МИНИСТЕРСТВО ОБРАЗОВАНИЯ КИРОВСКОЙ ОБЛАСТИ

Кировское областное государственное образовательное автономное учреждение дополнительного профессионального образования
Институт развития образования Кировской области
(ИРО Кировской области)

«УТВЕРЖДАЮ»
ректор ИРО Кировской области
Н.В. Соколова
«27» января 2022 г. №1

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
(повышения квалификации)

«Информационная безопасность»

для государственных и гражданских служащих, муниципальных служащих, сотрудников организаций, подведомственных органам государственной власти и ОМСУ, сотрудников негосударственных организаций

(в количестве 40 часов)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D71BF3C772EE800000000D29530002
Владелец: Соколова Наталья Вячеславовна
Действителен: с 18.03.2021 до 18.03.2022

Киров,
2022

РАЗДЕЛ 1. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность» разработана в соответствии с нормативными актами:

– Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», гл. 2, ст. 11, гл. 9, ст. 73, гл. 10, ст. 76;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

– Приказ Министерства образования и науки Российской Федерации от 01.07.2013 № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Приказ Минобрнауки России от 23.08.2017 № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

– Методические рекомендации по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утверждены Федеральной службой по техническому и экспортному контролю Российской Федерации 16.04.2018.

Программа сформирована с учётом квалификационных требований (видов профессиональной деятельности, трудовых функций и уровней квалификации), установленных в профессиональных стандартах «Специалист по защите информации в автоматизированных системах» (утв. приказом Минтруда России № 522н от 15 сентября 2016 г.) и «Специалист по безопасности компьютерных систем и сетей» (утв. приказом Минтруда России № 598н от 01 ноября 2016 г.).

При разработке содержания Программы учтены требования обеспечения преемственности по отношению к федеральным государственным образовательным стандартам высшего профессионального образования (ФГОС ВПО) по направлению подготовки «Информационная безопасность», а именно ФГОС ВПО «10.00.00 Информационная

безопасность», 10.05.01 «Компьютерная безопасность», (квалификация/степень «бакалавриат»).

Роль информации в современном обществе неуклонно растет. Информация становится одной из главных общественных ценностей. Информационная сфера сегодня – это совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также систему регулирования возникающих при этом отношений. Развитие информационной сферы, обеспечение ее безопасности становится одним из приоритетов национальной политики нашего государства. В «Доктрине информационной безопасности Российской Федерации» в качестве одной из основных задач указывается необходимость защиты интересов личности, общества, государства в информационной сфере.

Особую актуальность этой проблеме придает реализация национального проекта «Цифровая экономика», а также требований федеральных законов от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» существенно повышающим требования к организациям, которые хранят, собирают, передают или обрабатывают персональные данные с применением информационных технологий.

Прогноз научно-технологического развития Российской Федерации на период до 2030 г. (утвержден Правительством Российской Федерации 3 января 2014 г.) определяет угрозы для России в сфере информационно-коммуникационных технологий:

- ускоренное формирование единого глобального информационного пространства;
- обострение «цифрового неравенства»;
- неготовность к широкомасштабному предоставлению гражданам медицинских и иных социальных услуг с использованием ИКТ;
- возможность использования потенциала ИКТ в целях подрыва национальной безопасности, нарушения государственного и общественного порядка;
- необходимость обеспечения эффективного (защищенного) документооборота;
- неготовность к массовому применению технологий виртуальной реальности;
- растущая незащищенность личной жизни и личного жизненного пространства.

Решение указанных выше проблем делает актуальным повышение квалификации должностных лиц, сотрудников организаций, работающих с информацией и данными разных типов, в области информационной безопасности.

1.1. Цель реализации программы.

Цель программы – повышение профессионального уровня обучающихся в рамках имеющейся квалификации путём совершенствования имеющихся и/или формирования у них новых компетенций (знаний и умений), необходимых им для выполнения трудовых функций в рамках профессиональной деятельности (исполнения должностных обязанностей в области профессиональной деятельности) в сфере информационной безопасности, защиты информации.

Задачи программы:

- ознакомление слушателей с основными понятиями информационной безопасности, основными принципами построения систем защиты информации, нормативными правовыми и организационными основами обеспечения безопасности персональных данных в информационных системах персональных данных;

- формирование умений выбора решений из различных категорий методов и средств защиты информаций, соответствующих требованиям защиты информации в конкретных информационных системах;

- изучение методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценка степени их опасности;

- развитие умений оценки соответствия существующих решений требованиям защиты информации,

- формирование готовности к разработке предложений по совершенствованию системы обеспечения информационной безопасности организации,

- оказание помощи организациям и учреждениям в повышении квалификации сотрудников, в чьи должностные обязанности входит обеспечение защиты информации, по вопросам построения и эффективного применения комплексных систем и средств защиты информации;

1.2. Планируемые результаты обучения

Знания, умения, навыки и компетенции обучающегося, формируемые в результате освоения программы повышения квалификации.

В результате освоения дополнительной профессиональной программы слушатель должен **знать**:

–нормативно-правовые и организационные основы защиты информации и обеспечения безопасности персональных данных в Российской Федерации;

–базовый понятийный аппарат в области информационной безопасности и персональных данных;

–виды и состав угроз информационной безопасности;

–принципы и общие методы обеспечения информационной безопасности;

–меры обеспечения безопасности информации;

–основные положения обеспечения государственной политики обеспечения информационной безопасности;

–требования по обеспечению защиты информации;

–каналы и методы несанкционированного доступа к конфиденциальной информации;

–процедуры задания и реализации требований по защите информации в информационных системах персональных данных;

–классификацию видов, методов и средств защиты информации.

В результате освоения дополнительной профессиональной программы слушатель должен **уметь:**

–выявлять угрозы информационной безопасности применительно к объектам защиты;

–определять состав конфиденциальной информации применительно к видам тайн;

–выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия;

–выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации;

–определять направления и виды защиты информации с учетом характера информации и задач по её защите.

В результате освоения дополнительной профессиональной программы слушатель должен **владеть:**

–основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации.

В результате освоения дополнительной профессиональной программы слушатель должен **освоить компетенции:**

–готовность осуществлять собственную профессиональную деятельность в полном соответствии с требованиями информационной безопасности;

–готовность разрабатывать необходимые документы в интересах организации по обеспечению безопасности персональных данных;

–готовность к выбору решений из различных категорий методов и средств защиты информаций, соответствующих требованиям защиты информации в конкретных информационных системах;

–способность осуществлять оценку соответствия существующих решений требованиям защиты информации;

–готовность к разработке предложений по совершенствованию системы обеспечения информационной безопасности организации.

Имеющаяся квалификация (требования к слушателям): государственные и гражданские служащие, муниципальные служащие, сотрудники организаций, подведомственных органам государственной власти и органам местного самоуправления, сотрудники негосударственных организаций. Программа повышения квалификации рассчитана на сотрудников органов государственной власти организаций и учреждений, деятельность которых связана с процессами обработки персональных данных и защитой информации конфиденциального характера.

1.3. Форма обучения: очная, заочная, очная с применением ДОТ

РАЗДЕЛ 2. СОДЕРЖАНИЕ ПРОГРАММЫ
2.1 Учебно-тематический план
(объем программы 40 ч.)

№ п/п	Наименование разделов (модулей) и тем	Всего час.	Виды учебных занятий, учебных работ		Формы контроля
			Лекции	Интерактивные занятия	
1	**Раздел 1. Введение в информационную безопасность**	**5**	**5**	**0**	тестирование по темам раздела
1.1	Понятие, сущность и цели защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности РФ	2	2	0	
1.2	Определение объектов защиты (ИТ-активов организации) и их значимости. Классификация информации	1	1	0	
1.3	Система регулирования защиты информации. Нормативно-правовая база в области информационной безопасности в Российской Федерации	2	2	0	
2	**Раздел 2. Защита прав субъектов персональных данных в организации**	**8**	**4**	**4**	решение задач по темам раздела
2.1	Введение в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Правовые вопросы обработки персональных данных в организациях.	4	2	2	
2.2	Организация обработки персональных данных в организации. Основные организационные процессы и документы	4	2	2	
3	**Раздел 3. Комплексная система защиты информации в организации**	**5**	**5**	**0**	тестирование по темам раздела
3.1	Организация и внедрение системы управления информационной безопасностью в организации	2	2	0	
3.2	Документация системы обеспечения информационной безопасности	1	1	0	
3.3	Оценка защищенности информации. Оценка эффективности мер защиты информации. Аттестация объектов	2	2	0	

№ п/п	Наименование разделов (модулей) и тем	Всего час.	Виды учебных занятий, учебных работ		Формы контроля
			Лекции	Интерактивные занятия	
	информатизации				
4	**Раздел 4. Угрозы безопасности информации**	**6**	**4**	**2**	Практическая работа
4.1	Определение угроз безопасности информации. Риски информационной безопасности. Классификация уязвимостей	2	2	0	
4.2	Моделирование угроз безопасности информации.	4	2	2	
5	**Раздел 5. Защита информации в информационных системах**	**10**	**10**	**0**	Тестирование по темам раздела
5.1	Аутентификация и идентификация. Управление доступом. Меры аудита и учета событий безопасности.	2	2	0	
5.2	Основы обеспечения безопасности в ИТ-инфраструктурах организаций	2	2	0	
5.3	Обеспечение безопасности в корпоративных сетях	2	2	0	
5.4	Архитектуры информационных систем, технологические процессы обработки информации и связанные с ними угрозы информационной безопасности	2	2	0	
5.5	Обеспечение безопасности на уровне автоматизированного рабочего места	2	2	0	
6	**Раздел 6. Криптографическая защита информации**	**4**	**4**	**0**	Тестирование по темам раздела
6.1	Общие положения о криптографических методах защиты информации. Симметричное и ассиметричное шифрование. Электронная подпись	2	2	0	
6.2	Общие требования к организации криптографической защиты информации. Криптографическая защита информации в информационных системах	2	2	0	
7.	**Итоговая аттестация**	**2**			**Итоговый тест**
	ИТОГО:	**40**			

2.2. Рабочая программа

РАЗДЕЛ 1. Введение в информационную безопасность

Тема 1.1 Понятие, сущность и цели защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности Российской Федерации.

Введение в информационную безопасность. Современное состояние развития ИТ и основные угрозы информационной безопасности. Определение понятия «информационная безопасность». Основные принципы и содержание деятельности по обеспечению информационной безопасности. Цели государства, организаций и физических лиц в сфере информационной безопасности и основные задачи по ее обеспечению. Сущность информационной безопасности и кибербезопасности.

Тема 1.2. Определение объектов защиты (ИТ-активов организации) и их значимости. Классификация информации

Определение и классификация объектов защиты: информации, процессов, информационных систем, автоматизированных систем управления, персонала, организационной среды и других. Определение информации и основные свойства безопасности информации. Классификация информации. Определение информации ограниченного доступа, информации ограниченного распространения. Коммерческая тайна. Служебная тайна. Персональные данные. Основные правовые режимы информации.

Тема 1.3. Система регулирования защиты информации. Нормативно-правовая база в области информационной безопасности в Российской Федерации

Введение в информационное право. Обзор законодательства Российской Федерации в области информационной безопасности. Стандарты и руководящие документы в области информационной безопасности.

Доктрина информационной безопасности Российской Федерации. Место информационной безопасности в обеспечении национальной безопасности. Государственные органы в области защиты информации. Характеристика деятельности органов государственной власти, выступающих регуляторами в области информационной безопасности.

Лицензирование деятельности в области защиты информации. Лицензирование деятельности по технической защите конфиденциальной информации и разработке и производству средств защиты конфиденциальной информации.

Ответственность за нарушение законодательства в информационной сфере.

РАЗДЕЛ 2. Защита прав субъектов персональных данных в организации.

Тема 2.1. Введение в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Правовые вопросы обработки персональных данных в организациях.

Характеристика Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Основные понятия, связанные с обработкой персональных данных. Принципы и условия обработки персональных данных. Цели обработки персональных данных. Обязанности оператора персональных данных. Права субъекта персональных данных. Категории персональных данных. Способы обработки персональных данных. Особенности обработки персональных данных в информационных системах персональных данных. Государственный контроль и надзор за обработкой персональных данных. Правовые меры обеспечения безопасности персональных данных при их обработке. Процессы обработки персональных в рамках трудовой деятельности. Согласие на обработку персональных данных. Биометрические персональные данные. Договоры с субъектами персональных данных. Договоры поручения обработки персональных данных. Разъяснение субъекту условий обработки персональных данных. Обработка персональных данных, разрешенных субъектом для распространения. Политика в отношении обработки персональных данных.

Тема 2.2. Организация обработки персональных данных в организации. Основные организационные процессы и документы

Структура локальных актов оператора, определяющих политику оператора в отношении обработки персональных данных. Лица, ответственные за организацию обработки персональных данных в организациях. Обработка персональных данных, осуществляемая без использования средств автоматизации. Автоматизированная обработка персональных данных. Места хранения персональных данных. Сроки обработки персональных данных. Формы, предназначенные для сбора персональных данных. Типовые формы и формы, утверждаемые оператором персональных данных. Обязательства о конфиденциальности персональных данных. Меры обеспечения физической защиты персональных данных. Внутренний контроль и (или) аудит соответствия обработки персональных данных действующему законодательству и локальным актам оператора.

РАЗДЕЛ 3. Комплексная система защиты информации в организации

Тема 3.1. Организация и внедрение системы управления информационной безопасностью в организации

Менеджмент информационной безопасности. Основные процессы информационной безопасности. Понятие и организация жизненного цикла защищаемых объектов.

Меры защиты конфиденциальной информации: правовые, организационные, технические.

Тема 3.2. Документация системы обеспечения информационной безопасности

Особенности документационного обеспечения информационной безопасности. Перечень локальных актов оператора при обработке персональных данных в информационных системах. Характеристика принимаемых мер безопасности персональных данных в информационных системах. Политики информационной безопасности. Инструкции, положения, учетная документация. Управление конфигурацией ИС.

Тема 3.3. Оценка защищенности информации. Оценка эффективности мер защиты информации. Аттестация объектов информатизации.

Оценка эффективности защиты информации. Аттестация объектов информатизации. Порядок аттестации объектов информатизации. Аттестационные испытания. Прохождение контроля защищенности объектов информатизации. Мониторинг информационной безопасности.

РАЗДЕЛ 4. Угрозы безопасности информации

Тема 4.1. Определение угроз безопасности информации. Риски информационной безопасности. Классификация уязвимостей

Определение, анализ и классификация возможных угроз безопасности информации. Источники угроз информационной безопасности и модели нарушителей. Иные угрозы и факторы, воздействующие на информацию и активы организации. Уязвимости и их классификация. Риски информационной безопасности. Методы оценки рисков информационной безопасности.

Тема 4.2. Моделирование угроз безопасности информации

Модель угроз безопасности информации: понятие, назначение. Методика оценки угроз безопасности информации ФСТЭК России от 05.02.2021. Порядок оценки угроз безопасности информации. Определение негативных последствий от реализации (возникновения) угроз безопасности информации. Определение возможных объектов воздействия угроз безопасности информации. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности (определение источников угроз безопасности информации, оценка способов реализации (возникновения) угроз безопасности информации, оценка

актуальности угроз безопасности информации). Практика написания модели угроз безопасности информации.

РАЗДЕЛ 5. Мероприятия по защите информации в информационных системах

Тема 5.1. Аутентификация и идентификация. Управление доступом. Меры аудита и учета событий безопасности.

Определение и назначение идентификации и аутентификации субъектов и объектов доступа. Однофакторная и многофакторная аутентификация, свойства, сравнение, примеры. Локальная и удаленная аутентификация, основные особенности и свойства. Понятие протокола аутентификации. Протоколы аутентификации без разглашения, с защитой обратной связи. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Понятие контроля доступа. Модели управления доступом: мандатная, дискреционная, ролевая, динамическая и другие. Меры по управлению доступом субъектов доступа к объектам доступа. Аудит и учет событий безопасности: понятие, цели, меры.

Тема 5.2. Основы обеспечения безопасности в ИТ-инфраструктурах организаций

Понятие ИТ-инфраструктуры. Распределенные инфраструктуры и проблемы управления ими. Центры обработки данных и сети хранения данных. Технологии виртуализации. Базовые сервисы сети и системная инфраструктура. Информационная безопасность в ИТ-инфраструктуре. Меры защиты в рамках ИТ-инфраструктуры в образовательных организациях. Системы управления ИТ-инфраструктурой. Системы управления конфигурацией.

Тема 5.3. Обеспечение безопасности в корпоративных сетях.

Структуры вычислительных сетей и основные компоненты. Корпоративные вычислительные сети. Протоколы взаимодействия в вычислительных сетях. Уязвимости в сетевых технологиях и связанные с этим угрозы. Средства защиты информации в сетях. Разделение трафика на канальном уровне. Межсетевые экраны и их назначение. Меры безопасности, выполняемые на уровне коммутаторов. Угрозы перехвата передаваемых по сети сообщений. Технологии виртуальных частных сетей (VPN). Средства мониторинга вычислительных сетей.

Тема 5.4. Архитектуры информационных систем, технологические процессы обработки информации и связанные с ними угрозы информационной безопасности

Информационные системы. Структура информационной системы и основные элементы технологического процесса обработки информации. Архитектура информационных систем. Типы архитектур информационных систем: автономные, файл-серверные, клиент-серверные, трехзвенные, терминальные, сервисные и другие. Облачные сервисы, микросервисы. Интеграция различных информационных систем, параллельные архитектуры. Архитектуры высокодоступных и высоконадежных систем. Современные Жизненный цикл информационных систем. Подходы к классификации информационных систем персональных данных исходя из их архитектуры. Влияние архитектуры информационных систем персональных данных на безопасность.

Тема 5.5. Обеспечение безопасности на уровне автоматизированного рабочего места.

Организация защиты информации на уровне персонального компьютера (хранение и обработка информации). Общие принципы построения защиты информации от несанкционированного доступа. Требования к защите от несанкционированного доступа к информации в автоматизированных системах. Базовые механизмы обеспечения безопасности в операционных системах. Оптимизация настроек параметров безопасности операционной системы. Настройка политик безопасности учетных записей. Настройка политики паролей. Политика блокировки учетных записей. Механизмы разграничения доступа. Авторизация в операционной системе. Аудит (журналирование) в операционной системе. Политика ограниченного использования программ. Аппаратно-программные и программные модули доверенной загрузки.

РАЗДЕЛ 6. Криптографическая защита информации

Тема 6.1. Общие положения о криптографических методах защиты информации. Симметричное и ассиметричное шифрование. Электронная подпись

Предмет и задачи криптографии. Методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Использование асимметричных алгоритмов для шифрования. Криптографические алгоритмы с открытым ключом. Защита каналов связи. Электронная подпись. Виды электронных подписей в Российской Федерации. Инфраструктура электронной подписи.

Тема 6.2. Общие требования к организации криптографической защиты информации. Криптографическая защита информации в информационных системах

Организация защиты информации с использованием средств криптографии в организации. Нормативно-правовые требования. Методы криптографической защиты носителей информации. Состав и содержание организационных и технических мер по обеспечению безопасности информации с использованием средств криптографии в информационных системах. Ведение журналов по эксплуатации средств криптографической защиты информации. Журнал учета ключевых носителей. Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. Журнал учёта ключей, печатей, пломбиров от помещений и сейфов. Журнал контроля соблюдения условий эксплуатации и работоспособности средств криптографической защиты информации.

РАЗДЕЛ 3. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Вид аттестации	Формы контроля	Виды оценочных материалов
Промежуточная	Тестирование, практическая работа, решение кейсовых задач	Тест
Итоговая	Итоговое тестирование	Тест

Оценочные материалы по дисциплине (модулю, курсу) включают основные вопросы, выносимые на аттестацию (тестирование).

Раздел №1 Введение в информационную безопасность.

Вопрос 1: Федеральным законом, регулирующим отношения, возникающие при применении информационных технологий и обеспечения защиты информации является:

Варианты ответа:

a) закон РФ «О безопасности»

b) закон «О техническом регулировании»

c) ФЗ «Об участии в международном информационном обмене»

d) ФЗ «Об информации, информационных технологиях и о защите информации»

e) ФЗ «Об информации, информатизации и защите информации»

Вопрос 2: Маркер «Для служебного пользования» является…

Варианты ответа:

a) Ограничительной пометкой

b) Грифом секретности

c) Степенью конфиденциальности

Вопрос 3: Информация по категории доступа классифицируется как: (выберите все варианты ответов)

Варианты ответа:

a) Особо конфиденциальная

b) Конфиденциальная

c) Широкого доступа

d) Общедоступная

e) Ограничительного доступа

Вопрос 4: К информации, составляющей коммерческую тайну относятся сведения о…

Варианты ответа:

a) Размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества

b) Результатах интеллектуальной деятельности в научно-технической сфере

Раздел 2. Защита прав субъектов персональных данных в организации (примеры задач)

Задача 1. Арутюнов обратился в ООО «Звезда» с просьбой принять его на работу в качестве ведущего специалиста отдела продаж. Начальник кадровой службы направил запрос в психоневрологический диспансер по месту жительства Арутюнова, в котором просил сообщить сведения о состоянии психологического здоровья и о фактах обращения Арутюнова за психиатрической помощью, поскольку организации необходимо решить вопрос о пригодности Арутюнова для выполнения работы.

Законны ли действия начальника кадровой службы?

Задача 2. Задача 6. Менеджер проектов ООО «Перспектива» Савельева сделала запрос о предоставлении персональных данных юриста ООО «Новые возможности» Илютиной, в связи с осуществлением совместного проекта. Директор ООО «Новые возможности» без согласования с Илютиной предоставил запрашиваемые данные.

Правомерны ли действия директора ООО? Какие требования установлены для передачи персональных данных работника?

Задача 8. Директор ООО «Альянс» обратился в УМВД России с просьбой предоставить сведения о фактическом месте жительства на работника ООО Григорьева.

Законно ли обращение директора? Какой порядок получения персональных данных работника установлен Трудовым Кодексом Российской Федерации? Изменится ли решение задачи, если с запросом о предоставлении персональных данных о фактическом месте жительства Григорьева обратится Прокуратура?

Раздел №3 Комплексная система защиты информации в организации.

Вопрос 1: Для чего разрабатывается модель угроз?

Варианты ответа:

a) Чтобы определить объекты защиты

b) Чтобы определить состав защищаемой информации

c) Чтобы разработать план защиты информации

d) Чтобы определить актуальные угрозы безопасности информации

Вопрос 2: Создание контролируемой зоны относится к:

Варианты ответа:
a) Правовым мерам защиты информации
b) Контрольным мероприятиям защиты информации
c) Техническим мерам защиты информации
d) Организационным мерам защиты информации

Вопрос 3: Регистрация действий пользователей (событий) является:
Варианты ответа:
a) Функцией СЗИ от утечки информации по техническим каналам
b) Функцией СЗИ от специальных воздействий
c) Функцией СЗИ от несанкционированного доступа к информации
d) Функцией средств криптографической защиты информации

Вопрос 4: Шифрование информации осуществляется:
Варианты ответа:
a) Программными средствами защиты информации
b) Специальными средствами защиты информации
c) Программно-техническими средствами информации
d) Средствами криптографической защиты информации

Раздел №5 Защита информации в информационных системах.

Вопрос 1: К основным возможностям программно-аппаратного комплекса «Соболь» относятся…
Варианты ответа:
a) Реализация механизмов мандатного и дискреционного разграничения доступа
b) Идентификация пользователей по электронным идентификатора, разграничение доступа пользователей к защищаемым ресурсам, контроль целостности программной среды до загрузки операционной системы
c) Идентификация пользователей по электронным идентификаторам, запрет загрузки операционной системы с внешних носителей, контроль целостности программной среды до загрузки операционной системы

Вопрос 2: Является ли средство «Secret Net» средствами анализа защищённости?
Варианты ответа:
a) Нет, не является
b) Да, является

Вопрос 3: Назовите основные требования к паролям пользователей
Варианты ответа:
a) Минимальная длинна, сложность, неповторимость
b) Соответствие криптографическому ключу
c) Инерционность, минимальная длинна, сложность

Вопрос 4: Дайте определение «Субъект доступа»

Варианты ответа:

a) Пользователь автоматизированной системы обработки информации (в том числе Администратор безопасности), действия которого регламентируются правилами разграничения доступа

b) Лицо, или процесс, действие которого регламентируются правилами разграничения доступа

c) Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Раздел №6 Криптографическая защита информации.

Вопрос 1: В чём суть атаки «Человек по середине»?

Варианты ответа:

a) Уязвимость, обусловленная необходимостью использования неавтоматизированных операций по шифрованию, выполняемых шифровальщиком вручную и приводящая к возможности искажения сообщений

b) Потенциальный нарушитель может перехватывать и изменять сообщения, передаваемые в канале связи от отправителя к получателю

Вопрос 2: Какие системы шифрования называются ассиметричными

Варианты ответа:

a) Используются различные ключи для расшифровывания и зашифровывания

b) В которых длинна зашифрованного текста отличается от длинны ключа открытого текста

Вопрос 3: Какой ключ шифрования делают открытым?

Варианты ответа:

a) Ключ зашифровывания

b) Ключ расшифровывания

Вопрос 4: Что такое криптография?

Варианты ответов:

a) Наука о шифровании информации

b) Наука о разработке криптографических алгоритмов

Вопрос 5: Что такое шифрование?

Варианты ответа:

a) Преобразование текста к нечитаемому виду

b) Процесс зашифровывания и расшифровывания

РАЗДЕЛ 4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1. Учебно-методическое обеспечение и информационное обеспечение программы

Нормативно-правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года).
2. Федеральный закон «О безопасности» от 28.12.2010 г. № 390-ФЗ.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ (в ред. от 21.07.2011 г. № 252-ФЗ).
4. Федеральный закон «О государственной тайне» от 21.07.1993 г. №5485-I (в ред. от 08.11.2011 г. № 309-ФЗ).
5. Федеральный закон «О коммерческой тайне» от 18.12.2006 г. № 231-ФЗ.
6. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 г. № 99-ФЗ (в ред. от 28.07.2012 г. № 133-ФЗ).
7. Федеральный закон «О персональных данных» от 27.07.2006 г. № 149-ФЗ.
8. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.
8. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации № 646 от 05.12.2016 г.).
9. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
10. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
11. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
12. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
13. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения

установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Основная литература

1. Глинская Е.В. Информационная безопасность конструкций ЭВМ и систем: учеб. пособие / Е.В. Глинская, Н.В. Чичварин. М.: ИНФРА-М, 2018. 118с. URL: http://znanium.com/catalog.php?bookinfo=925825 (дата обращения: 05.01.2021).

2. Баранова Е.К. Информационная безопасность и защита информации: учеб. пособие / Е.К. Баранова, А.В. Бабаш. 3-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2017. 322 с. URL: http://znanium.com/catalog.php?bookinfo=763644 (дата обращения: 05.01.2021).

3. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учеб. пособие. М.; Берлин: Директ-Медиа, 2015. 253 с.URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 05.01.2021).

4. Нестеров С.А. Основы информационной безопасности: учеб. пособие. СПб.: Издательство Политехнического университета, 2014. 322 с. URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 05.01.2021).

5. Информационная безопасность и защита информации: учеб. Пособие для вузов / Ю.Ю. Громов и др. Старый Оскол: ТНТ, 2010. 384 с. 6. Бабаш А.В. Информационная безопасность: лабораторный практикум: учеб. пособие. 2-изд., стер. М.: КноРус, 2013. 136 с.

Дополнительная литература

1. Гришина Н.В. Информационная безопасность предприятия: учеб.пособие. 2-е изд., доп. М.: ФОРУМ: ИНФРА-М, 2017. 239 с. URL: http://znanium.com/catalog.php?bookinfo=612572 (дата обращения 05.01.2021).

2. Вдовенко Л.А. Информационная система предприятия: учеб. пособие. 2-е изд., пераб. и доп. М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. 304 с. URL: http://znanium.com/catalog.php?bookinfo=501089 (дата обращения 05.01.2021).

3. Артемов А.В. Информационная безопасность: курс лекций. Орел: МАБИВ, 2014. 257 с. URL: http://biblioclub.ru/index.php?page=book&id=428605 (дата обращения 05.01.2021).

4. Золотарев В.В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков: учеб. пособие / В.В. Золотарев, Е.А. Данилова. Красноярск: Сиб. гос. аэрокосмич. ун-т, 2010. 144 с. URL: http://znanium.com/catalog.php?bookinfo=463037 (дата обращения 05.01.2021).

5. Жукова М.Н. Управление информационной безопасностью. Ч. 2.Управление инцидентами информационной безопасности: учеб. пособие / М.Н.Жукова, В.Г. Жуков, В.В. Золотарев. Красноярск: Сиб. гос. аэрокосмич.

ун-т, 2012. 100 с. URL: http://znanium.com/catalog.php?bookinfo=463061 (дата обращения 05.01.2021).

6. Бабаш А.В. Информационная безопасность: лабораторный практикум: учеб. пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. М.: КНОРУС, 2012. 131 с.

7. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. 3-е изд., стер. М.: Академия, 2008. 336 с.

8. Партыка Т.Л. Информационная безопасность: учеб. пособие для сред. проф. образования / Т.Л. Партыка, И.И. Попов. 2-е изд., испр. и доп. М.: ФОРУМ: ИНФРА-М, 2007. 368 с.

9. Филин С.А. Информационная безопасность: учеб. пособие. М.: АльфаПресс, 2006. 412 с.

10. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для студ. высш. учеб. заведений. М.: Горячая линия-Телеком, 2004. 280 с.

Программное обеспечение и интернет-ресурсы

1. Дистрибутивы антивирусных программ с официальных сайтов разработчиков.
2. Справочно-информационная система (СИС) «Гарант».
3. Справочно-информационная система «Консультант».

4.2. Материально – технические условия реализации программы

Для реализации программы необходимо следующее материально-техническое обеспечение для слушателей:

- доступ к платформе дистанционного обучения Moodle;
- компьютер, колонки, наушники, камера;
- доступ в Интернет;

Необходимое программное обеспечение:

– современный браузер (Yandex, Opera, Firefox или аналоги);

– текстовый редактор.