков.

4.Организационно-педагогические условия.

Квалификация поступающего на обучение по программе должна соответствовать требованиям предъявляемым к руководителям подразделений и специалистам по информационной безопасности. Ответственность за выполнение данного условия лежит на заказчике обучения. Данное условие включается в договор об оказании образовательных услуг.

5.Форма аттестации и оценочные материалы.

5.1. Итоговая аттестация обучающихся проводится в виде итогового теста или защиты выпускной аттестационной работы.

План учебного процесса

№ п/п	Наименование учебных модулей	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа	Формы аттестации и контроля знаний
				лекции	семинары	практические занятия	лабораторные работы	промежуточная аттестация		
1	Основы информационной безопасности. Организационное и правовое обеспечение информационной безопасности.	35	29	8	12		8	1	6	зачет
2	Аппаратные средства вычислительной техники. Сети и системы передачи информации. Информационные технологии.	24	18	14	2	1		1	6	зачет
3	Программно-аппаратные средства защиты информации. Техническая защита информации.	27	20	10	6	3		1	7	зачет
4	Криптографические средства и методы защиты информации	18	10	5	4			1	8	зачет
5	Итоговая аттестация	4	4					4		Экзамен и (или) выпускная аттестационная работа
Итого		108	81	37	24	4	8	8	27	

***КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК**
(108 академических часов)

Срок обучения по дополнительной профессиональной программе повышения квалификации, месяцы (недели)				n
Срок обучения по дополнительной профессиональной программе повышения квалификации, недели (дни)	1	….	…	m
Виды занятий, предусмотренные дополнительной профессиональной программой повышения квалификации	А	А	А	И

А – аудиторная и самостоятельная работа
И – итоговая аттестация
n – количество месяцев (недель)
m – количество недель (дней)

*Календарный учебный график составляется для каждой группы обучения при её формировании.

Содержание учебных модулей

1. «Основы информационной безопасности. Организационное и правовое обеспечение информационной безопасности»

Основные понятия, термины и определения в области информационной безопасности; актуальность проблемы защиты информации; защита информации как составная часть общей системы безопасности организации, предприятия; понятие национальной безопасности; виды безопасности; информационная безопасность (ИБ) в системе национальной безопасности Российской Федерации; основные понятия, общеметодологические принципы теории ИБ; анализ угроз ИБ, проблемы информационной войны; государственная информационная политика; проблемы региональной информационной безопасности; виды информации; методы и средства обеспечения ИБ; методы нарушения конфиденциальности, целостности и доступности информации; причины, виды, каналы утечки и искажения информации.

Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; государственная тайна как особый вид защищаемой информации; конфиденциальная информация; система защиты государственной тайны; правовой режим защиты государственной тайны; правовое регулирование взаимоотношений администрации и персонала в области защиты информации; правовые режимы конфиденциальной информации; лицензирование и сертификация в области защиты информации; правовые основы защиты информации с использованием технических средств; защита интеллектуальной собственности; правовая регламентация охранной деятельности; международное законодательство в области защиты информации; преступления в сфере компьютерной информации; экспертиза преступлений в области компьютерной информации; криминалистические аспекты проведения расследований; ответственность за нарушения при обработке конфиденциальной информации.

2 «Аппаратные средства вычислительной техники. Сети и системы передачи информации. Информационные технологии»

Понятие микропроцессора (МП); обобщенная структура МП; поколения МП и их основные характеристики; перспективные МП. Организация и структура памяти, системы прерывания; системы ввода-вывода; периферийные устройства. Архитектура ПЭВМ, рабочих станций и серверов, системная магистраль, буферизация шин, управление системной магистралью, подключение дополнительных и интерфейсных схем. Универсальные и специализированные ЭВМ высокой производительности; архитектура специализированных вычислительных комплексов, ориентированных на программное обеспечение, машины баз данных, объектно-ориентированная архитектура. Оценка качества программного обеспечения. Общие принципы методы и средства проектирования архитектуры и структуры, проектирования логики, тестирования и отладки, документирования и сопровождения программного обеспечения с учетом повышенных требований к надежности программ и их защищенности от несанкционированного доступа. Особенности разработки и сопровождения программного обеспечения для рабочих групп. CASE-технологии, технологии виртуального программирования и объектно-ориентированного программирования

Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основы организации и функционирования сетей. Сетевые операционные системы; основные сетевые стандарты. Средства взаимодействия процессов в сетях. Распределенная обработка информации в системах клиент-сервер; одноранговые сети. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.

Проблематика задач автоматизации. Общие проблемы автоматизации. Классификация программного обеспечения автоматизации задач делопроизводства и документооборота. Автоматизация документооборота и делопроизводства Российский и зарубежный документооборот, основные отличия. Системы электронного документооборота Терминология

3. «Программно-аппаратные средства защиты информации. Техническая защита информации»

Цели и задачи программно-аппаратной защиты информации. Место программно-аппаратной (ПА) защиты информации в системе комплексной защиты информации на объектах информатизации. Предмет, цели, задачи и содержание курса в целом, его роль и место в подготовке специалистов по комплексной защите информации. Классификация методов и средств ПА защиты информации. Основные подходы к ПА защите данных от несанкционированного доступа (НСД). Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлам. Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Разграничение и контроль доступа к информации. Защита сетевого файлового ресурса, фиксация доступа к файлам, доступ к данным со стороны процесса. Способы фиксации факта доступа. Контроль и управление доступом средствами операционной системы. Система SecretNet 6.0. Надежность систем ограничения доступа.

Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защищенные операционные системы. Средства защиты программного обеспечения от

несанкционированной загрузки. ПА защита программ от несанкционированного копирования, пароли и ключи.
Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI.
Компьютерные вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

4.«Криптографические средства и методы защиты информации»

Исторический обзор криптографических методов защиты информации. Основные задачи защиты информации криптографическими методами. Математическая модели открытых текстов. Критерии на открытый текст. Понятие шифра, модель шифра. Классификация шифров. Понятие цифровой подписи. Простейшие шифры замены и их анализ. Простейшие шифры перестановки и их анализ. Шифры гаммирования и их анализ. Дисковые шифраторы многоалфавитной замены. Теоретическая стойкость шифров по Шеннону. Расстояние единственности. Практическая стойкость шифров. Поточные шифрсистемы и принципы их построения. Типовые генераторы псевдослучайных последовательностей и их свойства. Методы усложнения линейных рекуррентных последовательностей. Изучение современных поточных шифрсистем. Блочные шифрсистемы и принципы их построения. Выбор линейных и нелинейных блоков. Режимы использования блочных шифров. Изучение стандартов современных блочных шифрсистем. Определяемые ключом и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций. Использование хеш-функций и блочных шифров в системах аутентификации сообщений. Изучение стандартов современных хеш-функций. Криптосистемы на основе открытого ключа. Вычислительно сложные задачи математики. Криптосистема RSA и ее анализ. Криптосистема Эль-Гамаля, Мак-Эллиса, Меркля-Хеллмана. Схемы цифровой подписи.