ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ
проект«Онлайн Академия «ЦИФРОСФЕРА»
АНО ДПО «МЦК «ЦЕЛЬ»

МЦК ЦЕЛЬ
АНО ДПО в составе группы SPG

УТВЕРЖДАЮ

О.В. Самоварова
Директор АНО ДПО «МЦК «Цель»
14.10.2020

Протокол заседания
педагогического совета
№ 11 от 13.10.2020

Титульный лист программы

АНО ДПО «МЦК «Цель»

Дополнительная профессиональная программа повышения квалификации

«Основы кибербезопасности для пользователей информационных систем»

72 час.

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ
ДЛЯ ПОЛЬЗОВАТЕЛЕЙ
ИНФОРМАЦИОННЫХ СИСТЕМ
проект«Онлайн Академия «ЦИФРОСФЕРА»
АНО ДПО «МЦК «ЦЕЛЬ»

2020 год

ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.Цель программы

Цель программы - сформировать и развить у пользователей ПК профессиональные компетенции, позволяющие им применять современные технологии защиты информации, выбирать средства и инструменты защиты информации, минимизирующие угрозы несанкционированного доступа к данным.

2.Планируемые результаты обучения:

Перечень формируемых профессиональных компетенций (ПК):

ПК-1 Способность определять риски, угрозы и уязвимости информационных ресурсов, компьютерных сетей и данных.
ПК-2 Способность использовать существующие методы, стандарты и средства защиты данных.

В результате обучения слушатель получит:

2.1. Знание (осведомленность в областях)

Основные методики и инструментарий применения способов и методов решения задач обеспечения личной КБ, а также КБ на предприятиях и в организациях государственного и частного сектора.
Основной инструментарий и программное обеспечение для решения задач обеспечения КБ данных.

2.2. Умение (способность к деятельности)

Применять методики и инструментарий способов и методов для построения и оценки эффективности математических моделей различных процессов КБ. Рассчитывать эти модели и интерпретировать результаты расчетов для оценки параметров процессов КБ.
Выбирать инструментарий и ПО для решения задач обеспечения КБ данных

2.3 Навыки (использование конкретных инструментов)

Обоснования возможности и эффективности применения статистических методов при решении задач обеспечения КБ.
Использования программных продуктов, решающих задачи обеспечения КБ данных.

3.Категория слушателей (возможно заполнение не всех полей)

4.1. Образование: высшее, среднее специальное
4.2. Квалификация: -
4.3. Наличие опыта профессиональной деятельности: -
4.4. Предварительное освоение иных дисциплин/курсов /модулей: -

4.Учебный план программы «Основы кибербезопасности для пользователей информационных систем»

№ п/п	Модуль	Всего, час	Виды учебных занятий		
			лекции	**Практичес-кие занятия**	**Самостоятельная работа**
1	Вводный модуль	**8**	**5**	**2**	**1**
2	Управление кибербезопасностью	**12**	**5**	**6**	**1**
3	Система кибербезопасности	**10**	**3**	**6**	**1**
4	Техническая защита информации (данных)	**16**	**7**	**8**	**1**
5	Защита информации с использованием шифровальных (криптографических) средств	**5**	**2**	**2**	**1**
6	Комплексная защита объектов информатизации (объектов защиты)	**19**	**7**	**11**	**1**
Итоговая аттестация		**2**		Итоговое контрольное задание – 1 ч.	Выходная диагностика – 1 ч.
		72			

5.Календарный план-график реализации образовательной программы

(дата начала обучения – дата завершения обучения) в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

№ п/п	Наименование учебных модулей	Трудоёмкость (час)	Сроки обучения
1	Вводный модуль	**8**	**01.11-02.11**
2	Управление кибербезопасностью	**12**	**03.11 -06.11**
3	Система кибербезопасности	**10**	**07.11-09.11**
4	Техническая защита информации (данных)	**16**	**10.11-13.11**
5	Защита информации с использованием шифровальных (криптографических) средств	**5**	**14.11**
6.	Комплексная защита объектов информации (объектов защиты)	**19**	**15.11-19.11**
	Итоговая аттестация	**2**	**20.11**
Всего:		**72**	**01.11-20.11**

6.Учебно-тематический план программы «Основы кибербезопасности для пользователей информационных систем»

№ п/п	Модуль / Тема	Всего, час	Виды учебных занятий			Формы контроля
			лекции	практические занятия	самостоя-тельная работа	
1	**Вводный модуль**	**8**	**5**	**2**	**1**	Самоконтроль--рефлексия
1.1	Введение в КБ	2	1		1	
1.2	Теория и методология КБ	2	1	1		
1.3	Правовое обеспечение и стандарты КБ	1	1			
1.4	Проблемы КБ	1	1			
1.5	Методы атак и способы защиты	2	1	1		
2	**Управление кибербезопасностью**	**12**	**5**	**6**	**1**	Самоконтроль--рефлексия
2.1	Управление КБ	2	1	1		
2.2	Аудит КБ	2	1	1		
2.3	Управление рисками КБ	3	1	2		
2.4	Стандарты КБ	3	1	1	1	
2.5	Конфиденциальное делопроизводство	2	1	1		
3	**Система кибербезопасности**	**10**	**3**	**6**	**1**	Самоконтроль--рефлексия
3.1	Система КБ	5	1	3	1	
3.2	Аттестация объектов информатизации	5	2	3		
4	**Техническая защита информации (данных)**	**16**	**7**	**8**	**1**	Самоконтроль--рефлексия
4.1	Классификация и идентификация угроз КБ в ИС. Уязвимость ИС	3	1	1	1	
4.2	Оценка уровня защищенности ИС	2	1	1		

4.3	Средства и методы защиты информации. Современные технические средства защиты информации	2	1	1		
4.4	Проектирование систем защиты информации	2	1	1		
4.5	Антивирусное ПО	2	1	1		
4.6	Средства защиты от несанкционированного доступа к данным	3	1	2		
4.7	Сетевые атаки и поиск уязвимостей	2	1	1		
5	**Защита информации с использованием шифровальных (криптографических) средств**	**5**	**2**	**2**	**1**	Самоконтроль--рефлексия
5.1	Криптография	3	1	1	1	
5.2	Электронная подпись	2	1	1		
6	**Комплексная защита объектов информатизации (объектов защиты)**	**19**	**7**	**11**	**1**	Самоконтроль--рефлексия
6.1	Комплексная защита объектов информатизации и систем данных	6	1	4	1	
6.2	Администрирование Windows	2	1	1		
6.3	Защита персональных данных	3	1	2		
6.4	Коммерческая тайна	1	1			
6.5	Безопасность в глобальных сетях	3	1	2		
6.6	Защита систем управления базами данных (СУБД) и ОС	2	1	1		
6.7	Поиск уязвимостей	2	1	1		
7	**Аттестация**	**2**	**0**	**1**	**1**	

7.1	Зачет	1		1		Зачет
7.2	Выходная диагностика	1			1	Выходная диагностика
	Итого	72	29	36	7	

7. Учебная (рабочая) программа повышения квалификации «Основы кибербезопасности для пользователей информационных систем»

Модуль 1. Вводный модуль 8 час. (в том числе 2 часа практики)
Тема 1.1 Введение в КБ
Содержание темы: Основные понятия КБ, направления деятельности в области защиты информации и данных. История развития проблемы защиты информации. Типовые причины и популярные методы атак на информационные ресурсы и системы со стороны злоумышленников, и их последствия.
Тема 1.2 Теория и методология
Содержание темы: Теория кибербезопасности и методология защиты данных.
Тема 1.3 Правовое обеспечение и стандарты КБ
Содержание темы: Правовое, нормативное и методическое регулирование деятельности в области защиты информации. Обзор нормативно правового обеспечения информационной безопасности и защиты информации РФ. Отраслевые и межотраслевые индустриальные стандарты и нормативные документы в области кибербезопасности. Организационное обеспечение информационной безопасности в РФ. Анализ мировых систем защиты информации и международных нормативных документов в области кибербезопасности.
Отраслевые и межотраслевые индустриальные стандарты, а также иные внутренние и международные нормативные документы в области информационной безопасности.
Тема 1.4 Проблемы КБ
Содержание темы: Современные проблемы информационной безопасности. Биометрическая и поведенческая идентификация: мифы и реальность. Как защититься от фрода и типовых атак на информационные ресурсы.
Тема 1.5 Методы атак и способы защиты
Содержание темы: Популярные методы, типовые причины атак со стороны злоумышленников. Основные способы защиты информационных систем, в том числе и веб-приложений, обеспечения безопасности и целостности данных от атак злоумышленников.

Модуль 2. Управление кибербезопасностью (**в том числе 6 часов практики)**
Тема 2.1 Управление КБ
Содержание темы: Управление кибербезопасностью. Структура подразделения КБ и особенности организации его работы на предприятии. Общественные и некоммерческие организации в КБ. Крупнейшие ежегодные форумы и конференции. Научные и отраслевые средства информации.
Тема 2.2 Аудит КБ
Содержание темы: Аудит кибербезопасности (АКБ) и методы его проведения. Методы анализа данных при АКБ. Способы и рекомендации по обследованию объектов защиты и обобщения данных о их состоянии. Методика проведения аудита информационной безопасности. Подходы, задачи и содержание работ при проведении

АКБ. Современные программные средства для проведения АКБ и особенности использования различных сканеров безопасности.

Тема 2.3 Управление рисками КБ

Содержание темы: Анализ информационных рисков. Управление информационными рисками. Программные средства анализа рисков информационной безопасности. Библиотеки найденных и опубликованных критических уязвимостей в операционных системах и серверах.

Тема 2.4 Стандарты КБ

Содержание темы: Стандарты информационной безопасности. Международный стандарт управления информационной безопасностью ISO 17799. Управление защитой информации в соответствии с ISO 27001.

Тема 2.5 Конфиденциальное делопроизводство

Содержание темы: Организация конфиденциального делопроизводства.

Модуль 3. Система кибербезопасности (**в том числе 6 часов практики)**

Тема 3.1. Система КБ

Содержание темы: Система информационной безопасности, ее элементы и связи между ними. Создание и развитие системы информационной безопасности.

Тема 3.2 Аттестация объектов информатизации

Содержание темы: Подготовка документов для аттестации объектов информатизации по требованиям безопасности данных. Методики обоснования выбора средств технической и криптографической защиты данных. Проверка и настройка технических средств и ПО защиты данных.

Модуль 4. Техническая защита информации (**в том числе 8 часов практики)**

Тема 4.1 Классификация и идентификация угроз КБ в ИС. Уязвимость ИС

Содержание темы: Идентификация угроз и уязвимостей информационных систем и приложений. Общепринятые классификации угроз информационной безопасности. Классификация технических каналов утечки данных. Виды уязвимостей автоматизированных информационных систем. Различные методологии поиска уязвимостей информационных ресурсов, компьютерных сетей и приложений.

Тема 4.2 Оценка уровня защищенности ИС

Содержание темы: Оценка уровня защищённости информационных систем.

Тема 4.3 Средства и методы защиты информации. Современные технические средства защиты информации.

Современные технические методы и средства защиты конфиденциальной информации. Особенности эксплуатации технических средств защиты информации. Применение шифровальных (криптографических) средств защиты информации различных производителей.

Тема 4.4 Проектирование систем защиты информации

Содержание темы: Порядок проектирования технических систем защиты информации. Оценка защищенности конфиденциальной информации (конфиденциальности данных) от утечки по техническим каналам.

Тема 4.5 Антивирусное ПО

Содержание темы: Возможности антивирусного программного обеспечения. Выбор, установка, настройка и эксплуатация средств антивирусной защиты.

Тема 4.6 Средства защиты от несанкционированного доступа к данным

Содержание темы: Программно-аппаратные средства защиты информации от несанкционированного доступа к данным.

Тема 4.7 Сетевые атаки и поиск уязвимостей

Содержание темы: Сетевые атаки и анализ трафика. Особенности использования различных сканеров безопасности. Средства обнаружения вторжения и утечек данных. Работа со сканерами уязвимостей. Методология составления отчета о проведенном поиске уязвимостей. Основные способы защиты от атак на типовые уязвимости приложений.

Модуль 5 Защита информации с использованием шифровальных (криптографических) средств

(**в том числе 2 часа практики)**

Тема 5.1 Криптография

Содержание темы: Основы шифрования (СКЗИ). Криптографические методы защиты информации. Технологии криптографической защиты информации. Защита автоматизированных систем с помощью средств криптографической защиты информации.

Тема 5.2 Электронная подпись

Содержание темы: Использование современных систем защиты информации. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.

Модуль 6 Комплексная защита объектов информатизации. (**в том числе 11 часов практики)**

Тема 6.1 Комплексная защита объектов информатизации и систем данных

Содержание темы: Концепция безопасности и принципы построения комплексных систем защиты информации в организации. Информационная безопасность автоматизированных систем и данных.

Тема 6.2 Администрирование Windows

Содержание темы: Основные принципы администрирования Windows и работа с PowerShell.

Тема 6.3 Защита персональных данных

Содержание темы: Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн). Классификация ИСПДн. Трансграничная передача персональных данных.

Тема 6.4 Коммерческая тайна

Содержание темы: Особенности защиты информации, составляющей коммерческую тайну компании. Защита и обработка конфиденциальных документов и данных.

Тема 6.5 Безопасность в глобальных сетях

Содержание темы: Безопасность беспроводных систем передачи данных. Безопасность веб-приложений. Анализ программного кода веб-сервисов на наличие уязвимостей. Безопасность мобильных приложений. Тестирование программного обеспечения, в том числе и веб-приложения, на наличие потенциальных и скрытых уязвимостей.

Тема 6.6 Защита систем управления базами данных (СУБД) и ОС

Содержание темы: Принципы работы СУБД и основы обеспечения их безопасности. Анализ целостность данных СУБД. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры.Найденные и опубликованные критические уязвимости в операционных системах и оборудовании.

Тема 6.7 Поиск уязвимостей

Содержание темы: Самостоятельная проверка технических средств и настроек сетевого и серверного программного обеспечения на наличие уязвимостей. Тестирование информационных систем и серверов хранения данных на наличие известных и широко распространенных уязвимостей. Состав и актуальность последних

обновлений операционных систем и программного обеспечения для обеспечения информационной безопасности.

Аттестация (2 ак. час, в том числе 1 час практики)
Зачет на основании выполненного итогового контрольного задания, выходной диагностики по программе, наличия отчетов по самоконтролю-рефлексии..

Описание практико-ориентированных заданий и кейсов

	Номер темы/модуля	**Наименование практического занятия**	**Описание**
1	Вводный модуль		
1.1	Введение в КБ	Поиск информации о известных атаках на информационные ресурсы. Анализ инцидентов	Поиск информации об известных атаках на информационные ресурсы. Анализ инцидентов
1.2	Теория и методология КБ	Разработка проекта защиты информации на объекте, предложенном слушателями	Разработка проекта защиты информации на объекте, предложенном слушателями
1.3	Правовое обеспечение и стандарты КБ	Самостоятельное изучение предложенной нормативной документации	Самостоятельное изучение предложенной нормативной документации
1.4	Проблемы КБ	Самостоятельное изучение предложенной нормативной документации	Самостоятельное изучение предложенной нормативной документации
1.5	Методы атак и способы защиты		
2	Управление кибербезопасностью		
2.1	Управление КБ	Самостоятельное изучение предложенных стандартов информационной безопасности	Самостоятельное изучение предложенных стандартов информационной безопасности
2.2	Аудит КБ	Разработка плана проведения аудита КБ на конкретном примере	Разработка плана проведения аудита КБ на конкретном примере
2.3	Управление рисками КБ	Разработка матрицы рисков КБ на конкретном примере	Разработка матрицы рисков КБ на конкретном примере

2.4	Стандарты КБ	Самостоятельное изучение предложенной нормативной документации	Самостоятельное изучение предложенной нормативной документации
2.5	Конфиденциальное делопроизводство	Работа с системами электронного документооборота с возможностью шифрования документов	Работа с системами электронного документооборота с возможностью шифрования документов
3	Система информационной безопасности		
3.1	Система КБ	Разбор элементов системы информационной безопасности	Разбор элементов системы информационной безопасности
3.2	Аттестация объектов информатизации	Самостоятельное изучение предложенной нормативной документации	Самостоятельное изучение предложенной нормативной документации
3.3	Компьютерная криминалистика и развитие систем КБ		
4	Техническая защита информации		
4.1	Классификация и идентификация угроз КБ в ИС. Уязвимость ИС	Разработка модели угроз на конкретном примере. Разработка плана поиска уязвимостей на конкретном примере	Разработка модели угроз на конкретном примере. Разработка плана поиска уязвимостей на конкретном примере
4.2	Оценка уровня защищенности ИС	Разработка плана оценки защищенности конкретной системы	Разработка плана оценки защищенности конкретной системы
4.3	Средства и методы защиты информации. Современные технические средства защиты информации	Демонстрация средств защиты информации. Демонстрация средств криптографической защиты информации (СКЗИ)	Демонстрация средств защиты информации. Демонстрация СКЗИ
4.4	Проектирование систем защиты информации	Разработка проекта системы защиты информации на конкретном примере	Разработка проекта системы защиты информации на конкретном примере
4.5	Антивирусное ПО	Установка и настройка средств антивирусной защиты	Установка и настройка средств антивирусной

			защиты
4.6	Средства защиты от несанкционированного доступа	Демонстрация средств защиты от НСД, настройка	Демонстрация средств защиты от НСД, настройка
4.7	Сетевые атаки и поиск уязвимостей	Анализ сетевого трафика.	
5	Защита информации с использованием шифровальных (криптографических) средств		
5.1	Криптография	Демонстрация методов кодирования, помехозащищенное кодирование, самостоятельное кодирование и декодирование с помощью простейших кодов.	Демонстрация методов кодирования, помехозащищенное кодирование, самостоятельное кодирование и декодирование с помощью простейших кодов.
5.2	Электронная подпись	Практическое использование электронной подписи. Подписание электронных документов. Тест по разделу 5.	Практическое использование электронной подписи. Подписание электронных документов
6	Комплексная защита объектов информатизации		
6.1	Комплексная защита объектов информатизации	Разработка комплексной системы защиты информации на конкретном примере	Разработка комплексной системы защиты информации на конкретном примере
6.2	Администрирование Windows	Настройка параметров безопасности Windows. Демонстрация работы с PowerShell	Настройка параметров безопасности Windows. Демонстрация работы с PowerShell
6.3	Защита персональных данных	Классификация ИСПДн на конкретном примере. Самостоятельное изучение предложенной нормативной документации	Классификация ИСПДн на конкретном примере. Самостоятельное изучение предложенной нормативной документации
6.4	Коммерческая тайна	Использование различных средств шифрования документов. Передача зашифрованных документов по электронной почте	Использование различных средств шифрования документов. Передача зашифрованных документов по электронной почте

6.5	Безопасность в глобальных сетях	Рассмотрение конкретных приложений для поиска возможных уязвимостей	Рассмотрение конкретных приложений для поиска возможных уязвимостей
6.6	Защита СУБД и ОС	Демонстрация работы с СУБД	Демонстрация работы с СУБД
6.7	Поиск уязвимостей	Тестирование информационной системы для поиска уязвимостей. Общее выходное тестирование.	Тестирование информационной системы для поиска уязвимостей. Общее выходное тестирование.
7	Аттестация		
7.1	Зачет		

8.Оценочные материалы по образовательной программе

8.1. Вопросы тестирования по модулям

№ модуля	Вопросы входного тестирования	Вопросы промежуточного тестирования	Вопросы итогового тестирования
1	в пункте 8.4 вопросы входной диагностики	не предусмотрена, описание самоконтроля/рефлексии - см. пункт 8.5.	в пункте 8.4 вопросы входной диагностики

8.2. описание показателей и критериев оценивания, шкалы оценивания .

Оцениваемые показатели - уровень сформированности компетенций, заявленных в Приложении 2.
Критерии оценивания - унифицированные значения оценок уровня владения знаниями, умениями, навыками по итогам входной и выходной диагностики.

Методика оценки:

1. Для каждого слушателя проводятся входная и выходная диагностики уровней сформированности компетенций (перечислены в приложении №2).
2. Оценочная шкала результатов оценки компетенций определяется в %-ной системе.
3. По результатам проведения входной и выходной диагностики, производится определение количества правильных ответов на унифицированные вопросы диагностики по формуле:

$$П_к = В_к - Н_к, \quad \text{где:}$$

- П к - Количество правильных ответов по компетенции
- В к- Количество вопросов по компетенции
- Н к- Количество неправильных ответов по компетенции

4. По итогам определения количества правильных ответов, определяется их доля в количестве вопросов. Определение результата оценки по компетенции (в %) производится по формуле:

$$Р_к\ (\%) = П * 100 / В, \quad \text{где:}$$

- Р к - Результат оценки по компетенции

- П к - Количество правильных ответов по компетенции
- В к - Количество вопросов по компетенции

5. Далее результат оценки по компетенциям усредняется и вычисляется среднее значение оценки по всем компетенциям, по формуле:

$$Р\ (\%) = (Р\ к1 + Р\ к2) : 2 \text{ , где}$$

- Р - результат оценки по компетенциям.

6. Далее слушателю присваивается оценка по результатам выходной диагностики - по 100%-ной шкале оценивания:

- значение Р вых более 75% - “отлично”;
- значение Р вых более 60%, но менее или равно 75% - “хорошо”;
- значение Р вых от 40% до 60% - “удовлетворительно”;
- значение Р вых менее 40% - “неудовлетворительно”;

Где Р вых - результат оценки по итогам выходной диагностики

7. Далее (справочно и по запросу) производится определение образовательного прироста компетенций слушателя - отдельно по каждой компетенции, или сразу по всем компетенциям, по формуле:

$$Пр = Р\ вых - Р\ вх \text{ , где:}$$

- Пр - образовательный прирост
- Р вых - результат оценки по итогам выходной диагностики
- Р вх - результат оценки по итогам входной диагностики

8.3. примеры контрольных заданий по модулям или всей образовательной программе .

Аттестационное испытание

Зачет:

– Успешное выполнение итогового контрольного задания по эффективной работе с задачами по кибербезопасности (правильное выполнение не менее 50% задач задания).
– Выполнение выходной диагностики (согласно п.8.2 не ниже «удовлетворительно»).
– Предоставление отчетов о самоконтроле-рефлексии в установленной форме в установленные сроки.

8.4. тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий .

Вопросы входной /выходной диагностики уровня сформированности компетенций:

Примеры вопросов:

ПК-1 Способность определять риски, угрозы и уязвимости информационных ресурсов, компьютерных сетей и данных.

1. Чем регулируется ответственность за нарушение информационной безопасности во внешней среде с целью нанести вред владельцу информации, а также вопросы взаимоотношений между различными субъектами?
   - внутренними корпоративными документами
   - федеральными законами РФ, региональными, муниципальными и пр. нормативными актами (верно)
   - международными стандартами в области информационной безопасности
   - Доктриной информационной безопасности
2. Чем регулируется ответственность за причинение вреда и ответственность за реализацию мероприятий по разработке, внедрению и использованию систем КБ во внутренней среде?

- внутренними корпоративными документами (верно)
- действующим законодательством РФ и стран, с которыми осуществляется бизнес (верно)
- международными стандартами в области информационной безопасности
- Доктриной информационной безопасности

3. Чем регулируется ответственность за формирование и реализацию КБ в различных областях информационной деятельности предприятия?

- внутренними корпоративными документами (верно)
- действующим законодательством РФ и стран, с которыми осуществляется бизнес
- международными стандартами в области информационной безопасности
- Доктриной информационной безопасности

5. К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности (верно)

6. Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций (верно)

7. Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы (верно)
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

8. Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации (верно)

9. Принципом политики информационной безопасности является принцип:

- Разделения доступа (обязанностей, привилегий) клиентам сети (системы) (верно)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

ПК-2 Способность использовать существующие методы, стандарты и средства защиты данных.

9. Цифровой сертификат содержит:

- открытый ключ пользователя; (верно)
- секретный ключ пользователя;
- имя пользователя.

10. Криптография необходима для реализации следующих сервисов безопасности:

- идентификация;
- экранирование;
- аутентификация. (верно)

11. Криптография необходима для реализации следующих сервисов безопасности:

- контроль конфиденциальности; (верно)
- контроль целостности;
- контроль доступа.

12. Экран выполняет функции:

- разграничения доступа; (верно)
- облегчения доступа;
- усложнения доступа.

13. Демилитаризованная зона располагается:

- перед внешним межсетевым экраном;
- между межсетевыми экранами; (верно)
- за внутренним межсетевым экраном.

14. Экранирование на сетевом и транспортном уровнях может обеспечить:
    - разграничение доступа по сетевым адресам; (верно)
    - выборочное выполнение команд прикладного протокола;
    - контроль объема данных, переданных по TCP-соединению.
15. Системы анализа защищенности помогают предотвратить:
    - известные атаки; (верно)
    - ошибки пользователей
    - разрыв соединения с сервером

Самоконтроль-рефлексия

Вопросы для реализации самоконтроля-рефлексии:

- Выполнение каких упражнений из модуля “…..” далось Вам легче всего?
- Как Вы думаете, по какой причине Вам легко далось выполнение определенных упражнений из Модуля “...”?
- Выполнение каких упражнений из Модуля “…..” далось Вам труднее всего?
- Как Вы думаете, по какой причине Вам оказалось трудным выполнение определенных упражнений из Модуля “...”?
- Как вы оцените ваши достижения, в развитии Ваших знаний, умений и навыков по итогам выполнения практических заданий из Модуля “...” по 5 бальной шкале, где 1-мало продвинулся(ась), 2 - сделал(а) небольшие продвижения, 3- продвинулся(ась) достаточно для своего темпа, 4 - продвинулся(ась) хорошо, 5 - Продвинулся(ась) отлично, могу перечислить знания умения и навыки, которые выработались во время выполнения проектов

Примеры заданий для рефлексии (См. список практических занятий в таблице “Описание практико-ориентированных заданий и кейсов”):

1. **«Работа со справочно-информационными правовыми системами «КонсультантПлюс» и «Гарант»»**

Цель работы: приобретение практических навыков работы с информационной правовой системой «КонсультантПлюс» и «Гарант» по вопросам защиты информации.

Пояснения к работе

Справочные правовые системы (СПС) КонсультантПлюс и «Гарант» включают все законодательство РФ: от основополагающих документов до узкоотраслевых актов. Для удобства поиска информации все документы содержатся в Едином информационном массиве. Поскольку документы каждого типа имеют свои специфические особенности, они включаются в соответствующие Разделы информационного массива (рис. 1, рис. 2). Названия разделов сформулированы таким образом, чтобы можно было легко ориентироваться, какие документы в каком разделе находятся. Каждый из разделов Единого информационного массива, в свою очередь, состоит из близких по содержанию Информационных банков.

Порядок работы

Запустить справочно-правовую систему «КонсультантПлюс».

Ознакомиться со структурой и возможностями Стартового окна информационно-справочной системы «КонсультантПлюс».

Войти из Стартового окна в режим «Обзоры». Просмотреть всю информацию в разделе: Правовые новости.

Из Стартового окна перейти в раздел «Законодательство». Ознакомиться с общим построением справочно-информационной правовой системы «КонсультантПлюс».

Изучить поочередно все подпункты основного меню системы. Зайти в «Карточку поиска», рассмотреть все её элементы.

Зайти в режим Правового навигатора. Изучить: особенности поиска информации по конкретному правовому вопросу; двухуровневую структуру словаря; ключевые понятия и группы ключевых понятий; различные виды сортировки списка.

Найти нормативно-правовые документы, используя различные виды поиска.

Изучить самостоятельно возможности СПС «Гарант».

Задание:

1) Проверить представленные документы на предмет их соответствия и действия по состоянию на 15.02.15.
2) Расположить их по степени важности и принадлежности к правовым группам (видам нормативного акта).
3) Указать документы, утратившие силу.
4) Дополнить указанный список документами РТ по вопросам информационной безопасности.
5) Дополнить список документами, не включёнными в перечень, необходимыми при изучении вопросов Информационной безопасности.

Перечень документов

Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.

Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента Российской Федерации от 12 мая 2009 г. № 537.

Основы организации защиты информации в Приволжском федеральном округе (Одобрены Решением Координационного Совета по защите информации при полномочном представителе Президента Российской Федерации в Приволжском федеральном округе от 12 ноября 2009 года).

Концепция защиты информации ограниченного доступа в РТ.

Конституция Российской Федерации.

Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности"

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»

Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»

«Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утверждено постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 г. № 912-51.

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».

Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

Указ Президента Российской Федерации от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании

информационно-телекоммуникационных сетей международного информационного обмена".

Приказ Федеральной службы охраны Российской Федерации от 7.08.2009 № 487 "Об утверждении положения о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

Федеральный закон РФ от 29 июля 2004 г № 98-ФЗ «О коммерческой тайне».

Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности»

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. Изучение основных положений Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149- ФЗ в последней редакции.

Краткие теоретические сведения

Информация существовала всегда. Независимо ни от чего, она была отражением объективно существующей действительности. Но пришло время, когда информации выпало играть первостепенную роль не только в простом человеческом общении, но и во всех сферах жизнедеятельности общества. Постепенно эта роль обрела коммерческое содержание.

Развитие науки н техники, особенно в эпоху рыночных отношений, показывает, насколько важной может быть информация. Ее достоверность и оперативное получение сегодня являются залогом правильности и своевременности принятия любого решения.

В основе информационного законодательства находится свобода информации и запретительный принцип права (все, что не запрещено законом - разрешено). Это закреплено в основных как международных, так и российских правовых документах, например, в ст. 3 Всеобщей декларация прав человека от 10.12.48 г. и в ст. 29 Конституции РФ, принятой 12.12.93 г.

В целях реализации этих прав и свобод принимаемые законодательные акты устанавливают:

- гарантии;
- обязанности;
- механизмы защиты;
- ответственность.

За минувшие годы в России было принято значительное число нормативных актов, в том числе федеральных законов, указов Президента и постановлений Правительства Российской Федерации, как всецело посвященных вопросам регулирования отношений, возникающих в процессе создания, преобразования и потребления информации, так и затрагивающих информационные отношения отдельными нормами. Совокупность юридических норм, регулирующих информационные отношения, образует сравнительно новую и активно развивающуюся отрасль российского законодательства, получившую в литературе название федерального информационного права.

Информационное законодательство – это совокупность норм права, регулирующих общественные отношения в информационной сфере.

Предмет информационного законодательства составляют следующие вопросы:

- права граждан и других субъектов права на информацию;
- правовой режим информации и информационных ресурсов;
- государственная политика и управление в сфере информации и информатизации;
- правовое положение информационных центров и автоматизированных систем;

- вопросы собственности, владения и распоряжения;
- правовые вопросы, возникающие при оказании информационных услуг;
- информация в условиях рынка и развития предпринимательства;
- индустрия информатизации, информационные ресурсы;
- международно-правовое сотрудничество в сфере информации и информатизации.

Следует также выделить некоторые отрасли законодательства, нормы которых в значительной степени посвящены вопросам, связанным с информацией:

- законодательство об информационной безопасности:
- законодательство об информационных ресурсах, которое, в свою очередь, можно условно разделить на:

законодательство о правовой информации;
законодательство о международном обмене информацией;
законодательство о связи;
законодательство о персональных данных;
законодательство об архивном фонде и архивах;
законодательство о библиотечном деле;
законодательство о статистической информации:

- законодательство о служебной и коммерческой тайне;
- законодательство о государственной тайне;
- законодательство о средствах массовой информации.

Нормы об информации также содержатся в законодательстве об интеллектуальной собственности (исключительных правах), которое включает в себя:

- законодательство об авторском праве н смежных правах;
- патентное законодательство;
- законодательство о товарных знаках обслуживания и наименованиях мест происхождения товаров;
- законодательство о фирменных наименованиях;
- законодательство об открытиях.

В настоящее время законодательная база в информационной сфере включает пакет Федеральных законов, Указов Президент РФ, постановлений Правительства РФ, обеспечивающих нормативное регулирование как процессов информационного обмена, так и формирования информационного общества, т.е. информатизации.

Порядок выполнения работы

Задание 1. Изучить содержание Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ.

Задние 2. Подготовить протокол выполнения лабораторной работы, в котором отразить: название работы, цель работы, пояснения по ходу выполнения работы, ответы на контрольные вопросы.

Контрольные вопросы:

1) Предмет информационного законодательства.
2) Термины, используемые в Федеральном законе от 27 июля 2006 года №149-ФЗ, их определения.
3) Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
4) Информация как объект правовых отношений.
5) Права и обязанности обладателя информации.
6) Доступ к информации.
7) Государственное регулирование в сфере применения информационных технологий.
8) Государственные информационные системы.

9) Порядок ограничения доступа к информации, распространяемой с нарушением закона.
10) Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

3. «Разработка справочника специалиста по информационной безопасности»

Порядок выполнения работы:

Задание 1. Изучить требования законодательства в сфере информационной безопасности.

Задние 2. Разработать и оформить справочник специалиста по информационной безопасности.

Предполагаемый вариант содержания справочника:

Конституция Российской Федерации.

Конституция РТ.

Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента Российской Федерации от 12 мая 2009 г. № 537.

Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.

Основы организации защиты информации в Приволжском федеральном округе (Одобрены Решением Координационного Совета по защите информации при полномочном представителе Президента Российской Федерации в Приволжском федеральном округе от 12 ноября 2009 года).

Концепция защиты информации ограниченного доступа в РТ.

Трудовой кодекс РФ.

Положение о Совете Безопасности РТ

Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности"

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»

Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»

«Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утверждено постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 г. № 912-51.

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».

Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

Указ Президента Российской Федерации от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена".

Приказ Федеральной службы охраны Российской Федерации от 7.08.2009 № 487 "Об утверждении положения о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

Федеральный закон РФ от 29 июля 2004 г № 98-ФЗ «О коммерческой тайне».

Гражданский кодекс РФ.

Уголовный кодекс РФ
Федеральный закон РФ от 21 июля 1993 г № 5485-1 -ФЗ «О государственной тайне».
Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».
Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности»
Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
Глоссарий по основным понятиям информационной безопасности.

4. «Решение ситуационных задач по теме: «Информационные преступления в сфере компьютерной информации и меры защиты от них»

Теоретическая часть:
Алгоритм решения задачи включает в себя следующую последовательность действий:
1. Ответ на поставленный вопрос;
2. Законодательная (нормативная) база;
3. Обоснование решения со ссылкой на соответствующие законодательные предписания и фактические обстоятельства дела (фабулу).

В качестве образца предлагается решение задачи:
В деянии А.Иванова можно усмотреть признаки состава преступления, предусмотренные ст. 274 УК РФ «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей ». законодательная база для решения задачи – ст. 274 УК РФ, примечания к ст. 272 УК РФ.

Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии А.Иванова усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей. Он также обладает признаками субъекта данного преступления – вменяем и достиг 16 лет. Субъективная сторона преступления характеризуется виной как в форме умысла, так и неосторожности.

Однако, вопрос об уголовной ответственности А.Иванова зависит от того, в каком размере был причинен ущерб его деянием, так как состав преступления является материальным. Согласно примечанию к ст. 22 УК РФ крупным ущербом в статьях данной главы признается ущерб сумма которого превышает один миллион рублей. Таким образом, А.Иванов будет подлежать уголовной ответственности по ч. 1 ст. 274 УК РФ, если его деянием причинен ущерб на сумму свыше одного миллиона рублей.

Задачи:
Студент заочного отделения А.Иванов решил использовать компью-тер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навы-ков работы на компьютере произошли сбои в работе машины,

что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.
Подлежит ли уголовной ответственности А.Иванов? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

Аспирант университета А.Петров, 26-ти лет, занимался исследова-тельской работой по компьютерной "вирусологии". Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые "сетевые чер-ви", проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников универ-ситета, расчеты бухгалтерии по зарплате, повреждены материалы науч-но-исследовательской работы, в том числе "пропали" две кандидатские и одна докторская диссертации.
Решите вопрос о правомерности действий А.Петрова. В чем заключается субъективная сторона преступлений в сфере компьютерной информации?

А.Сидоров и другие граждане Российской Федерации вступили в сговор на хищение денежных средств в крупных размерах, принадлежащих "City Bank of America", расположенного в г. Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 2012 г., используя электронную компьютерную систему телекоммуникационной связи "Интернет" и преодолев при этом несколько рубежей многоконтурной защиты от несанкционированного доступа с помощью персонального компьютера стандартной конфигурации из офиса предприятия, находящегося в г. Санкт-Петербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате этих операций было осуществлено не менее 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка на счета лиц, входящих в состав преступной группы, проживающих в шести странах: США, Великобритании, Израиле, Швейцарии, ФРГ, России.
Дайте уголовно-правовую оценку действиям А.Сидорова и других членов организованной группы.

Студент технического вуза А.Григорьев во время занятий по информатике подключился к сети "Интернет" и регулярно получал в течение семестра материалы разного содержания, в том числе и сексуального характера. В конце семестра в институт поступил запрос о работе в "Интернет" и пришел чек на оплату 105 часов пребывания в сети "Интернет".
Руководство института поставило вопрос о привлечении А.Григорьев к уголовной и гражданской ответственности.
Дайте правовую оценку действиям студента А.Григорьева.
Оператор ЭВМ одного из государственных учреждений А.Сергеев, ис-пользуя многочисленные дискеты с информацией, получаемые от сотрудни-ков других организаций, не всегда проверял их на наличие "вирусов", доверя-ясь заверениям поставщиков о том, что "вирусов" нет. В результате этого в компьютер А.Сергеева, а затем и в компьютерную сеть учреждения попал ком-бинированный вирус, что привело к утрате информации, содержащей госу-дарственную тайну, и поставило под угрозу срыва запуск одного из космичес-ких объектов.

Дайте юридический анализ действий А.Сергеева. Что следует понимать под тяжкими последствиями нарушении правил эксплуатации информационно-телекоммуникационных сетей?

А.Андреев осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Ситибанка». Рассылка представляла собой электронное письмо с сообщением о переводе 100 долларов США на личный счет клиента и содержала просьбу зайти в систему Интернет-бакинта «CitibankOnline» для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный А.Андреевым, и очень похожий на стартовый экран «CitibankOnline». Десять человек ввели номер кредитной карты и пин-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, А.Андреев совершил завладение денежными средствами Г.Никонова и Д.Корюшкина, находящимися в Ситибанке, в сумме 15 и 20 тысяч долларов соответственно.
Квалифицируйте содеянное А.Андреева.

Содержание отчета:

- указать наименование занятия и его номер,
- цель занятия (самостоятельно),
- отразить ход выполнения работы,
- ответить письменно на контрольные вопросы,
- сделать вывод по работе.

8.5. описание процедуры оценивания результатов обучения .

Формы оценочных мероприятий:

1. Входная/Выходная диагностика

Диагностика проводится по методике, описанной в п.8.2.

Входная диагностика проводится в формате входного тестирования, определяющего стартовый уровень владения знаниями, умениями и навыками до начала обучения по формируемым компетенциям, и в среднем по всем трем компетенциям.

Выходная диагностика проводится в форме выходного тестирования, определяющего финишный уровень владения знаниями, умениями и навыками, по итогам обучения, по формируемым компетенциям, и в среднем по всем трем компетенциям.

В целях анализа эффективности проведенного обучения, АНО ДПО “МЦК “Цель” справочно определяет прирост знаний, умений и навыков по окончанию обучающего процесса как разницу между результатами входной и выходной диагностики по компетенциям.

2. Самоконтроль-рефлексия

Самоконтроль-рефлексия – это самоконтроль слушателем результативности собственной работы по выполнению практических заданий по итогам каждого модуля.

Форма оценки реализуется посредством написания ответов на ряд открытых вопросов, нацеленных на выявление субъективной оценки обучающегося результатов собственной работы, и сдачи их провайдеру курса в установленной форме (заданная провайдером табличная форма с вопросами для самоконтроля) и в установленные сроки (в срок не позднее 2 дней с окончания модуля).

Результаты самоконтроля-рефлексии сдаются слушателем через личный кабинет в установленные сроки в АНО ДПО “МЦК “Цель” для проведения контроля. При выявлении непроведения самоконтроля-рефлексии слушателем в установленные сроки, оценка считается невыполненной, слушателю ставится отметка “не зачтено” при итоговой аттестации.

3. Зачет

Итоговая аттестация является обязательной. Под итоговой аттестацией понимается проверка соответствия результатов освоения настоящей программы заявленным целям и планируемым результатам обучения в виде формирования заявленных компетенций.

Вид итоговой аттестации - итоговый зачет по программе.

Слушатели, успешно прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации по курсу.

Слушатели, не прошедшие итоговую аттестацию, вправе пройти повторно итоговую аттестацию в сроки, определяемые АНО ДПО “МЦК “Цель”.

Слушателям, не прошедшим итоговую аттестацию, выдается справка о периоде обучения по образцу, установленному АНО ДПО “МЦК “Цель”.

Справочно по запросу слушателя выдается справка с описанием результатов образовательного прироста у слушателя:

- результаты выходной диагностики по компетенциям (в %),
- образовательный прирост по итогам обучения (в %).

Аттестационные испытания включают в себя:

- Результаты выходной диагностики

Испытание считается пройденным при наличии у слушателя оценок: не ниже “удовлетворительно”, “хорошо”, “отлично”.

- Результаты самоконтроля-рефлексии.

Испытание считается пройденным при своевременной сдаче отчета о проведении самоконтроля/рефлексии в установленные сроки по установленной форме.

- Выполнение итогового контрольного задания по эффективной работе с задачами по кибербезопасности.

Испытание считается пройденным при наличии у слушателя оценки не ниже “удовлетворительно” за выполнение итогового контрольного задания курса (оценка «удовлетворительно» ставится при наличии не менее 50% успешно выполненных задач итогового контрольного задания; и «оценка «неудовлетворительно» - при менее чем 50% успешно выполненных задач итогового контрольного задания).

Результаты прохождения аттестации.

- **отметка "не зачтено"** выставляется слушателю, показавшему неудовлетворительный результат выходной диагностики, или получившему неудовлетворительную оценку за итоговое контрольное задание, или не сдавшему отчеты о самоконтроле-рефлексии в установленной форме в установленные сроки.
- **отметку "зачтено"** заслуживает обучающийся, показавший как минимум удовлетворительный результат выходной диагностики, получивший удовлетворительную оценку за итоговое контрольное задание, сдавший все отчеты о самоконтроле-рефлексии в установленной форме в установленные сроки.

9.Организационно-педагогические условия реализации программы

9.1. Кадровое обеспечение программы

№ п/п	Фамилия, имя, отчество (при наличии)	Место основной работы и должность, ученая степень и ученое звание (при наличии)	Ссылки на веб-страницы с портфолио (при наличии)	Фото в формате jpeg	Отметка о полученном согласии на обработку персональных данных
1	**Шакин Дмитрий Николаевич**	Управление ФСТЭК России по Северо-Западному федеральному округу, заместитель руководителя Управления; кандидат военных наук, доцент.			+
2	Иванов Игорь Валентинович	Управление ФСТЭК России по Северо-Западному федеральному округу, начальник отдела			+
3	Фадеев Илья Игоревич	Управление ФСТЭК России по Северо-Западному федеральному округу, начальник отдела			+
4	Маркевич Андрей Мирославович	Управление ФСТЭК России по Северо-Западному федеральному округу, главный специалист-эксперт			+
5	Бредов Роман Павлович	Управление ФСТЭК России по Северо-Западному федеральному округу, консультант			+
6	Соловьев Николай Александрович	ОАО «МЗ «Арсенал», заместитель начальника управления безопасности	https://yadi.sk/i/FDY4IuDHDbMcpw		+
7	Левашов Михаил Васильевич	НИУ ВШЭ, Профессор	http://on.all-over-ip.ru/2018/hse/p/levashov-michael/?lang=ru		+
8	Рудаков Андрей Александрович	методист онлайн обучения			

9.2.Учебно-методическое обеспечение и информационное сопровождение

Учебно-методические материалы	
Методы, формы и технологии	Методические разработки, материалы курса, учебная литература
Основным дидактическим средством обучения в области информационной безопасности является учебно-практическая деятельность обучающихся. Приоритетными методами являются изучение и применение законодательства в области информационной безопасности, методов и средств защиты, практические работы, выполнение проектов: • дифференцированное обучение; • практические методы обучения; • проектные технологии; • технология применения средств ИКТ в предметном обучении; • технология организации самостоятельной работы; • элементы технологии компьютерного урока.	1. Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с. 2. Аверченков В.И., Рытов М.Ю. Служба защиты информации: организация и управление. Учебное пособие для вузов. – Брянск: БГТУ, 2005. – 186 с. 3. Арутюнов В.В. Основы информационной безопасности. Учебное пособие.- М.: МФЮА, 2008. 4. Бабурин А.В., Чайкина Е.А., Воробьева Е.И. Физические основы защиты информации от технической разведки. Учебное пособие. — Воронеж: Воронежский государственный технический университет, 2006. — 193 с. 5. Масалков Андрей Сергеевич «Особенности киберпреступлений. Инструменты нападения и защита информации», 2018 ДКМ Пресс 6. Диогенес Юрий, Озкайя Эрдаль «Кибербезопасность. Стратегии атак и обороны», 2020 ДМК Пресс 7. Шелупанов Александр Александрович, Смолина Анна Равильевна «Форензика. Теория и практика расследования киберпреступлений», 2019 Горячая линия-Телеком 8. Белоус Анатолий Иванович, Солодуха Виталий Александрович «Кибероружие и кибербезопасность. О сложных вещах простыми словами», 2020 Инфра-Инженерия 9. Бирюков Андрей Александрович «Информационная безопасность.

	Защита и нападение», 2017 ДМК Пресс

Информационное сопровождение	
Электронные образовательные ресурсы	**Электронные информационные ресурсы**
https://safe-surf.ru/	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty https://bdu.fstec.ru/threat https://rkn.gov.ru/personal-data/portal/ https://safe-surf.ru/ https://threats.kaspersky.com/ru/ https://www.anti-malware.ru/ http://cyberrus.com/

9.3.Материально-технические условия реализации программы

Вид занятий	**Наименование оборудования, программного обеспечения**
Вебинар	Браузер Google Chrome Сайт на базе WordPress и плагинами (программными модулями) Tutor LMS, Elementor, WebinarPress
Лабораторная/ практическая работа	Браузер Google Chrome Сайт на базе WordPress и плагинами (программными модулями) Tutor LMS, Elementor, WebinarPress
Рефлексия	Браузер Google Chrome Сайт на базе WordPress и плагинами (программными модулями) Tutor LMS, Elementor, WebinarPress

II. ПАСПОРТ КОМПЕТЕНЦИЙ (ПРИЛОЖЕНИЕ 2)

ПАСПОРТ КОМПЕТЕНЦИИ ПК-1

Дополнительная профессиональная образовательная программа повышения квалификации «Основы кибербезопасности для пользователей информационных систем»

АНО ДПО «МЦК «Цель»

1.	Наименование компетенции ПК1		Способность определять риски, угрозы и уязвимости информационных ресурсов, компьютерных сетей и данных.
2.	Указание типа компетенции	общекультурная/ универсальная	
		общепрофессиональная	
		профессиональная	+
		профессионально-специализированная	
3.	Определение, содержание и основные сущностные характеристики компетенции		Под компетенцией понимается способность анализировать, определять и формировать необходимые данные по информационным системам и системам их безопасности. Слушатель должен: **Знать**: - основные принципы организации технического, программного обеспечения защищенных информационных систем данных; - цели и задачи управления кибербезопасностью; - основные концепции, стандарты в том числе отраслевые и индустриальные, построения систем управления кибербезопасностью; - основные способы защиты информационных систем обработки данных, обеспечения безопасности и целостности данных; - методики оценки состояния КСЗИ автоматизированных информационных и телекоммуникационных систем; цели и задачи планирования функционирования КСЗИ **Уметь**: - разрабатывать модели угроз, карты рисков данных в системах и средств хранения, обработки и передачи информации, подлежащих защите; - вырабатывать обоснованные рекомендации по

		совершенствованию систем управления кибербезопасностью объектов и организаций, предотвращению рисков и возможных негативных последствий от атак; - оценивать состояние КСЗИ автоматизированных информационных и телекоммуникационных систем; оценивать показатели защищенности (эффективности) КСЗИ автоматизированных информационных и телекоммуникационных систем. **Владеть** навыками: - формулировать и решать задачи моделирования защищенных информационных систем, в том числе средств их защиты, средств и сетей хранения данных, обработки и передачи информации; - разработки и реализации политик безопасности на объектах информатизации, информационных ресурсов, на которых циркулирует информация ограниченного доступа и обрабатываются данные, подлежащие защите; - аудита и анализа состояния информационной безопасности на объектах информатизации и в организациях, использующих в своей деятельности информационные системы; -использования метода групповых экспертных оценок, других экспертных методов оценки эффективности КСЗИ автоматизированных информационных и телекоммуникационных систем обработки данных..	
4.	Дескриптор знаний, умений и навыков по уровням	Уровни сформированности компетенции обучающегося	Индикаторы
		Начальный уровень (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.)	**Знать**: структуру законодательства по информационной безопасности, защите информации **Уметь**: Выделять нужные требования и принципы кибербезопасности **Владеть** навыками: оформления простых требований по безопасности к информационным системам и ресурсам

		Базовый уровень (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределенности, сложности.)	**Знать**: конкретные требования законодательства по информационной безопасности в зависимости от состава информации и характеристик информационной системы **Уметь**: Определять угрозы системам и данным и требования по реализации защиты от них **Владеть** навыками: оформления технических требований по безопасности к информационным системам и данным с учетом полного перечня угроз
		Продвинутый (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)	**Знать**: конкретные требования законодательства по информационной безопасности, защите информации в зависимости от состава информации и данных, характеристик информационной системы, возможные пути обеспечения информационной безопасности. **Уметь**: Оформлять и проводить оценку актуальности перечня угроз, разрабатывать конкретные мероприятия по реализации защиты данных **Владеть** навыками:

			оформления технических требований по безопасности к информационным системам и оценку результатов их применения
		Профессиональный (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)	**Знать**: - конкретные требования законодательства по информационной безопасности, а также современные принципы и подходы в обеспечении информационной безопасности данных и для широкого круга информационных систем, современные и наиболее эффективные пути обеспечения информационной безопасности. **Уметь**: Формировать полный перечень мероприятий по защите информации, данных и внедрять их в информационные системы. **Владеть** навыками: Внедрения, применения конкретных организационных и технических мер информационной безопасности в информационных системах с предварительной оценкой их эффективности.

			Самостоятельно устанавливать, настраивать и проверять эффективность технических и программных средств защиты данных
5.	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции	Компетенции цифровой грамотности: - Применение навыков работы с персональным компьютером, текстовыми редакторами, электронными таблицами, браузерами, мультимедийным оборудованием; - Анализ данных - Управление данными.	
6.	Средства и технологии оценки	Выходное тестирование	

ПАСПОРТ КОМПЕТЕНЦИИ ПК-2

Дополнительная профессиональная образовательная программа повышения квалификации «Основы кибербезопасности для пользователей информационных систем»

АНО ДПО «МЦК «Цель»

1.	Наименование компетенции ПК2		Способность использовать существующие методы, стандарты и средства защиты данных.
2.	Указание типа компетенции	общекультурная/ универсальная	
		общепрофессиональная	
		профессиональная	+
		профессионально-специализированная	
3.	Определение, содержание и основные сущностные характеристики компетенции		Под компетенцией понимается способность оценивать полноту информации в ходе профессиональной деятельности, при необходимости восполнять и синтезировать недостающую информацию и работать в условиях неопределенности. Слушатель должен: **Знать**: - современные методы, применяемые при решении задач обеспечения информационной и кибербезопасности на государственных и частных предприятиях, основные используемые при этом подходы и инструментарий - основные способы защиты от атак на информационные ресурсы и системы - основы различных отраслевых подходов к решению поставленных задач. - знать комплексы международных и национальных стандартов, связанных с обеспечением КБ, а также соответствующие отраслевые стандарты. **Уметь**: - оценивать риски информационной безопасности, обрабатывать их и составлять отчеты о проведенном поиске уязвимостей. - проводить аудиты информационной безопасности. - применять различный инструментарий при защите информации и данных - использовать в работе комплексы международных и национальных стандартов, связанных с обеспечением КБ, а также соответствующие отраслевые стандарты. **Владеть** навыками: - построения и обеспечению процессов защиты информации, данных и информационных систем - использовать комплексный подход к построению и

		обеспечению процессов защиты информации, данных и информационных систем - анализа уязвимостей и рисков, возникающих при их наличии - использования стандартов информационной безопасности и нормативной базы по защите информации	
4.	Дескриптор знаний, умений и навыков по уровням	Уровни сформированности компетенции обучающегося	Индикаторы
		Начальный уровень (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.)	**Знать**: Принципы системы построения КБ **Уметь**: Выделять основные критические блоки в информационных системах обработки данных, формировать для них требования и принципы КБ **Владеть** навыками: Определения критических информационных структур и оформления простых требований по безопасности к ним и обрабатываемым в них данным
		Базовый уровень (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределенности, сложности.)	**Знать**: Принципы и технические особенности системы построения информационной безопасности информационных систем и объектов информатизации **Уметь**: Выделять основные критические блоки, их уязвимости и

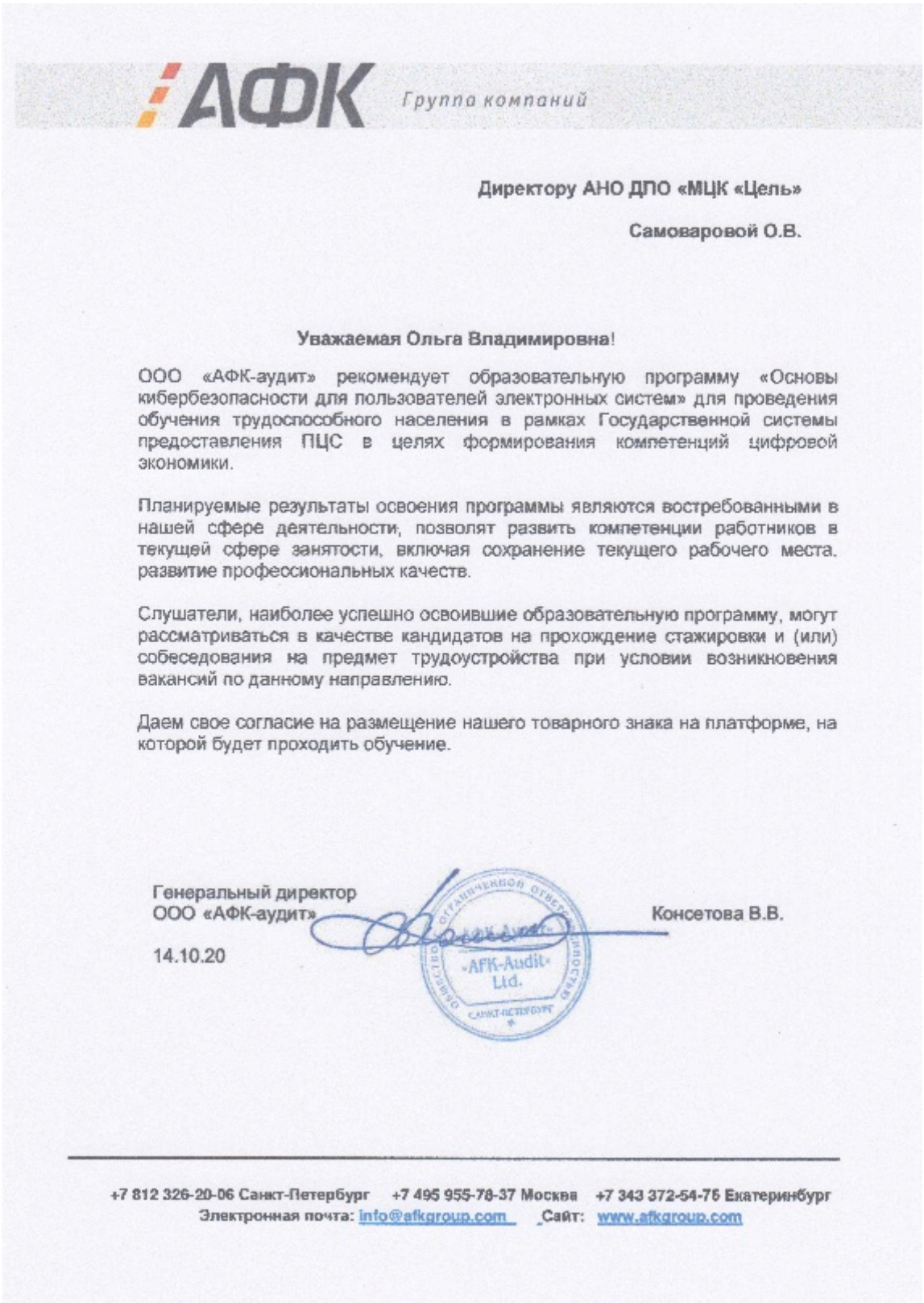
			определять риски в информационных системах, формировать для них требования и принципы КБ, формировать перечни рисков и возможные пути их предотвращения уничтожения, искажения и несанкционированного доступа к данным в них **Владеть** навыками: Определения критических информационных, критических узлов в них, оформления конкретных технических предложений по безопасности данных узлов
		Продвинутый (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)	**Знать**: Современные требования, средства и возможные методы реализации требований к построению систем кибербезопасности **Уметь**: Формировать требования и мероприятия по предотвращению рисков кибербезопасности в информационных системах, формировать и реализовывать перечни технических и организационных мероприятий по

			защите данных. **Владеть** навыками: оформления технических требований, составления технических заданий по обеспечению безопасности в информационных системах, проводить анализ их эффективности и развития.
		Профессиональный (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)	**Знать**: Современные требования, средства и их технические особенности; методы реализации требований к построению систем кибербезопасности и их ключевые особенности **Уметь**: Реализовывать и внедрять требования и мероприятия по предотвращению рисков информационной безопасности в информационных системах; Реализовывать технические и организационные мероприятия по защите информации, поддерживать их в актуальном состоянии, вести аналитику по возможным необходимым изменениям.

			Владеть навыками: оформления технических требований, составления технических заданий по обеспечению безопасности в информационных системах; по реализации требований, внедрению конкретных технических и программных средств, проводить анализ эффективности их применения, адаптировать и развивать в зависимости от развития систем и изменения внутренних и внешних факторов.
5.	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции	Компетенции цифровой грамотности: – Применение навыков работы с персональным компьютером, текстовыми редакторами, электронными таблицами, браузерами, мультимедийным оборудованием; – Анализ данных – Управление данными.	
6.	Средства и технологии оценки	Выходное тестирование	

VI. Иная информация о качестве и востребованности образовательной программы (результаты профессионально-общественной аккредитации образовательной программы, включение в системы рейтингования, призовые места по результатам проведения конкурсов образовательных программ и др.) (при наличии)

V. Рекомендаций к программе от работодателей:



АФК Группа компаний

Директору АНО ДПО «МЦК «Цель»

Самоваровой О.В.

Уважаемая Ольга Владимировна!

ООО «АФК-аудит» рекомендует образовательную программу «Основы кибербезопасности для пользователей электронных систем» для проведения обучения трудоспособного населения в рамках Государственной системы предоставления ПЦС в целях формирования компетенций цифровой экономики.

Планируемые результаты освоения программы являются востребованными в нашей сфере деятельности, позволят развить компетенции работников в текущей сфере занятости, включая сохранение текущего рабочего места, развитие профессиональных качеств.

Слушатели, наиболее успешно освоившие образовательную программу, могут рассматриваться в качестве кандидатов на прохождение стажировки и (или) собеседования на предмет трудоустройства при условии возникновения вакансий по данному направлению.

Даем свое согласие на размещение нашего товарного знака на платформе, на которой будет проходить обучение.

Генеральный директор
ООО «АФК-аудит» Консетова В.В.

14.10.20

«AFK-Audit» Ltd.

+7 812 326-20-06 Санкт-Петербург +7 495 955-78-37 Москва +7 343 372-54-75 Екатеринбург
Электронная почта: info@afkgroup.com Сайт: www.afkgroup.com

Общество с ограниченной ответственностью
«Медэксп ресс-сервис»
ООО «Медэкспресс-сервис»
191186, г. Санкт-Петербург, ул. Гороховая, д. 14/26
ИНН 7825101838, ОГРН 1037843100745
т: +7 (812)4930301
ф: +7 (812)314 39 59
e: info@myclinic.ru
w: www.myclinic.ru

Директору АНО ДПО «МЦК«Цель»

Самоваровой О.В.

Уважаемая Ольга Владимировна!

ООО «Медэкспресс-сервис» рекомендует образовательную программу «Основы кибербезопасности для пользователей электронных систем» для проведения обучения трудоспособного населения в рамках Государственной системы предоставления ПЦС в целях формирования компетенций цифровой экономики.

Планируемые результаты освоения программы являются востребованными в нашей сфере деятельности, позволят развить компетенции работников в текущей сфере занятости, включая сохранение текущего рабочего места, развитие профессиональных качеств.

Слушатели, наиболее успешно освоившие образовательную программу, могут рассматриваться в качестве кандидатов на прохождение стажировки и (или) собеседования на предмет трудоустройства при условии возникновения вакансий по данному направлению.

Даем свое согласие на размещение нашего товарного знака на платформе, на которой будет проходить обучение.

Генеральный директор
ООО «Медэкспресс-сервис» А.В. Шумилова

12.10.2020

VI. Указание на возможные сценарии профессиональной траектории граждан по итогам освоения образовательной программы (в соответствии с приложением)

Сценарии профессиональной траектории граждан

Цели получения ПЦС	
текущий статус	**цель**
Развитие компетенций в текущей сфере занятости	
работающий по найму в организации, на предприятии	сохранение текущего рабочего места
работающий по найму в организации, на предприятии	развитие профессиональных качеств
работающий по найму в организации, на предприятии	повышение заработной платы
работающий по найму в организации, на предприятии	смена работы без изменения сферы профессиональной деятельности
временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.)	повышение уровня дохода
временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.)	сохранение и развитие квалификации
Переход в новую сферу занятости	
освоение смежных профессиональных областей	повышение уровня дохода, расширение профессиональной деятельности

Директор АНО ДПО «МЦК Цель» О.В. Самоварова

14.10.2020