Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Костромской государственный университет»
Институт профессионального развития

Утвержден на заседании
Ученого совета КГУ
«17» ноября 2020 г.
Протокол № 4

Подписано цифровой подписью:
Тимонина Любовь Ильинична
Дата: 2021.03.25 14:00:50 +03'00'

Учебно-методический комплекс
по программе повышения квалификации

«Информационная безопасность»

Кострома
2020

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

1.1. Нормативные документы для разработки программы

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность» 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;

– 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».

1.2. Актуальность ДПП и область ее применения

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 № 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 РФ 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 различной ведомственной принадлежности, работающих с информацией и данными разных типов в области информационной безопасности.

Область применения ДПП –повышение квалификации сотрудников организаций любого типа и ведомственной принадлежности, которые работают в информационной сфере и обязаны выполнять требования информационной безопасности, установленные законодательством РФ.

1.3. Связь дополнительной профессиональной программы с профессиональными стандартами

Наименование ДПП	Наименование выбранного профессионального стандарта, ОТФ и/или ТФ	Уровень квалификации ОТФ и/или ТФ
Информационная безопасность	06.033 «Специалист по защите информации в автоматизированных системах»(зарегистрировано в Минюсте России 28 сентября 2016 г. № 43857). ОТФ:Обеспечение защиты информации в автоматизированных системах в процессе их функционирования.	6
	07.002 «Специалист по организационному и документационному обеспечению управления организацией». ОТФ: Организационное, документационное и информационное обеспечение деятельности руководителя организации.	6
	07.004 «Специалист по управлению документацией организации». ОТФ:Документационное обеспечение управления организацией.	6
	ОТФ 3.2: Управление деятельностью по документаци-	7

	онному обеспечению управления организацией.	
	ОТФ 3.3: Управление документацией организации.	8

1.4. Цель и задачи ДПП

Цель ДПП – формирование у слушателей готовности к реализации собственной профессиональной деятельности в полном соответствии с требованиями информационной безопасности.

Задачи ДПП:

- ознакомление слушателей с основными понятиями информационной безопасности, основными принципами построения систем защиты информации, а также основными категориями мер защиты информации, их возможностями с точки зрения защиты информации, сильными и слабыми сторонами;

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

- развитие умений оценки соответствия существующих решений требованиям защиты информации;

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

1.5. Планируемые результаты освоения ДПП

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

В результате освоения ДПП слушатель должен **знать:**

– базовый понятийный аппарат в области информационной безопасности;

– виды и состав угроз информационной безопасности;

– принципы и общие методы обеспечения информационной безопасности;

– основные положения обеспечения государственной политики обеспечения информационной безопасности;

– критерии, условия и принципы отнесения информации к защищаемой;

– виды носителей защищаемой информации;

– виды тайн конфиденциальной информации;

– виды уязвимостей защищаемой информации;

– источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;

– каналы и методы несанкционированного доступа к конфиденциальной информации;

– 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;

– 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 ДПП слушатель должен **владеть:**

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

В результате освоения ДПП слушатель должен **освоить компетенции:**

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

-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.

1.6. Категория слушателей и требования к уровню подготовки

Повышение квалификации по настоящей программе осуществляется на базе высшего и среднего профессионального образования. Программа повышения квалификации рассчитана на сотрудников предприятий и организаций, деятельность которых связана с процессами обработки информации конфиденциального характера.

Для освоения материала курса будут полезны основные знания из общего курса физики, высшей алгебры, теории чисел, информационных технологий. Их наличие позволит понять принципы действия криптографических средств защиты информации, средств технической защиты информации, а также цифровых стеганографических систем.

1.7. Срок освоения и форма обучения

Форма обучения: заочная, с применением дистанционных образовательных технологий.

Объем программы: 72 часа.

Срок освоения: 14 дней.

1.8. Формы промежуточной и итоговой аттестации

Промежуточная аттестация по темам ДПП включает в себя прохождения слушателями заданий двух уровней:

1) пороговый уровень – тестирование;

2) повышенный уровень – выполнение практического задания.

Итоговая аттестация организуется по накопительной системе. Для прохождения итоговой аттестации необходимо выполнить задания порогового или повышенного уровня по каждой из предложенных тем и получить положительную отметку за каждое из них.

1.9. Документ, который выдается слушателю по результатам освоения ДПП

Удостоверение о повышении квалификации установленного образца.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1.Объем и виды учебной работы, в том числе с использованием дистанционных образовательных технологий

Виды учебной работы	Всего, часов
Общая трудоемкость	72
Лекции	17
Практические (лабораторные) занятия	39
Самостоятельная работа	16

2.2.Учебно-тематический план

№ п/п	Наименование разделов	Всего, часов	В том числе		
			Лекции	Практические занятия	Самостоят. работа
Раздел 1. Организационные и правовые основы информационной безопасности					
1	Понятие цифровой экономики и компетенции цифровой эпохи	3	2	1	-
2	Значение информационной безопасности и ее место в системе национальной безопасности. Классификация видов национальной безопасности	6	1	3	2
3	Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности	7	2	3	2
4	Классификация информации, подлежащей защите. Государственные органы в области защиты информации	7	2	3	2
Раздел 2. Угрозы информационной безопасности					
5	Угрозы информационной безопасности	7	2	3	2
6	Виды атак на информационную систему	7	2	3	2

Раздел 3. Способы и методы защиты информации (при формировании индивидуальной траектории учитываются любые три темы раздела)					
7	Способы и методы защиты информации	9	2	5	2
8	Модели информационной безопасности	7	1	5	1
9	Классификация автоматизированных систем	7	1	5	1
10	Подходы к реализации и этапы построения систем защиты информации	6	1	4	1
11	Информационная безопасность интернета вещей	6	1	4	1
Итоговая аттестация: зачет					
Итого		72	17	39	16

2.3.Рабочая программа

РАЗДЕЛ 1.**Организационные и правовые основы информационной безопасности**

Тема 1.Понятие цифровой экономики и компетенции цифровой эпохи

Тенденции современного общества, критичные с точки зрения информационной безопасности. Становление и развитие понятия «информационная безопасность». Современные подходы к определению понятия. Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия «информационная безопасность». Значение информационной безопасности для субъектов информационных отношений.

Тема 2. Значение информационной безопасности и её место в системе национальной безопасности. Классификация видов национальной безопасности

Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности. Понятие и назначение доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Виды и состав угроз информационной безопасности. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.

Тема 3.Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности

Обзор законодательства России как основы для обеспечения интересов личности, общества и государства в информационной сфере. Характеристика стандартов в области информационной безопасности.

Тема 4. Классификация информации, подлежащей защите. Государственные органы в области защиты информации

Свойства информации как предмета защиты. Источник конфиденциальной информации. Сведения, которые могут быть отнесены к государственной тайне. Политический и экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну. Основные виды конфиденциальной информации, нуждающейся в защите. Коммерческая тайна. Банковская тайна. Основные объекты профессиональной тайны. Государственные органы в области защиты информации. Система безопасности РФ. Характеристика деятельности федеральных служб – основных государственных регуляторов в области информационной безопасности.

РАЗДЕЛ 2.**Угрозы информационной безопасность**

Тема 5. Угрозы информационной безопасности

Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

Тема 6. Виды атак на информационную систему

Основные способы несанкционированного доступа к конфиденциальной информации. Методы, используемые злоумышленниками для получения доступа к конфиденциальной информации либо вывода из строя информационной системы.

РАЗДЕЛ 3.**Способы и методы защиты информации**

Тема 7. Способы и методы защиты информации

Способы предупреждения возможных угроз. Способы обнаружения угроз. Способы пресечения или локализации угроз. Основные способы ликвидации последствий. Основные защитные действия при реализации способов защиты информации. Защита от разглашения. Защитные действия от утечки и от несанкционированных действий (НСД) к конфиденциальной информации. Мероприятия по технической защите информации.

Тема 8. Модели информационной безопасности

Основными структурными элементами информационной безопасности компьютерных систем в данной модели являются:

1.Цели защиты информации.

2.Субъекты, участвующие в процессах информационного обмена.

3.Угрозы безопасности информационных систем.

4.Уязвимость информации и информационной инфраструктуры. Понятие, классификация. Причины возникновения.

5. Риски информационной безопасности (ИБ). Классификация и оценка рисков ИБ. Методы сокращения рисков ИБ.

Обеспечение безопасности состоит в достижении трех взаимосвязанных целей: конфиденциальность, целостность и доступность.

Тема 9. Классификация автоматизированных систем

Понятие автоматизированной системы. Цели классификации автоматизированных систем. Подходы к классификации автоматизированных систем. Классификация автоматизированных систем и требования к обеспечению безопасности различных классов.

Тема 10. Подходы к реализации и этапы построения систем защиты информации

Реализация системы защиты информации на основе встраиваемых и встроенных средств защиты. Организация безопасной среды для обработки конфиденциальной информации. Этапы проектирования и реализации систем защиты конфиденциальной информации. Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации. Основные меры и архитектурные принципы обеспечения обслуживаемости информационных систем.

Тема 11. Информационная безопасность интернета вещей

Понятие Интернет вещей (IoT – internet of things), бытовые и промышленные IoT. Уязвимости IoT. Инцеденты безопасности, связанные с IoT. Обеспечение безопасности интернета вещей: безопасность связи, защита устройств, контроль устройств, контроль взаимодействия устройств в сети.

IoT становится все более распространенным явлением и все чаще появляется в системах, от которых зависит жизнь людей, например, автомобилях, самолетах и промышленном оборудовании, поэтому безопасность должна встраиваться в эти системы, чтобы они были безопасны по архитектуре, встроенной изначально.

2.4.Содержание и требования к самостоятельной работе слушателей

№	Название раздела, темы. Задание	Время, необходимое для выполнения задания	Форма контроля
1	*Раздел 1. Организационные и правовые основы информационной безопасности* Задание 1.Выделить нормативно-правовые акты, регулирующие циркулирование информации в организации (из списка организаций). Задание 2. Выявить категории персональных данных и порядок обращения с ними в ситуации обращения за услугой в организацию (из списка ситуаций). Задание 3. Выделить нормативно-правовые	6	Проверка письменного задания преподавателем, оценка результатов тестирования.

	акты закрепляющие недопустимость сокрытия или ограничения доступа к информации (из списка организаций). Задание 4. Подготовиться к тестированию по темам раздела.		
2	*Раздел 2.Угрозы информационной безопасность* Задание 1. Выявить угрозы информационной безопасности в предлагаемой ситуации (общение в социальной сети, передача логина/ пароля специалисту обслуживающей организации). Задание 2. Оценить действия сотрудника предприятия, приведшие к инциденту, связанному с угрозой информационной безопасности (в предлагаемой ситуации). Задание 3. Подготовиться к тестированию по темам раздела.	4	Проверка письменного задания преподавателем, оценка результатов тестирования.
3	*Раздел 3. Способы и методы защиты информации* Задание 1.Выполнить упражнения по проверке контрольной суммы файла, расшифровыванию фразы, вычислению результата хеширования. Задание 2. Проектирование модели угроз путем сопоставления угроз и методов их парирования (в предлагаемой ситуации). Задание 3. Подготовка к тестированию по темам раздела.	6	Предъявление отчета работы антивируса по обнаружению тестовой вирусной сигнатуры, проверка письменного задания преподавателем, оценка результатов тестирования.

2.6. Варианты индивидуальной траектории обучающихся

Индивидуальная траектория обучающихся реализуется за счет конкретных методических приемов:

- дифференциация практических заданий и самостоятельной работы слушателей на два уровня: пороговый и повышенный;

- вариативность при выборе тем для изучения. Темы из разделов 1 и 2 обязательны к изучению для всех слушателей курса. Темы из раздела 3 слушатель может выбирать по желанию, для успешного завершения курса слушателю необходимо освоить минимум три темы.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДПП

3.1. Материально-технические условия реализации программы

Для проведения занятий по программе повышения квалификации «Информационная безопасность» потребуется рабочее место, оснащенное персональным компьютером с высокоскоростным доступом к сетиИнтернет.

Необходимое программное обеспечение:

– современныйбраузер (GoogleChrome, Opera, Firefoxили аналоги);

– текстовый редактор (Notepadили аналог);

– официальный дистрибутив программыдля проверки контрольной суммы (скачиваются с официального сайта разработчика либо из системы дистанционного образования во время занятий).

3.2. Учебно-методическое и информационное обеспечение программы

Нормативно-правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.)(с учетом поправок, внесенных Законами Российской Федерацию поправках к Конституции Российской Федерации от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ,от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ).

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 28.07.2012г. №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 № 646от 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. 118 с. URL: http://znanium.com/catalog.php?bookinfo=925825 (дата обращения: 27.11.2019).

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: 27.11.2019).

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: 27.11.2019).

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: 27.11.2019).

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. *ГришинаН.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 27.11.2019).

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 27.11.2019).

3. *Артемов А.В.* Информационная безопасность: курс лекций. Орел: МАБИВ, 2014. 257с. URL: http://biblioclub.ru/index.php?page=book&id=428605(дата обращения 27.11.2019).

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 27.11.2019).

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 27.11.2019).

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.: Альфа-Пресс, 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 программ для проверки контрольных сумм с официальных сайтов разработчиков.

2. Справочно-информационная система (СИС) «Гарант».

3. Справочно-информационная система «Консультант».

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ
(Формы промежуточной и итоговой оценки, оценочные и методические материалы)

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 4-балльной шкале. Отметки 5, 4 и 3 – положительные. Отметка 2 – неудовлетворительная и означает, 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.
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) антропогенные.

6. Основные цели организационных мер защиты информации:
1) обеспечение правильности функционирования механизмов защиты;
2) предоставление бесперебойного доступа к необходимой информации авторизованным сотрудникам;
3) регламентация автоматизированной обработки информации;
4) шифрование информации.

7. Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Назовите тип этого злонамеренного кода:
1) макровирус;
2) троянский конь;
3) червь;
4) файловый вирус.

8. Самым слабым элементом в помещении с точки зрения звукоизоляции являются:
1) двери, стены, система заземления;
2) двери, пол, потолок;
3) двери, окна;
4) окна, система заземления, пол.

9. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?
1) организационное;
2) организационно-техническое;
3) техническо-организационное;
4) техническое.

10. Какие пункты относятся к активным методам защиты речевой информации?
1) создание маскирующих акустических и вибрационных помех;

2) выявление факта несанкционированного подключения к линии;
3) создание прицельных электромагнитных помех акустическим закладным устройствам;
4) выявление излучений акустических закладных устройств;
5) уничтожение средств несанкционированного подключения к телефонной линии.

11.В число основных принципов построения системы безопасности, с точки зрения её архитектуры, входят:
1) следование признанным стандартам;
2) применение нестандартных решений, не известных злоумышленникам;
3) разнообразие защитных средств.

12.Оценка рисков позволяет ответить на следующие вопросы:
1) Как спроектировать надежную защиту?
2) Какую политику безопасности предпочесть?
3) Какие защитные средства экономически целесообразно использовать?

13.Окно опасности появляется, когда:
1) становится известно о средствах использования уязвимости;
2) появляется возможность использовать уязвимость;
3) устанавливается новое программное обеспечение.

14.Окно опасности перестает существовать, когда:
1) администратор безопасности узнает об угрозе;
2) производитель программного обеспечения выпускает заплату;
3) заплата устанавливается в защищаемой информационной системе.

15.В число направлений физической защиты входят:
1) мобильная защита систем;
2) системная защита средств мобильной связи;
3) защита мобильных систем;
4) противопожарные меры;
5) межсетевое экранирование;
6) контроль защищенности;
7) физическая защита пользователей;
8) защита поддерживающей инфраструктуры;
9) защита от перехвата данных.

16.Политика безопасности:
1) строится на основе общих представлений об информационной системе организации;
2) строится на основе изучения политик родственных организаций;
3) строится на основе анализа рисков;
4) фиксирует правила разграничения доступа;
5) отражает подход организации к защите своих информационных активов;
6) описывает способы защиты руководства организации.

17.Оценка рисков позволяет ответить на следующие вопросы:
1) Как спроектировать надежную защиту?
2) Какую политику безопасности предпочесть?

3) Какие защитные средства экономически целесообразно использовать?
4) Чем рискует организация, используя информационную систему?
5) Чем рискуют пользователи информационной системы?
6) Чем рискуют системные администраторы?
7) Существующие риски приемлемы?
8) Кто виноват в том, что риски неприемлемы?
9) Что делать, чтобы риски стали приемлемыми?

18.Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией о методах использования уязвимостей?
1) да, поскольку знание таких методов помогает ликвидировать уязвимости;
2) нет, поскольку это плодит новых злоумышленников;
3) не имеет значения, поскольку, если информация об использовании уязвимостей понадобится, ее легко найти.

19.Риск является функцией:
1) вероятности реализации угрозы;
2) стоимости защитных средств;
3) числа уязвимостей в системе.

20.В число принципов физической защиты входят:
1) беспощадный отпор;
2) непрерывность защиты в пространстве и времени;
3) минимизация защитных средств.

21.В число основных принципов архитектурной безопасности входят:
1) применение наиболее передовых технических решений;
2) применение простых, апробированных решений;
3) сочетание простых и сложных защитных средств.

22.Меры информационной безопасности направлены на защиту от:
1) нанесения неприемлемого ущерба;
2) нанесения любого ущерба;
3) подглядывания в замочную скважину.

23.Из принципа разнообразия защитных средств следует, что:
1) в разных точках подключения корпоративной сети к Internet необходимо устанавливать разные межсетевые экраны;
2) каждую точку подключения корпоративной сети к Internet необходимо защищать несколькими видами средств безопасности;
3) защитные средства нужно менять как можно чаще.

24.При анализе стоимости защитных мер следует учитывать:
1) расходы на закупку оборудования;
2) расходы на закупку программ;
3) расходы на обучение персонала.

25.Обеспечение информационной безопасности зависит от:
1) руководства организаций;
2) системных и сетевых администраторов;
3) пользователей.

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).
3. Выделить нормативно-правовые акты, закрепляющие недопустимость сокрытия или ограничения доступа к информации (из списка организаций).
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. Проверить целостность файла путем вычисления и сравнения его контрольной суммы с помощью специализированного сертифицированного программного обеспечения.
7. Проверить авторство и подлинность документа, подписанного электронной подписью (с использованием специализированных сервисов в Интернет).
8. Проектирование модели угроз путем сопоставления угроз и методов их парирования (в предлагаемой ситуации).
9. Расшифровать сообщение с помощью специализированного ресурса.
10. Вычислить результат хеш-функции от предложенной фразы с помощью специализированного ресурса

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РАЗРАБОТКЕ И ОРГАНИЗАЦИИ КУРСА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «ИНФОРМАЦИОНАЯ БЕЗОПАСНОСТЬ» С ИСПОЛЬЗОВАНИЕМ ЭЛЕМЕНТОВ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

5.1. Основные подходы к включению элементов дистанционного обучения в различные формы организации ДПО

Использование элементов дистанционного обучения возможно при любой форме организации учебного процесса в ходе создания программ дополнительного профессионального образования.

При очной форме обучения курс имеет структуру, состоящую из двух элементов: присутственные занятия и самостоятельная работа слушателей. Дистанционные технологии могут быть использованы для обеспечения самостоятельной работы.

При очно-заочной форме обучения структура курса разделяется на три элемента: присутственные занятия, занятия в дистанционной форме и самостоятельная работа слушателей. Второй компонент такого курса обязательно и в полной мере обеспечивается учебными, методическими и оценочными материалами при использовании системы дистанционного обучения (СДО). При разработке и проведении нашего курса использовалась LMS (learningmanagementsystem) Moodle.

При заочной форме обучения присутственные занятия сводятся к минимуму (установочная и/или итоговая обзорная лекции) или отсутствуют вовсе. В этом случае весь материал курса обеспечивается средствами СДО. Образовательный контент в СДО должен включать саму учебную информацию (учебный материал), средства организации практической и самостоятельной работы обучающихся, средства оценивания, самооценивания и взаимооценивания обучающихся, средства организации взаимодействия обучающегося и преподавателя.

5.2. Проектирование дистанционных элементов в программе дополнительного профессионального образования

В зависимости от приведенных выше форм организации обучения по программе дополнительного профессионального образования система дистанционного обучения наполняется различными по объему компонентами, среди которых следующие.

1. Методические материалы по курсу, в том числе:

- пояснительная записка/инструкция для слушателя, в которой преподаватель рекомендует методику освоения курса, объясняет требования к промежуточной и итоговой аттестации;
- учебно-методический комплекс курса;

- видеолекция «О курсе» и иное.

2. Учебные материалы и оценочные средства, в которые входят:

- глоссарий;
- список источников и литературы для освоения курса;
- видеолекции;
- текстовые лекции или конспект видеолекции;
- видеозаписи практического занятия (методом «захват экрана» или иными способами);
- презентации;
- практические задания;
- тесты;
- дидактические игры и иное.

Варианты структуры дистанционного обеспечения курса ДПО представлены в таблице 1.

Объем образовательного контента определяется преподавателем исходя из рабочей программы курса, определяющей учебную нагрузку слушателей по всем видам работ.

При проектировании дистанционного обеспечения программы ДПО необходимо достичь такого баланса трудозатрат и образовательного контента, чтобы для освоения учебного материала в СДО слушателю требовался именно тот объем времени, который определен на эту тему в рабочей программе.

Достичь этого возможно объединяя экспертную оценку преподавателя и результаты апробации курса с привлечением отдельных слушателей и четким определением трудозатрат обучающегося.

Можно очень условно выделить нормативный показатель – один лекционный час соответствует не менее чем четырем стандартным страницам текста. Таким образом, базовый объем для курса составит произведение количества часов по учебному плану и нормативного показателя. Так, если по плану объем курса декларируется в 100 часов, то максимально допустимый объем основной части курса составит 400 стандартных страниц.

Под стандартной страницей понимается страница, сформированная в текстовом редакторе MS Word, в формате А4 со следующими параметрами:

- левое поле – 3 см;
- правое поле – 1 см;
- верхнее поле – не менее 2 см;
- нижнее поле – не менее 2 см;
- межстрочный интервал – одинарный;
- абзацный отступ – 1.25;
- шрифт Times New Roman;
- размершрифта 12;
- режим «выравнивание по ширине»;
- без расстановки переносов.

При проектировании учебного процесса по дисциплине с элементами дистанционного обучения необходимо учитывать следующие временные затраты обучаемых:

- изучение инструкций преподавателя по работе с курсом;
- изучение теоретических материалов курса;
- изучение основных и дополнительных источников из рекомендуемого библиографического списка;
- выполнение текущих контрольных заданий;
- подготовка и участие в контрольных мероприятиях (семинарах, чатах) как в режиме on-line, так и в режиме off-line;
- консультации с преподавателем как в режиме on-line, так и в режиме off-line;
- подготовка к аттестации и собственно аттестацию по курсу.

Суммарное время всех видов работ слушателя по курсу должно соответствовать количеству часов по учебному плану.

Для разработки курса с использованием элементов дистанционного обучения могут применяться три метода: пилотный (создание прототипа курса со всеми необходимыми технологическими элементами), метод шахт (проработка отдельной темы до логического конца одним из членов коллектива авторов) и метод пластов (разработка всех тем курса на одном глубоком методическом и техническом уровне одним автором).

Для первоначального построения курса необходимо использовать пилотный метод, который в значительной степени помогает избежать ложного старта (ощущения, что все сделано не так, отказ от предыдущей версии курса и работа по курсу «с нуля»). Кроме того, необходимо учесть то, что создание курса именно с помощью такого метода вполне доступно любому преподавателю университета, достаточно уверенно владеющему системой дистанционного обучения и материалом своей дисциплины.

При проектировании курса необходимо:

- определить целевые ориентиры программы ДПО, которые должны быть обусловлены результирующими компетенциями слушателей, иметь связь с профессиональными стандартами;
- произвести отбор учебного материала, форм и методов его представления, оценочных средств;
- провести четкую структуризацию учебного материала, выделив небольшие, легко усваиваемые блоки информации. Предпочтительно, чтобы темы в программе ДПО не были слишком крупными (оптимально – 2 часа);
- продумать единый стиль представления учебной информации. Хорошо, если удастся представить все темы в общих компонентах. Все дидактические компоненты (например, все лекции) должны иметь единую внутреннюю структуру и оформление;
- активно использовать различные формы наглядности, шире использовать иллюстративные элементы;

- обязательно использовать различные формы контроля учебных достижений слушателя. К наиболее распространенным относят тесты и практические задания. Тесты удобны автоматизированной проверкой. С их помощью можно обеспечить наполняемость курса отметками и повысить объективность итоговой аттестации. Практические задания предполагают качественную оценку и отзыв преподавателя. Это имеет большое обучающее значение для слушателей;

- продумывать формы обратной связи и взаимодействия преподавателя и слушателя. Среди них: форумы, чаты, электронная переписка, в том числе рассылка, содержащая методические советы по освоению курса.

Более детальный алгоритм разработки дистанционного курса выглядит как поэтапное решение следующих задач:

1. Определить цели и задачи курса.

2. Учесть особенности целевой группы, для которой создается этот курс, и выбрать методику дистанционного обучения с учетом целей курса - продумать организацию учебного процесса, методы взаимодействия преподавателя и студента (слушателя), виды и формы занятий.

3.Структурировать и подготовить учебный материал: разбить курс на разделы, а раздел - на небольшие смысловые части – темы (занятия). Каждый раздел и каждое занятие модуля должны иметь заголовок.

4.Осуществить подбор практических заданий для каждой темы.

5.Подготовить медиафрагменты: рисунки, таблицы, схемы, видеоряд (согласно требованиям эргономики).

6.Подобрать литературу и гиперссылки на ресурсы Интернет для каждого модуля (темы). Тщательный подбор ссылок позволит обучающемуся сэкономить массу времени, избавив от самостоятельного поиска информации, и даст возможность связать курс с лучшими мировыми информационными источниками.

7.Разработать систему контроля и оценки знаний студента: подобрать тесты, задачи, контрольные вопросы, темы рефератов и курсовых работ и т.п.

8.Продумать варианты организации обратной связи.

9.Разработать методические материалы по изучению курса, календарь курса.

10.Разместить материалы курса в системе дистанционного обучения.

11.Протестировать курс, в том числе на различных разрешениях экрана и различных браузерах.

12.Привлечь к апробации курса коллегу (коллег) и нескольких обучающихся для выработки критических замечаний по курсу.

13.Доработать курс с учетом высказанных замечаний.

14.Апробировать курс в дистанционном учебном процессе.

15.Модернизировать курс по результатам учебной апробации.

В дальнейшем модернизировать курс с учетом его использования в системе дистанционного обучения (в значительной мере опираясь на отзывы студентов, полученные в конце изучения дисциплины), а также с учетом достижений науки и техники.

Курс необходимо построить так, чтобы оказывать консультативную помощь студенту в минимально короткие сроки. Самым предпочтительным вариантом оказания консультаций является форум, позволяющий исключить дублирование вопросов.

Для успешного ведения образовательного процесса преподавателю необходимо предусмотреть организацию дистанционной мотивации студентов к выполнению учебных работ по курсу. Построение индивидуальной обратной связи, с фокусировкой внимания и усилий обучаемого, позволяет повысить эффективность обучения.

Курс должен быть построен так, чтобы отвечать требованиям декомпозиции, т.е. обладать возможностью изменения отдельных фрагментов курса без изменения курса в целом.

Критерий качества дистанционного курса можно определить так: «в любое время в любом месте доступно и понятно с первого раза».

Таблица 1

Возможные компоненты дистанционного обеспечения программы ДПО

№ п/п	Наименование элемента	Содержание элемента
1.	Титульные компоненты курса	Название курса; сведения об авторе (авторах); аннотация.
2.	Учебно-методический комплекс	Рабочая программа; методическое обеспечение курса.
3.	Методические указания по освоению курса	Руководство к изучению дисциплины и прохождению промежуточной и итоговой аттестации; методические рекомендации к разделам курса и отдельным оценочным средствам.
4.	Учебный материал	Электронные лекции; презентации; аудиолекции; видеолекции.
5.	Практические материалы	Практические и лабораторные работы; Семинары.
6.	Оценочные материалы	Вопросы к зачету (экзамену); перечень тем рефератов, курсовых работ (проектов); задания для контрольных и самостоятельных работ; вопросы и тесты для самопроверки; промежуточные тесты; контрольные тесты.
7.	Глоссарий	Основные понятия, термины и определения, использующиеся при изучении курса.
8.	Список источников информации	Список основной учебной литературы; список дополнительной литературы (справочные из-

		дания и словари, периодические и отраслевые издания, научная литература и т.п.); ссылки на Интернет-ресурсы.

5.3. Требования к содержанию компонентов дистанционного обеспечения программы ДПО

5.3.1. Титульные компоненты курса

Титульные элементы курса включают название курса, сведения об авторе/авторах, аннотацию.

Название курса должно максимально точно отражать его содержание. Не допускается расхождение наименования, которое определяет ожидания слушателей, и содержания курса.

Сведения об авторе (авторах). В сведениях об авторе указывается фамилия, имя, отчество разработчика курса, ученая степень и ученое звание. Рекомендуется указать опыт и практические компетенции преподавателя в области курса.

В аннотации необходимо указать, для какой аудитории предназначается курс, его цели и задачи. При этом необходимо помнить, что цель – это конечный результат, а задачи – этапы и действия, посредством выполнения которых достигается поставленная цель.

Аннотация также может содержать методические рекомендации по освоению курса. Нужно указать последовательность и характер работы с разными элементами курса, их предназначение.

Важно четко и однозначно определить требования к слушателям по прохождению ими текущей и итоговой аттестации.

Этот элемент включается в аннотацию, если в курсе не разрабатывается отдельный элемент – методические рекомендации по освоению курса.

В том случае, если курс преподается не автором-разработчиком или курс разработан группой авторов, необходимо четкое указание того, кто именно будет работать со слушателями данной группы. Нужно определить характер взаимодействия с преподавателем, каналы коммуникации.

5.3.2. Учебно-методические комплекс курса в структуре программы ДПО

Учебно-методический комплекс включает в себя:

- общую характеристику курса, его актуальность, цели, задачи, связь с профессиональными стандартами, результаты освоения курса, формы и сроки, в которых реализуется курс;

- рабочую программу курса, в том числе содержание курса и тематический план, требования к самостоятельной работе, промежуточной и итоговой аттестации;

- методическое обеспечение курса, которое включает в себя методические рекомендации для преподавателей и слушателей, учебно-методическое обеспечение, материально-техническое обеспечение курса.

Одной из самых важных частей УМК является описание содержания курса. Лучше организовывать курс по модульному принципу, т.е. разбивать содержание курса на модули или разделы, каждый из которых ограничен определенным временем и информационно логически замкнут, представляя из себя четко определенный объем учебного материала. Результат работы с модулем должен фиксироваться одним или несколькими видами контрольных мероприятий. Рекомендуемое число модулей в течение семестра равно трем, по аналогии с количеством рубежных контролей.

При написании аннотаций, помимо определения основных смысловых акцентов модуля, необходимо отметить особенность каждого модуля и его важность в общей структуре курса, заострить внимание студента (слушателя) на особенно трудных или своеобразных моментах и т.п.

Модуль, в свою очередь, разбивается на более мелкие структурные единицы – темы или занятия. Именно эта структурная единица курса является аналогом обычного аудиторного занятия. Как правило, тема должна в своем составе содержать несколько разнородных видов учебной деятельности (учебный материал, практические задания и оценочные средства), содержание и состав которых должны быть достаточными для усвоения содержания темы за 2 академических часа.

5.3.3. Разработка методических указаний по освоению курса

Руководство к изучению дисциплины содержит методические указания по изучению дисциплины, выполнению контрольных, практических и лабораторных работ, организации самостоятельной работы, определяет количество контрольных заданий, которые нужно выполнить для допуска к итоговой аттестации по программе курса, а также форму промежуточной и итоговой аттестации. Представляет собой комплекс разъяснений и указаний, помогающих студенту эффективно организовать процесс обучения. При разработке данного элемента необходимо помнить о том, что основная часть курса изучается студентом самостоятельно, а значит, необходимо максимально предусмотреть все возможные сложности и вопросы для любого этапа дистанционного курса.

В общих методических указаниях желательно отдельно оговорить следующие позиции:

- дополнительные программы, необходимые для комфортного прохождения курса;
- основную методику работы с курсом (самостоятельная работа, работа в группе, работа с преподавателем, порядок ликвидации задолженностей и т.д.);
- требования к начальной подготовке, необходимые для успешного усвоения дисциплины;
- рекомендации по организации обратной связи и т.п.

Методические указания к модулю или теме могут содержать следующие позиции:

- цели и задачи;
- обязательная и дополнительная литература с указанием конкретных страниц (в случае необходимости);
- перечень заданий, которые надо выполнить;
- требования к выполнению заданий и критерии их оценивания;
- контрольные сроки выполнения заданий;
- примерное (рекомендуемое) распределение времени на изучение модуля (темы);
- указания требуемых (допустимых) уровней усвоения;
- предупреждающие ответы на часто задаваемые студентами (слушателями) вопросы.

Таким образом, этот элемент курса в зависимости от своего назначения может варьироваться – от общего руководства по изучению дисциплины до пояснения к отдельным темам курса и различным рекомендациям более узкого характера (например, рекомендации по работе с литературой).Описывая каждый элемент курса как можно подробнее, с максимальным количеством инструкций, преподаватель предупредит поток единообразных вопросов и уточнений, а студентам (слушателям) поможет легко сориентироваться в новом для них курсе.

Иногда построение курса логично требует составления методических указаний не в целом по курсу, а по каждой теме. Но в любом случае указания должны быть сформулированы так, чтобы студент имел возможность от учебной деятельности под руководством преподавателя перейти к самостоятельному освоению курса и самоконтролю.

Тематический план-график курса определяет порядок изучения и преподавания учебного курса, расписание проведения учебных занятий всех видов и контрольных мероприятий изучаемой дисциплины. Включает в себя:
- сроки прохождения курса, модуля, темы;
- формы и время отчетности;
- график практических и семинарских занятий;
- график консультаций.

5.3.4. Методические требования к разработке и представлению учебных материалов

Гипертексты. Должны содержать развернутое системное изложение модуля, в котором раскрывается содержание каждого учебного элемента. Кроме ссылок на основную литературу должны содержать ссылки на дополнительные и сетевые информационные ресурсы. Информация, представленная в элементе, должна быть достаточной для ответа на контрольные и тестовые задания. Стиль изложения в этом элементе, как правило, академический.

Электронные лекции. Именно в этом структурном элементе должна содержаться основная учебная информация, при этом лекция должна быть организована и наполнена так, чтобы:

- обзорно освещать материал с выделением ключевых вопросов;

- содержать всю необходимую информацию для успешного ответа на промежуточные и контрольные вопросы по теме и тестовые задания;

- минимизировать обращение студента к дополнительным источникам информации;

- включать в себя дополнительные элементы для иллюстрации изучаемого материала: звук, видео, графику, анимацию и т.д.; при этом включаемые элементы не должны превалировать над основным информационным содержанием лекции, не должны отвлекать внимание студента (слушателя) от основного учебного процесса;

- содержать обобщающие таблицы, диаграммы, схемы, графики, отражающие главные сведения или выводы. Материал, представляемый в такой форме, должен быть наглядным и содержать емкие комментарии;

- содержать ссылки (список рекомендуемой литературы по теме) на литературные источники по теме согласно приведенной библиографии в рабочей программе курса, с указанием конкретных глав, разделов, страниц;

- включать вопросы для самопроверки (в разной форме) после каждого раздела (темы) лекции;

- завершаться краткими выводами с целью ориентирования студента на определенную совокупность сведений, которые следует надежно усвоить и запомнить.

Аудиолекции, видеолекции в некоторых случаях более предпочтительны, чем электронная лекция. Например, вводную, установочную лекцию оправданно представлять в видеоряде: в этом случае сразу же налаживается личностный контакт студент-преподаватель и дальнейшее обучение становится не безличным. Аудиолекции удобны для студента тем, что, в отличие от электронного текста, изучать их можно в более широком диапазоне времени. Но необходимо помнить, что при включении данных элементов в курс может ограничиваться возможность комфортного их использования из-за высоких требований к хранению информации большого объема и низкой пропускной способности каналов связи.

Презентации. Презентационные материалы отражают основные понятия дисциплин (терминологию), содержат иллюстративные, схематические, графические материалы и позволяют в обобщенном и наиболее привлекательном виде представить содержание дисциплины. Их использование значительно повышает информативность и выразительность подаваемого материала, поскольку при этом одновременно задействованы как слуховой, так и зрительный каналы восприятия информации.

Подборки статей или фрагменты учебных пособий необходимо использовать в том случае, если необходимая информация недоступна или содержится в объемных изданиях; также указанные источники могут использоваться в иных случаях, оправданных логикой курса.

5.3.5. Методические рекомендации по разработке практических материалов

Практические работы. Блок должен содержать практические задания, которые студенту необходимо выполнить для получения допуска к итоговой аттестации по дисциплине.

Практические занятия могут организоваться с использованием средств вебинаров, или с использованием видеозаписей практической работы преподавателя, или с использованием инструмента «захват экрана», если практическое выполняется с использованием персонального компьютера.

В практикум желательно включать примеры решения типовых задач и задач, аналогичных тем, которые включены в задания для итоговой аттестации. Необходимо предусмотреть блок, в котором будут представлены задачи для самостоятельной проработки.

Лабораторные работы. Блок должен содержать лабораторные работы, которые студенту необходимо выполнить для получения допуска к аттестации по дисциплине. Этот элемент, независимо от того, используются ли в курсе виртуальные лабораторные работы или их проведение запланировано на очную аттестационную сессию, должен включать в себя методические указания по проведению работ.

Семинары – активный деятельный элемент курса, направленный на многие цели:

- итоговое осмысление изучаемого материала;
- качественное изучение наиболее проблемных теоретических тем курса;
- коллективное обсуждение теоретических и методических вопросов курса;
- формирование психологического климата в группе, ее сплоченности;
- развитие навыков работы в коллективе.

При планировании данного элемента в обязательном порядке необходимо предусмотреть точные формулировки по подготовке к семинару и его проведению (заранее озвучить темы семинара, важность семинара в общей структуре курса, условия участия в нем и его оценки и т.д., т.е. фактически подготовить план семинара). Проведение семинара возможно как в режиме on-line с помощью средств вебинара, так и в режиме off-line (с помощью инструмента «Семинар») – в зависимости от целей и назначения. При проведении семинара в режиме on-line необходимо для «сбора» группы в определенное время использовать все возможные ресурсы: электронную почту, новостной форум, электронную доску объявлений, рассылки и т.п. Учитывая возможности и результативность элемента, настоятельно рекомендуется его использование в курсе не менее двух раз, но не чаще, чем один раз в две недели.

При подготовке всех практических материалов необходимо соблюдать следующие требования:

- тесная связь с теоретическим учебным материалом;

- конкретность, ясность формулировки;
- комплексность видов;
- разнообразие ступеней сложности;
- наличие нескольких вариантов с четкой системой выбора варианта (например, для контрольных работ);
- отсутствие организационных трудностей в выполнении;
- оптимальность объема в соответствии с нормами времени на самостоятельную работу.

5.3.6. Методические рекомендации по разработке оценочных материалов

Вопросы к зачету (экзамену): допускается приведение примерных вопросов.

Перечень тем рефератов, докладов, проектов, учебных исследований помимо собственно названий тем должен содержать рекомендации к выполнению работ (проектов, исследований), требования к их оформлению и другую информацию, необходимую, с точки зрения преподавателя, для успешной реализации задачи.

Задания для контрольных и самостоятельных работ должны сопровождаться четкими указаниями по их выполнению и выбору номера варианта.

Вопросы и тесты для самопроверки – необязательные, но желательные для выполнения студентами задания по изучаемой теме для более полного ее усвоения и закрепления.

Промежуточные тесты должны, в том числе содержать в себе задания (или аналогичные им), используемые при формировании тестов самоконтроля.

Контрольные тесты должны содержать в себе задания для проверки уровня знаний по всему теоретическому курсу.

Опыт дистанционного обучения показывает, что нужна отчетность за каждый модуль или тему курса; студенту нельзя двигаться дальше, не изучив и «закрыв» текущий раздел. Наличие в курсе такого контроля смотивирует слушателя на ежедневную планомерную работу. Однако возможны ситуации, особенно при обучении взрослых, когда преподаватель не устанавливает зависимости между выполнением одного и другого задания.

При составлении тестов важно использовать разные типы тестовых заданий:

- открытые задания. Предполагают пропуск ключевого термина, смысловой части утверждения. Допускается пропуск одного или двух слов, не более. Пропущенные слова должны быть однозначными и сущностными в предлагаемом утверждении;
- закрытые задания. Обучающемуся предлагается незавершенное утверждение, которое надо завершить выбором правильного варианта или вариантов. Предлагаемые варианты должны содержать верные и неверные ответы. Невер-

ных ответов должно быть столько же или больше, чем верных. Неверные ответы не должны быть абсурдными, но и не должны специально «мимикрировать» под верные ответы. Отличия между верными и неверными ответами должны быть сущностными;

- задания на соответствие. В этом случае обучающемуся предлагается соотнести одну группу компонентов с другой. Установление правильной связи показывает освоение учебного материала. Важно оставлять один лишний компонент в одном из двух рядов, чтобы последняя пара не формировалась автоматически;

- задания на установление правильного порядка. Слушатель должен расставить категории в правильном порядке. Этот порядок определяется преподавателем в задании. Может быть хронологический порядок или порядок от общего к частному и т.д.;

- задания в форме эссе. Это задание предполагает ответ в свободной форме. Оно проверяется преподавателем и, как правило, имеет больший вес в итоговой оценке, чем другие типы заданий.

Методические требования к составлению тестов ограничивают задания в вопросной и отрицательной форме. Искомое задание лучше размещать в начале утверждения.

Тест может быть ограничен по времени выполнения, по сроку, по количеству попыток. Эти ограничения вводятся преподавателем для достижения педагогических целей. Преподаватель также принимает решение о пороговом значении верных ответов, которое нужно достичь для получения положительной отметки по тесту.

5.3.7. Методические рекомендации по разработке иных компонентов курса с использованием элементов дистанционного обучения

Глоссарий

Обеспечивает толкование и определение основных понятий и терминов, необходимых для осмысления и освоения учебного материала в полном объеме. Формируется в алфавитном порядке и с гиперссылками из разделов курса.

Список источников информации

Должен включать в себя списки основной и дополнительной литературы, составленные в порядке значимости источников для изучения дисциплины и оформленный в соответствии с ГОСТ 7.1–2003. Желательно наличие ссылок на Интернет-ресурсы. Преподаватель должен принять в учет доступность рекомендованной литературы и источников для слушателей.

Иллюстративный материал

Электронный ресурс подразумевает большое количество иллюстративного материала, помогающего облегчить пользователю курса усвоение теоретического материала, поэтому его подготовка требует особой продуманности и тщательности.

Иллюстрации должны быть выполнены с высоким качеством и в форматах .jpg, .gif, .cdr, .wmf. В любом случае следует избегать экзотических форматов данных. Во всех случаях необходимо принять меры по минимизации объема графического файла. Формулы, которые набираются в редакторе MS Equation (MathType), сохраняются (для облегчения дальнейшего внедрения в оболочку ДО) как html-файл или набираются непосредственно во встроенном в оболочке редакторе формул TEX.

Анимация. Некоторые задачи обучения (например, показ динамики некоторого процесса) для большей наглядности требуют включения в курс анимации: мультфильмов или видеофильмов в форматах .swf или .avi (без сжатия).

5.4. Проектирование вариативности программы ДПО

Вариативность в рамках программы ДПО может обеспечиваться рядом методических способов:

- проектирование содержательных компонентов курса в нескольких уровнях сложности;
- проектирование компонентов курса в разном содержании, которое зависит от образовательных потребностей обучающихся;
- проектирование оценочных средств с дифференциацией уровня сложности (например, тесты – пороговый, обязательный уровень; открытые практические задания – повышенный уровень сложности);
- проектирование самостоятельной работы с дифференциацией по содержанию (например, освоение онлайн-курса или серия заданий, предложенных преподавателем);
- проектирование самостоятельной работы с дифференциацией по уровню сложности;
- проектирование промежуточной аттестации с вариативными маршрутами (накопительная система, решение итогового интегративного задания, выполнение проекта или исследования и др).

Проектирование вариативного курса повышает его образовательный потенциал, позволяет индивидуализировать процесс обучения.

5.5. Методические рекомендации по проектированию содержания курса «Информационная безопасность»

Проблемы информационной безопасности могут рассматриваться с различных позиций. При формировании курса нами были выбраны три основных раздела:

- Организационные и правовые основы информационной безопасности;
- Угрозы информационной безопасности;
- Способы и методы защиты информации.

Эти разделы являются базовыми с точки зрения построения целостного курса по информационной безопасности.

В первом разделе освещены темы, содержащие понятийный аппарат и обзор нормативно-правовой базы, на которую опирается информационная безопасность в России:

- Понятие цифровой экономики и компетенции цифровой эпохи;
- Значение информационной безопасности и её место в системе национальной безопасности. Классификация видов национальной безопасности;
- Базовое законодательство в области информационных технологий и защиты информации;
- Стандарты в области информационной безопасности;
- Классификация информации, подлежащей защите. Государственные органы в области защиты информации.

Выбор тем обусловлен важной специфической особенностью терминологической системы информационной безопасности – ее тесной связью с правовой лексикой. Это следствие того факта, что информационная безопасность давно перестала быть технической дисциплиной или частью информатики, получив большой, постоянно развивающийся организационно-правовой блок.

Осваивая темы первого раздела, слушатели получают знания о структуре нормативно-правовой базы информационной безопасности в России, области действия и применения нормативных документов и зоны ответственности государственных регуляторов.

Второй раздел курса посвящен обзору и классификации угроз информационной безопасности и возможных атак на информационные системы. Главной целью деятельности по обеспечению информационной безопасности является превентивное обнаружение и нейтрализация угроз, и только за этим – противодействие атакам.

Практическая ценность тем второго раздела заключается в приобретении слушателями навыков распознавания и классификации угрозы или атаки информационной безопасности.

Третий раздел курса «Способы и методы защиты информации» является центральным с точки зрения построения систем безопасности. В нем разобраны темы:

- Способы и методы защиты информации;
- Модели информационной безопасности;
- Классификация автоматизированных систем;
- Подходы к реализации и этапы построения систем защиты информации.

Темы раздела выбраны с точки зрения максимального охвата вопросов построения систем защиты: учет требований регуляторов в области информационной безопасности, знакомство с конкретными криптографическими методами защиты информации, получения целостного представления о всей системе защиты информации.

Осваивая темы третьего раздела, слушатели получают навыки применения средств криптографической защиты информации, построения модели нарушителя информационной безопасности.

При условии расширении объема курса и в зависимости от выбранного направления углубления, его можно дополнить.

В направлении «Организация и управление информационной безопасностью» актуальными будут темы:

- Политика информационной безопасности предприятия;
- Ведение режима секретности в организации и на предприятии;
- Моделирование систем информационной безопасности.

В направлении технической защиты информации курс может быть дополнен темами:

- Противодействие техническим каналам утечки информации;
- Технические средства противодействия несанкционированному доступу к информации.

В направлении программно-аппаратной и криптографической защиты информации курс может быть дополнен темами:

- Построение защищенной сети предприятия средствами VPN, Криптографические средства защиты;
- Использование электронных подписей для ведения юридически значимого электронного документооборота.

При необходимости сокращения объема курса из него могут убраны либо уменьшены до краткого упоминания темы:

- Классификация автоматизированных систем;
- Подходы к реализации и этапы построения систем защиты информации.

Сложность практических заданий одинакова на всем протяжении курса. Но в зависимости от базового образования слушателя различные темы будут восприниматься по-разному. Первый раздел покажется проще в освоении слушателями с гуманитарным или юридическим базовым образованием. Слушатели с техническим базовым образованием с легкостью будут воспринимать второй и третий разделы курса. При изучении курса рекомендуется начинать с просмотра видеолекции, затем изучить конспект лекций и презентации (для закрепления материала). При выполнении практических заданий необходимо воспринимать задачу с позиции собственного опыта и применительно к своей профессиональной деятельности.

При изучении тем первого раздела слушатель самостоятельно изучает содержание нормативных документов в официальной редакции.

При изучении тем второго раздела слушатель самостоятельно изучается банк данных угроз и уязвимостей ФСТЭК. Также рекомендуется провести анализ собственного опыта или опыта родственников и коллег на предмет признаков угроз информационной безопасности или совершенных атак безопасности.

При изучении тем третьего раздела слушатель самостоятельно знакомится с пользовательским интерфейсом, изучает руководства пользователя конкретных средств защиты информации.

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СЛУШАТЕЛЕЙ, ОСВАИВАЮЩИХ КУРС "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Освоение курса "Информационная безопасность" требует от слушателя заинтересованности и участия в нескольких видах деятельности.

Методические рекомендации по освоению курса позволят решить поставленные задачи максимально эффективно.

Курс состоит из четырех компонентов:

- лекционные и практические занятия, организованные в присутственной форме;
- лекционные и практические занятия, организованные с использованием дистанционных технологий;
- самостоятельная работа;
- промежуточная и итоговая аттестация.

Все материалы структурированы по разделам и темам.

Для успешного освоения курса рекомендуем следующую логику действий слушателя:

- посещение присутственных занятий. Оптимально, если слушатель заранее ознакомится с содержанием тем в СДО. Это позволит преподавателю не репродуцировать учебный материал, а работать в диалоге со слушателями, поясняя сложные моменты, выявляя неочевидное содержание и взаимосвязи между компонентами учебного материала, объясняя связь учебного материала с жизненным опытом слушателей;
- просмотр видеолекций и видеозаписей практических занятий. При невозможности посетить присутственное занятие слушатель может воспользоваться видеозаписью. Работа с видеозаписью лекции предпочтительна для тех слушателей, у кого доминирующим каналом усвоения учебного материала является слуховой. В видеозаписи соединены текст лекции и презентация. Видеозапись практического занятия, выполненного способом «захват экрана» поможет слушателям освоить практические приемы работы с цифровыми средствами;
- работа с электронными лекциями. Хорошо, если слушатель не просто читает лекции, а аналитически обрабатывает их. Для такой обработки необходимо выявлять внутреннюю структуру материала, взаимосвязи и иерархию между его компонентами. Если совершать эти операции мысленно сложно, можно посоветовать составление развернутого плана материала, конспекта лекции, мнемонических схем, таблиц, рисунков;
- работа с презентациями. Презентация соответствует содержанию лекции, иллюстрирует и визуализирует ее. Презентация помогает структурировать материал. Она содержит самые важные элементы учебного материала;

- самостоятельная работа заключается в освоении всех компонентов курса по предложенным темам вне непосредственного контакта с преподавателем, в удобном темпе и в удобное время. Слушателю необходимо обратить внимание, какой объем самостоятельной работы предполагается по каждой из тем. Раздел 2.4. УМК конкретизирует содержание и задания по самостоятельной работе;

- промежуточный и итоговый контроль. Для самоконтроля прохождения курса и контроля со стороны преподавателей слушателям предлагается выполнить ряд заданий. Основными типами заданий являются тесты и практические задания.

Для прохождения промежуточной аттестации необходимо хорошо проработать содержание темы. При выполнении практических заданий слушателям рекомендуется соединять жизненный опыт с новыми компетенциями. Ответ должен быть точно по сути вопроса, лаконичным и структурированным. Ответ не должен быть заимствованным. Объем – не более 0,5 страницы.

Итоговая аттестация проводится по накопительной системе. Для прохождения итоговой аттестации необходимо выполнить пороговый или повышенный уровень заданий по каждой из предложенных тем. Подробно условия прохождения итоговой аттестации представлены в разделе 4 данного УМК.

Обращаем внимание слушателей на вариативные траектории освоения курса.

Слушатель может выбрать один из двух предложенных уровней заданий по каждой теме.

Пороговый уровень представлен тестом. Вы можете проходить тест дважды. Тест оценивается по шкале "зачтено - не зачтено". Чтобы получить зачет, вам необходимо правильно ответить на 60 и более % заданий.

Повышенный уровень представлен практическим заданием открытого типа. Вам необходимо выполнить задачу, поставленную преподавателем, и написать ответ в произвольной форме. Этот тип заданий оценивается по 4-балльной шкале.

Итак, по каждой теме слушатель может выбрать - пройти тест или выполнить практическое задание.

Для связи с преподавателем можно воспользоваться форумом или электронной почтой, сервисом «комментарии». В ходе курса осуществляется информационная и методическая рассылка, которая помогает слушателям в обучении и самоорганизации.

Освоение курса потребует от слушателей 72 часа присутственной и самостоятельной работы. Планомерная работа позволит завершить курс успешно, освоить новые компетенции и получить удостоверение о повышении квалификации.

7. СОСТАВИТЕЛИ ПРОГРАММЫ

Щекочихин Олег Владимирович, кандидат технических наук, заведующий кафедрой защиты информации Костромского государственного университета.

Кузнецов Александр Юрьевич, кандидат технических наук, доцент факультета безопасности информационных технологий Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет ИТМО».

Алексеев Дмитрий Станиславович, кандидат технических наук, доцент кафедры защиты информации Костромского государственного университета.

Виноградова Галина Леонидовна, кандидат технических наук, доцент кафедры защиты информации Костромского государственного университета.