МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Факультет повышения квалификации

УТВЕРЖДАЮ
Проректор по учебной работе
_____ С.В. Брованов
(подпись)
«__» февраля 2017 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«Техническая защита конфиденциальной информации. Криптографическое закрытие информации»

Составители программы повышения квалификации
Легкий В.Н., д.т.н., заведующий кафедрой автономных информационных и управляющих систем
Шумейко В.А., старший преподаватель кафедры автономных информационных и управляющих систем

Новосибирск 2017

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы: формирование научного подхода к обеспечению безопасности объектов информатизации, изучение методов обеспечения информационной безопасности; подготовка к участию во всех фазах проектирования и разработки комплексных систем безопасности. Основное внимание уделено методам и средствам обеспечения информационной безопасности и проблемам, возникающим при работе с конфиденциальной информацией.

1.2. Категория слушателей: программа адресована аспирантам и магистрантам, ориентированным на работу в сфере информационных систем и технологий, программа актуальна для научно-педагогических работников в области экономической (коммерческой) безопасности и информационных систем.

1.3. Срок обучения: 72 часа, из которых 48 аудиторных часов, 24 часа самостоятельной работы.

1.4. Форма обучения: очная.

1.5. Режим занятий: 10 дней, из которых 4 дня по 6 учебных часов в день и 6 дней по 4 учебных часа в день, включая итоговую аттестацию.

1.6. Выдаваемый документ: удостоверение о повышении квалификации.

1.7. Планируемые результаты обучения

Программа направлена на освоение (совершенствование) следующих общепрофессиональных компетенций (ОПК).

Виды деятельности	Профессиональные компетенции или трудовые функции	Знания	Умения	Практический опыт
ВД Осуществление организационно-управленческой деятельности	ОПК 1.1. Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З-1. виды защищаемой информации З-2. возможные угрозы безопасности информации организационные З-3. организационные меры поддержания информационной безопасности З-4. способы и методы комплексной защиты информации З-5. обязанности руководства	У-1. оценивать угрозы информационной безопасности У-2. соблюдать основные требования информационной безопасности	поддержание режима информацион-ной безопасности

		объекта и персонала при работе с защищаемой информацией 3-6. методы защиты информации от утечки по техническим каналам		

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план программы повышения квалификации

Наименование модулей	Общая трудо-емкость, ч.	Всего ауд. ч.	Аудиторные занятия, ч.			СРС, ч.
			лекции	лаборатор-ные работы	практические и семинарские занятия	
Введение: Предмет защиты. Информация общедоступная и ограниченного доступа. Категории ценности информации. Информация как объект права собственности. Назначение и задачи в сфере обеспечения информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной и коммерческой тайны. Международный стандарт безопасности информационных систем ISO 17799. Цели и задачи курса	**3**	**2**	**2**	**–**	**–**	**1**
Общие принципы обеспечении Информационной безопасности (ИБ): Основные термины и определения. Угрозы безопасности информационных систем. Классификация угроз безопасности: угрозы преднамеренные и случайные; каналы утечки информации прямые и косвенные; угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами. Модель нарушителя. Классификация методов и средств защиты информации. Службы защиты информации: обеспечение,	**10**	**7**	**7**	**–**	**–**	**3**

аутентичности субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации						
Общие сведения о защите ИС от Несанкционированного доступа (НСД): Принципы защиты информации от НСД Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Схема Kerberos. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Разграничение и контроль доступа к информации. Контроль и управление доступом средствами операционной системы	**30**	**23**	**8**	**–**	**15**	**7**
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. Защита информации на машинных носителях. Защита остатков информации	**6**	**4**	**4**	**–**	**–**	**2**
5. электронные замки и ключи. Средства ПА защиты фирмы «Информзащита» и «Конфидент»	**15**	**10**	**10**	**–**	**–**	**5**
5. Итоговая аттестация	**8**	**2**		**–**	**2**	**6**
Итого	**72**	**48**	**31**	**–**	**17**	**24**

2.2. Учебно-тематический план программы повышения квалификации

Наименование модулей и тем	Общая трудо-емкость, ч.	Всего ауд. ч.	Аудиторные занятия, ч.			СРС, ч.
			лекции	лабораторные работы	практические и семинарские занятия	
Модуль 1. Введение	**3**	**2**	**2**	**–**	**–**	**1**
Тема 1.1. Основные понятия и определения	3	2	2	–	–	1
Модуль 2. Информация общедоступная и ограниченного доступа. Категории ценности информации	**10**	**7**	**7**	**–**	**–**	**3**
Тема 2.1. Информация как объект права собственности. Назначение и задачи в сфере обеспечения информационной безопасности	3	2	2	–	–	1
Тема 2.2. Основные нормативные руководящие документы, касающиеся государственной и коммерческой тайны. Международный стандарт безопасности информационных систем ISO 17799. Цели и задачи курса	7	5	5	–	–	1
Модуль 3.	**30**	**23**	**8**	**–**	**15**	**7**
Тема 3.1. *Общие принципы обеспечении Информационной безопасности (ИБ):* Основные термины и определения. Угрозы безопасности информационных систем	6	4	4	–	–	2
Тема 3.2. Классификация угроз безопасности: угрозы преднамеренные и случайные	6	4	4	–	–	2
Тема 3.3. каналы утечки информации прямые и косвенные; угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами	6	5	–	–	5	1
Тема 3.4. Модель нарушителя. Классификация методов и средств защиты информации	6	5	–	–	5	1
Тема 3.5. Службы защиты информации: обеспечение, аутентичности субъектов информационного взаимодействия, управление	6	5	–	–	5	1

доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации						
Модуль 4. *Общие сведения о защите ИС от Несанкционированного доступа* (НСД)	**15**	**10**	**10**	**–**	**–**	**5**
Тема 4.1. Принципы защиты информации от НСД Идентификация, аутентификация и авторизация	6	4	4	–	–	2
Тема 4.2. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Схема Kerberos. Несимметричные методы аутентификации субъекта	3	2	2	–	–	1
Тема 4.3. Аутентификация объекта. Разграничение и контроль доступа к информации. Контроль и управление доступом средствами операционной системы	6	4	4	–	–	2
Модуль 5. 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. Защита информации на машинных носителях. Защита остатков информации	**6**	**4**	**4**	**–**	**–**	**2**
Тема 5.1. электронные замки и ключи. Средства ПА защиты фирмы «Информзащита» и «Конфидент»	6	4	4	–	–	2
Итоговая аттестация	**8**	**2**		**–**	**2**	**6**
Подготовка итоговой аттестационной работы	6	–	–	–	–	6
Процедура защиты итоговой аттестационной работы	2	2	–	–	2	–
Итого	**72**	**48**	**31**	**–**	**17**	**24**