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

«УТВЕРЖДАЮ»
Ректор КОГОАУ ДПО «ИРО Кировской области»
_____
Н.В. Соколова
«24» 06 2021 г.

КОГОАУ ДПО "ИРО Кировской области"

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

(повышения квалификации)

«Основы обеспечения информационной безопасности в образовательной организации»

(в количестве 40 часов)

ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ КИРОВСКОЙ ОБЛАСТИ

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

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

Киров 2021

РАЗДЕЛ 1. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дополнительная профессиональная программа повышения квалификации «Основы обеспечения информационной безопасности в образовательной организации» разработана в соответствии с нормативными актами:

– Федеральный закон от 29 декабря 2012 г. № 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 N 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 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Приказ Министерства образования и науки Российской Федерации от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»;

– Приказ Министерства образования и науки Российской Федерации от 09 января 2014 г. № 2 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

Роль информации в современном обществе неуклонно растет. Она 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 федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», 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 – формирование у слушателей готовности к реализации собственной профессиональной деятельности в полном соответствии с требованиями информационной безопасности, развитие практических навыков по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах.

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.

1.2. Планируемые результаты обучения.

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

В результате освоения ДПП 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 персональных данных;

–основные положения обеспечения государственной политики обеспечения информационной безопасности;

–требования по обеспечению безопасности персональных данных;

–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 ДПП 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;

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

В результате освоения ДПП 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): работники образовательных организаций. Программа повышения квалификации рассчитана на сотрудников предприятий и организаций, деятельность которых связана с процессами обработки персональных данных и 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**	**6**	**6**	**0**	тестирование по темам раздела
1.1	Понятие, сущность и цели защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности РФ. Система обеспечения информационной безопасности в РФ. Нормативно-правовая база информационной безопасности и направления обеспечения информационной безопасности	2	2	0	
1.2	Определение объектов защиты (ИТ-активов организации) и их значимости. Классификация информации	2	2	0	
1.3	Понятие и сущность правовых мер защиты информации. Ответственность за нарушение законодательства в сфере защиты информации	2	2	0	
2	**Раздел 2. Защита прав субъектов персональных данных в образовательных организациях**	**12**	**6**	**6**	тестирование по темам раздела
2.1	Введение в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	2	2	0	
2.2	Правовые вопросы обработки персональных данных в образовательных организациях. Оценка возможного вреда субъектам персональных данных	6	2	4	
2.3	Организация обработки персональных данных в образовательных организациях. Основные организационные процессы и документы	4	2	2	
3	**Раздел 3. Мероприятия по защите информации в информационных системах**	**20**	**18**	**4**	тестирование по темам раздела
3.1	Архитектуры информационных	2	2	0	

	систем, технологические процессы обработки информации и связанные с ними угрозы информационной безопасности				
3.3	Меры по идентификации и аутентификация субъектов доступа и объектов доступа. Меры и модели контроля доступа. Меры аудита и учета событий безопасности	2	2	0	
3.4	Основы информационной безопасности вычислительных сетей	2	2	0	
3.5	Основы обеспечения безопасности в IT-инфраструктурах организаций	2	2		
3.6	Подходы и меры защиты информации ограниченного доступа от утечки	2	2	0	
3.7	Криптографическая защита информации. Защита каналов связи, носителей информации, электронная подпись	2	2	0	
3.8	Угрозы и риски информационной безопасности в образовательных организациях. Классификация уязвимостей. Модель угроз безопасности информации и ИТ-активов	4	2	2	
3.9	Обеспечение кибербезопасности. Характеристика видов и этапов осуществления кибератак. Меры защиты от атак. Мониторинг информационной безопасности	2	2	0	
3.10	Документация системы обеспечения информационной безопасности персональных данных в информационных системах	2	2	0	
5.	**Итоговая аттестация**	**2**			**Итоговый тест**
	ИТОГО:	**40**			

2.2. Рабочая программа

РАЗДЕЛ 1. Введение в информационную безопасность

Тема 1. Понятие, сущность и цели обеспечения безопасности информации. Значение информационной безопасности и ее место в системе национальной безопасности РФ. Система обеспечения информационной безопасности в РФ. Нормативно-правовая база информационной безопасности и направления обеспечения информационной безопасности

История и развитие понятия «информационная безопасность». Современные подходы к определению понятия. Сущность информационной безопасности и кибербезопасности. Определение безопасности информации. Цели обеспечения безопасности информации. Состав и основные свойства безопасности информации. Основные принципы и содержание деятельности по обеспечению информационной безопасности. Доктрина информационной безопасности Российской Федерации. Место информационной безопасности в обеспечении национальной безопасности. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Общие методы обеспечения информационной безопасности. Основные направления государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Государственные органы в области защиты информации. Характеристика деятельности органов государственной власти, выступающих регуляторами в области информационной безопасности.

Тема 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. Средства и системы информатизации. Защищаемые помещения. Классификация информации. Определение информации ограниченного доступа. Классификация информации ограниченного доступа по видам тайн. Коммерческая тайна. Служебная тайна. Персональные данные.

Тема 3. Понятие и сущность правовых мер информационной безопасности. Ответственность за нарушение законодательства в сфере защиты информации

Обзор законодательства Российской Федерации в области информационной безопасности. Стандарты и руководящие документы в области информационной безопасности. Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению информационной безопасности. Правовая защита информации и ИТ-активов. Цели, задачи, сущность правовой защиты прав обладателей информации, субъектов

персональных данных. Способы обеспечения правовой защиты информации. Основы ответственности за нарушение законодательства в информационной сфере.

РАЗДЕЛ 2. Защита прав субъектов персональных данных в образовательных организациях.

Тема 4. Введение в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

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. Способы обработки персональных данных. Предоставление персональных данных. Блокирование персональных данных. Уничтожение персональных данных. Обезличивание персональных данных. Доступ субъекта к персональным данным. Распространение персональных данных. Особенности обработки персональных данных в информационных системах персональных данных. Государственный контроль и надзор за обработкой персональных данных.

Тема 5. Правовые вопросы обработки персональных данных в образовательных организациях. Оценка возможного вреда субъектам персональных данных

Правовые меры обеспечения безопасности персональных данных при их обработке. Процессы обработки персональных в рамках трудовой деятельности, образовательной деятельности. Основания для обработки персональных данных. Согласие на обработку персональных данных. Отзыв согласия на обработку персональных данных. Договоры с субъектами персональных данных. Договоры поручения обработки персональных данных. Разъяснение субъекту условий обработки персональных данных. Обработка персональных данных, разрешенных субъектом для распространения. Иные правовые случаи обработки персональных данных. Политика в отношении обработки персональных данных. Реестр операторов персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.

Тема 6. Организация обработки персональных данных в образовательных организациях. Основные организационные процессы и документы

Локальные акты оператора, определяющие 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. Мероприятия по защите информации в информационных системах

Тема 7. 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 ИСПДн исходя из их архитектуры. Влияние архитектуры ИСПДн на безопасность.

Тема 8. Меры по идентификации и аутентификация субъектов доступа и объектов доступа. Меры и модели контроля доступа. Меры аудита и учета событий безопасности.

Принцип ААА. 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 9. Основы информационной безопасности вычислительных сетей

Структуры вычислительных сетей и основные компоненты. Корпоративные вычислительные сети. Протоколы взаимодействия в вычислительных сетях. Уязвимости и слабости в сетевых технологиях и связанные с этим угрозы. 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 10. 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 11. Подходы и меры защиты информации ограниченного доступа от утечки

Каналы утечки информации и методы несанкционированного доступа к информации ограниченного доступа. Организационные, технические, инфо-коммуникационные, комбинированные каналы утечки информации. Угрозы утечки видовой информации. Человеческий фактор. Угрозы, связанные с использованием носителей информации. Подходы к защите информации от утечки: мониторинг потоков (DLP), управление правами (IRM), защиты от несанкционированного доступа (СЗИ НСД).

Тема 12. Криптографическая защита информации. Защита каналов связи, носителей информации, 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. Методы криптографической защиты носителей информации. Электронная подпись. Виды электронных подписей в Российской Федерации. Инфраструктура электронной подписи.

Тема 13. Угрозы и риски информационной безопасности в образовательных организациях. Классификация уязвимостей. Модель угроз безопасности информации и ИТ-активов

Определение, анализ и классификация возможных угроз информационной безопасности в образовательных организациях. Источники угроз информационной безопасности. Преднамеренные и непреднамеренные угрозы информационной безопасности. Основные методы реализации угроз информационной безопасности. Риски информационной безопасности в

образовательных организациях. Методы оценки риска. Уязвимости систем обработки информации. Модель угроз безопасности информации: понятие, назначение. Практика написания модели угроз безопасности информации.

Тема 14. Обеспечение кибербезопасности. Характеристика видов и этапов осуществления кибератак. Меры защиты от атак. Мониторинг информационной безопасности

Понятие компьютерной атаки. Вектора, виды и этапы осуществления кибератак. Целевые атаки. Инструменты, используемые злоумышленником. Вредоносные программы: понятие, пути распространения, проявление действия вируса. Программы-шпионы, бэк-доры, трояны, сетевые черви, шифровальщики, бот-сети. Защита от воздействия вредоносных программ. Виды и назначение антивирусных программ и программ для защиты конечных точек (EPP). Системы обнаружения и предотвращения атак (IDS/IPS). Системы анализа трафика (NTA). Системы обнаружения распределенных атак и реагирования (EDR).

Понятие мониторинга как необходимой компоненты системы защиты информации. Классификация отслеживаемых событий. Особенности построения систем мониторинга. Системы управления событиями информационной безопасности (SIEM). Сканеры безопасности (XSpider, Сканер-ВС, nmap). Тестирование на проникновение.

Тема 15. Документация системы обеспечения информационной безопасности персональных данных в информационных системах

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

РАЗДЕЛ 3. ФОРМЫ АТТЕСТАЦИИ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Вид аттестации	Формы контроля	Виды оценочных материалов
Текущая	Устный опрос	Анализ представленных текущих работ, созданных в ходе работы слушателей
Промежуточная	Опрос по содержанию раздела	Тест
Итоговая	Итоговое тестирование	Тест

Промежуточный контроль осуществляется после изучения каждого раздела курса с использованием дистанционных образовательных технологий.

Слушатель в соответствии со своими образовательными потребностями и уровнем подготовленности может выбрать пороговый уровень промежуточной аттестации по каждой теме (тестирование) или повышенный уровень (решение практической задачи на материале организации).

Тест оценивается по шкале «зачтено – не зачтено» и считается успешно выполненным, если слушатель верно ответит на 60 и более процентов поставленных тестовых заданий. Для прохождения тестирования слушателю предоставляется две попытки, период прохождения тестирования – весь срок реализации ДПП. Взаимозависимости между прохождением промежуточной аттестации по предыдущей теме и допуском к прохождению следующей темы не устанавливается.

Практическое задание повышенной сложности оценивается преподавателем по 5-балльной шкале. Отметки 5, 4 и 3 – положительные.

Отметки 1-2 – неудовлетворительные и означают, что практическое задание считается невыполненным. Слушатель может изменить решение о прохождении того или иного уровня промежуточной аттестации. Например, получив неудовлетворительную отметку по результатам выполнения практического задания, можно перейти к выполнению теста. Итоговая аттестация осуществляется по накопительной системе. Для прохождения итоговой аттестации слушатель должен выполнить с положительной отметкой одно задание по каждой теме (на выбор – тестирование или практическое задание).

Примеры тестовых заданий

1. Что такое защита информации?

1) защита от несанкционированного доступа к информации;

2) выпуск бронированных коробочек для дискет;

3) комплекс мероприятий, направленных на обеспечение информационной безопасности;

4) небольшая программа для выполнения определенной задачи.

2. К какой группе мер по защите информации относится шифрование информации?

1) организационным;
2) техническим;
3) аппаратным;
4) программным.

3. Укажите принципы создания комплексной системы защиты информации:
1) неизменности;
2) прозрачности;
3) модульности;
4) рациональности;
5) доступности.

4. Внешние техногенные угрозы информационной безопасности обусловлены:
1) средствами связи и помехами от них;
2) близко расположенными опасными производствами;
3) некачественными программными средствами;
4) взаимодействием технических средств.

5. К какой группе угроз информационной безопасности относятся ошибки программного обеспечения?
1) стихийные;
2) техногенные;
3) программные;
4) антропогенные.

Примеры практических задач

1. Выделить нормативно-правовые акты, регулирующие циркулирование информации в организации (из списка организаций).
2. Выявить категории персональных данных и порядок обращения с ними в ситуации обращения за услугой в организацию (из списка ситуаций).
4. Выявить угрозы информационной безопасности в предлагаемой ситуации (общение в социальной сети, передача логина пароля специалисту обслуживающей организации).
5. Оценить действия сотрудника предприятия, приведшие к инциденту, СВЯЗАННОМУ С УГРОЗОЙ информационной безопасности (в предлагаемой ситуации).
6. Установка, настройка антивируса, проверка его работоспособности путем создания тестового вирусного файла.

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. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации № 646 от 05.12.2016 г.).

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.

На группу из 25 слушателей

- оборудованные аудитории для проведения аудиторных занятий;
- мультимедийное оборудование (компьютер, интерактивная доска, мультимедиа проектор);

Необходимое программное обеспечение:

– современный браузер (Google Chrome, Opera, Firefox или аналоги);

– текстовый редактор (Notepad или аналог);

– официальный дистрибутив программы (скачиваются с официального сайта разработчика либо из системы дистанционного образования во время занятий).

4.3. Образовательные технологии, используемые в процессе реализации программы

В процессе реализации программы используются лекции с элементами обсуждения проблем, практические занятия.