

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«Национальный исследовательский ядерный университет «МИФИ»

**Димитровградский инженерно-технологический институт –**  
филиал федерального государственного автономного образовательного учреждения высшего образования  
«Национальный исследовательский ядерный университет «МИФИ»  
(ДИТИ НИЯУ МИФИ)

**СОГЛАСОВАНО**

От работодателя:

*Зам. директора ООО «МС Групп»*  
должность, название предприятия  
*А.Н. Наскальнико*

« 15 » апреля 2012 г.

М.П.



**УТВЕРЖДАЮ**

Руководитель ДИТИ НИЯУ МИФИ  
должность и название образовательного учреждения

*И.И. Бегина*  
И.И. Бегина

« 12 » мая 2012 г.

М.П.



## **РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА**

### **МДК.11.02 ПРОГРАММИРОВАНИЕ WEB – ПРИЛОЖЕНИЙ**

по программе подготовки специалистов среднего звена специальности  
09.02.07 Информационные системы и программирование

Форма обучения: очная

Учебный цикл: профессиональный

Составитель: А.А. Иванов, преподаватель техникума ДИТИ НИЯУ МИФИ

Димитровград

## **СОДЕРЖАНИЕ**

<b>1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>стр. 3</b>
<b>2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>5</b>
<b>3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ</b>	<b>13</b>
<b>4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>15</b>

# **1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

## **1.1. Область применения программы**

Рабочая программа МДК.11.02 Программирование Web – приложений программы подготовки специалистов среднего звена (ППССЗ), и составлена в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и соответствующих профессиональных компетенций (ПК). Квалификация: Программист.

Программа профессионального модуля ПМ.11 разработана в рамках выполнения работ по внесению изменений (дополнений) в образовательную программу по специальности среднего профессионального 09.02.07 Информационные системы и программирование, в целях внедрения международных стандартов подготовки высококвалифицированных рабочих кадров с учетом передового международного опыта движения WorldSkills International (WSI), на основании компетенции «Корпоративная защита от внутренних угроз информационной безопасности» с учетом профессионального стандарта Техник по защите информации» («Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N522н) и в соответствии со стандартами Союза «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы (Ворлдскиллс)».

## **1.2. Место дисциплины в структуре ППССЗ**

МДК.11.02 Программирование Web – приложений ПМ.11 по специальности 09.02.07 Информационные системы и программирование относится к обязательной части ППССЗ и принадлежит к циклу дисциплин профессионального модуля и является базой для освоения практик.

## **1.3. Цель и планируемые результаты освоения дисциплины:**

В результате изучения МДК профессионального модуля студент должен освоить основной вид деятельности (ВПД и соответствующие ему профессиональные и общие компетенции:

### **Общие компетенции:**

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

### **Перечень профессиональных компетенций:**

ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации

ПК 2.2 Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами

ПК 2.3 Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации

ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа

ПК 2.5 Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств

ПК 2.6 Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

ДПК.1 Способность разрабатывать модели компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек - электронно- вычислительная машина".

### **В результате освоения профессионального модуля студент должен согласно ФГОС СПО:**

В результате освоения профессионального модуля студент должен:

<b>Иметь практический опыт</b>	<ul style="list-style-type: none"><li>– установки, настройки программных средств защиты информации в автоматизированной системе;</li><li>– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;</li><li>– тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;</li><li>– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;</li><li>– применения электронной подписи, симметричных и</li></ul>
--------------------------------	--

	<p>асимметричных криптографических алгоритмов и средств шифрования данных;</p> <ul style="list-style-type: none"> <li>– учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;</li> <li>– работы с подсистемами регистрации событий;</li> <li>– выявления событий и инцидентов безопасности в автоматизированной системе.</li> </ul>
<b>уметь</b>	<ul style="list-style-type: none"> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</li> <li>– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;</li> <li>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</li> <li>– применять программные и программно-аппаратные средства для защиты информации в базах данных;</li> <li>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</li> <li>– применять математический аппарат для выполнения криптографических преобразований;</li> <li>– использовать типовые программные криптографические средства, в том числе электронную подпись;</li> <li>– применять средства гарантированного уничтожения информации;</li> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</li> <li>– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак</li> </ul>
<b>знать</b>	<ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</li> <li>– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;</li> <li>– основные понятия криптографии и типовых криптографических методов и средств защиты информации;</li> <li>– особенности и способы применения программных и программно-аппаратных средств гарантированного</li> </ul>

	<p>уничтожения информации;</p> <ul style="list-style-type: none"> <li>– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.</li> </ul>
--	---

**В результате освоения профессионального модуля студент должен согласно компетенции Ворлдскиллс Россия «Корпоративная защита от внутренних угроз информационной безопасности»:**

Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз:

Специалист должен знать и понимать:

- Технологии работы с политиками информационной безопасности;
- Создание новых политик, модификация существующих;
- Общие принципы при работе интерфейсом системы защиты корпоративной информации;
- Объекты защиты, персоны;
- Ключевые технологии анализа трафика;
- Типовые протоколы и потоки данных в корпоративной среде, такими как:
- корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4)
- веб-почта;
- Интернет-ресурсы: сайты, блоги, форумы и т.д. (протоколы HTTP, HTTPS);
- социальные сети;
- интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP;
- принтеры: печать файлов на локальных и сетевых принтерах;
- любые съемные носители и устройства;
- Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек;
- Типы угроз информационной безопасности, типы инцидентов,
- Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;
- Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации;
- Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;
- Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации;
- Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки;
- Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе;
- Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов;

- Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;

Специалист должен уметь:

- Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты;

- Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты;

- Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии;

- Работа со сводками, виджетами, сводками;

- Работа с персонами;

- Работа с объектами защиты;

- Провести имитацию процесса утечки конфиденциальной информации в системе;

- Создать непротиворечивые политики, соответствующие нормативной базе и законодательству;

- Задokumentировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации.

- Работа с категориями и терминами;

- Использование регулярных выражений;

- Использование морфологического поиска;

- Работа с графическими объектами;

- Работа с выгрузками и баз данных;

- Работа с печатями и бланками;

- Работа с файловыми типами;

- Эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;

Технологии анализа и защиты сетевого трафика

Специалист должен знать и понимать:

- Организационно-технические и правовые основы использования электронного документооборота в информационных системах;

- Структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPNсетей. Основные типы классификаций VPN-сетей

- Технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений;

- Ключевые компоненты VPN-сетей;

- Особенности VPN-сети и механизмы их управления;

- Современные криптографические алгоритмы. Криптопровайдеры, криптографические интерфейсы и библиотеки;

- Архитектура, основные компоненты РКІ их функции и взаимодействие;

- Жизненный цикл ключей и сертификатов;

- Электронный сертификат ключей ЭЦП. Формирование, подписание и использование сертификатов;

- Защита видео и конференций приложений;
- Назначение и основные сценарии применения IDS-технологий;
- Архитектуру и особенности внедрения IDS-технологий;
- Распространённые вектора атак и уязвимости современных корпоративных информационных систем.

Специалист должен уметь:

- Осуществлять развёртывание и администрирование VPN-сетью (добавление, удаление, изменение объектов сети, настройка параметров работы, контроль работоспособности и др.). Обновление ПО, установленного на узлах защищенной сети.

• Работать и удостоверяющей и ключевой информацией. Формирование и управление ключевой структурой сети.

Издание и управление сертификатами пользователей.

- Настраивать защиту сегментов IP-сетей, координация работы узлов защищенной сети. Защиты трафика, передаваемого по открытым каналам связи;

• Осуществлять защиту оконечных рабочих мест; Контроль пользовательских приложений;

- Реализовывать межсетевое взаимодействие и туннелирование;

• Компрометация рабочих мест;

• Обеспечение меж сетевого экранирования и криптографической защиты информации;

- ПО для электронного документооборота в VPN-системах

• Защита систем, обеспечивающих поддержку процессов информационного взаимодействия

• Устанавливать и конфигурировать современные IDS-системы корпоративного класса в сети предприятия;

- Выполнять настройку и проверку работоспособности;

• Проводить детектирование атак (потенциальных угроз) в ручном, автоматизированном и автоматическом режиме;

- Проводить правильную классификацию уровня угрозы инцидента;

• Использовать базы контентной фильтрации;

• Использовать дополнительные модули анализа

информационных потоков, если это продиктовано особенностями условий ведения бизнеса;

Технологии агентского мониторинга

Специалист должен знать и понимать:

- Функции агентского мониторинга;

• Общие настройки системы агентского мониторинга;

• Соединение с LDAP-сервером и синхронизация с Active Directory;

• Политики агентского мониторинга, особенности их настройки;

• Особенности настроек событий агентского мониторинга;

• Механизмы диагностики агента, подходы к защите агента.

Специалист должен уметь:

- Установка и настройка агентского мониторинга;

• Создание политик защиты на агентах;

- Работа в консоли управления агентом;
- Фильтрация событий;
- Настройка совместных событий агентского и сетевого мониторинга;
- Работа с носителями и устройствами;
- Работа с файлами;
- Контроль приложений;
- Исключение из событий перехвата.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Количество часов
<b>Максимальная учебная нагрузка (всего)</b>	<b>93</b>
<b>Обязательная аудиторная учебная нагрузка (всего) , в т.ч.:</b>	<b>93</b>
– курсовое проектирование	–
– теоретические занятия	-
– практические занятия	93
<b>Учебная практика:</b>	
<b>Производственная практика:</b>	

## 2.2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ МДК

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Уровень освоения	Объем часов	Осваиваемые элементы компетенций	
<i>МДК.02.03 Программирование и защита Web - приложений</i>					
<b>Раздел 1. Введение в Web-конструирование</b>			32		
Тема 1.1. Глобальные компьютерные сети.	Содержание учебного материала		6		
	Основные понятия и принципы функционирования.	2	2		
	Каталоги ресурсов	2	2		
	Поисковые системы	2	2		
	Тематика практических занятий и лабораторных работ				2
	Практическое занятие № 1. Подбор ресурсов Internet на заданную тематику				2
	Контрольные работы не предусмотрены				
Тема 1.2 Язык гипертекстовой разметки страниц HTML:;	Содержание учебного материала		4	<i>ОК 01-10 ПК 2.1-2.6 ДПК.1.</i>	
	Общая структура документа. Абзацы, цвета, ссылки. Списки. Графика (графические форматы, графический объект как ссылка). Таблицы и Фреймы	2	2		
	Общие подходы к дизайну сайта. Разработка макета страницы. Формы	2	2		
	Тематика практических занятий и лабораторных работ				8
	Практическое занятие № 2. Язык гипертекстовой разметки страниц HTML: общая структура документа, абзацы, цвета, ссылки; списки, графика (графические форматы, графический объект как ссылка) (4 часа)				4
	Практическое занятие № 3. Макет страницы.				4
	Контрольные работы не предусмотрены				
	Тема 1.3. Использование стиля при оформлении сайта.	Содержание учебного материала			4
Спецификации CSS1, CSS2		2	4		
Тематика практических занятий и лабораторных работ			4		
Практическое занятие № 4. Использование стиля при оформлении сайта.			4		

	Спецификации CSS1, CSS2			
	Контрольные работы не предусмотрены			
Тема 1.4. Хостинг. Бесплатный хостинг. FTP.	Содержание учебного материала		4	ОК 01-10 ПК 2.1-2.6 ДПК.1.
	Размещение Интернет-ресурса на сервере провайдера.	2	2	
	Регистрация Интернет-ресурса в каталогах и поисковых системах	2	2	
	Тематика практических занятий и лабораторных работ не предусмотрены			
	Контрольные работы не предусмотрены			
<b>Раздел 2. Программирование на JavaScript</b>			86	
Тема 2.1. DHTML	Содержание учебного материала		10	ОК 01-10 ПК 2.1-2.6 ДПК.1.
	Преимущества и ограничения программ, работающих на стороне клиента;	2	2	
	Язык JavaScript: основы синтаксиса;	2	2	
	Объектная модель HTML страницы;	2	2	
	Событийная модель DHTML: связывание событий с кодом, всплытие событий, объект Event;	2	2	
	Применение DHTML: <ul style="list-style-type: none"> <li>• программное изменение содержания документа;</li> <li>• программное изменение формата документа;</li> <li>• программное изменение положения элементов</li> </ul>	2	2	
	Тематика практических занятий и лабораторных работ		10	
	Практическое занятие № 5. Программирование на JavaScript		4	
	Практическое занятие № 6. XML. MathML		6	
	Контрольные работы не предусмотрены			
Тема 2.2. Язык PHP.	Содержание учебного материала		12	
	Введение в программирование на стороне сервера на примере PHP. Принцип работы.	2	2	
	Синтаксис языка программирования PHP.	2	2	
	Переменные. Константы. Операторы в PHP. Циклы. Массивы. Работа со строками.	2	2	
	Функции в PHP. Встроенные функции.	2	2	
	Связь PHP и HTML	2	4	
	Тематика практических занятий и лабораторных работ		14	
	Практическое занятие № 7. Программирование на PHP. PHP & MySQL		10	

	Практическое занятие № 8. Работа с датой и временем в PHP.		4	
	Контрольные работы не предусмотрены			
Тема 2.3. База данных в MySQL.	Содержание учебного материала		4	ОК 01-10 ПК 2.1-2.6 ДПК.1.
	Принципы хранения информации в базах данных MySQL.	2	2	
	Архитектура базы данных MySQL (таблицы, связи, триггеры).	2	2	
	Тематика практических занятий и лабораторных работ		4	
	Практическое занятие № 9 Проектирование баз данных. Нормализация таблиц.		2	
	Практическое занятие № 10 Варианты хранения информации в сети Internet.		2	
	Контрольные работы не предусмотрены			
Тема 2.4. Взаимодействие скриптов на языке PHP и базы данных MySQL.	Содержание учебного материала		6	ОК 01-10 ПК 2.1-2.6 ДПК.1.
	Вывод данных на PHP-страницу, попавших в выборку по SQL запросу.	2	4	
	Передача параметров в запрос	2	2	
	Тематика практических занятий и лабораторных работ		4	
	Практическое занятие № 11 Подключение к базе данных из PHP файла.		4	
	Контрольные работы не предусмотрены			
Тема 2.5. Решение прикладных задач.	Содержание учебного материала		8	
	Принципы проектирования страниц. Разделение информации по таблицам в базе данных.	2	2	
	Вывод группы данных, сортировка данных.	2	2	
	Постраничный вывод данных.	2	2	
	Разработка проекта	2	2	
	Тематика практических занятий и лабораторных работ		12	
	Практическое занятие № 12 Разработка проекта.		10	
	Практическое занятие № 13. Создание HTML-страниц средствами PHP.		2	
	Контрольные работы не предусмотрены			
<b>Раздел 3. Технологии обеспечения безопасности веб-приложений</b>			<b>54</b>	
Тема 3.1. Основные принципы построения безопасных сайтов. Понятие безопасности приложений и классификация опасностей	Содержание учебного материала		4	ОК 01-10 ПК 2.1-2.6 ДПК.1.
	Введение в безопасность Web приложений. Планирование системы безопасности Web приложений.	2	2	
	Введение в аутентификации Web клиентов.	2	2	
	Тематика практических занятий и лабораторных работ		4	
	Практическое занятие № 14 Сбор информации о web-приложении		2	

	Практическое занятие № 15 Использование STRIDE модели для определения возможных угроз.		2		
	Контрольные работы не предусмотрены				
Тема 3.2. Источники угроз информационной безопасности и меры по их предотвращению	Содержание учебного материала		4		
	Классы основных сетевых атак. Угрозы.	2	2		
	Создание защищённых Web приложений.	2	2		
	Тематика практических занятий и лабораторных работ			4	
	Практическое занятие № 16. Тестирование защищённости механизма управления доступом и сессиями			4	
	Контрольные работы не предусмотрены				
Тема 3.3. Регламенты и методы разработки безопасных веб-приложений	Содержание учебного материала		4		
	Создание защищённых Web приложений при помощи ASP.NET	2	2		
	Обеспечение конфиденциальности и целостности данных при работе с Web приложениями	2	2		
	Тематика практических занятий и лабораторных работ			4	
	Практическое занятие №17 Поиск уязвимостей к атакам XSS			4	
	Контрольные работы не предусмотрены				
Тема 3.4 Безопасная аутентификация и авторизация	Содержание учебного материала		4		
	Конфигурирование прав доступа к серверу	2	2		
	Аутентификация и права доступа	2	2		
	Тематика практических занятий и лабораторных работ			4	
	Практическое занятие № 18 Тестирование на устойчивость к атакам отказа в обслуживании			4	
	Контрольные работы не предусмотрены				
ВСЕГО за 7-й семестр			150		
Тема 3.5 Повышение привилегий и общая отказоустойчивость системы	Содержание учебного материала		4		
	Проверка пользовательского ввода	2	2		
	Обеспечение конфиденциальности и целостности данных	2	2		
	Тематика практических занятий и лабораторных работ			0	
	Контрольные работы не предусмотрены				
Тема 3.6 Проверка корректности данных, вводимых пользователем.	Содержание учебного материала		4		
	Система безопасности Microsoft SQL Server	2	2		
				ОК 01-10 ПК 2.1-2.6 ДПК..1.	
				ОК 01-10 ПК 2.1-2.6 ДПК..1.	

Публикация изображений и файлов. Методы шифрования. SQL- инъекции. XSS-инъекции	Тестирование безопасности Web приложений	2	2
	Тематика практических занятий и лабораторных работ		8
	Практическое занятие № 19. Поиск уязвимостей к атакам SQL-injection		4
	Практическое занятие № 20. Поиск уязвимостей к атакам XSS-injection		4
	Контрольные работы не предусмотрены		
Самостоятельная работа обучающихся	2.1.Подготовка к практическим занятиям 2.2.Подготовка мультимедийной презентации «Планирование системы безопасности Web приложений». 2.3.Подготовка реферата по теме: Классы основных сетевых атак. Угрозы.		6
ВСЕГО за 8-й семестр			22
Консультация			2
Дифференцированный зачёт			2

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

#### 3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия Лаборатории Программных и программно-аппаратных средств защиты информации.

Оборудование:

- рабочее место преподавателя, оборудованное персональным компьютером с лицензионным или свободным программным обеспечением, соответствующим разделам программы, подключенным к сети Internet и средствами вывода звуковой информации;
- посадочные места по количеству обучающихся;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения вторжений;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства выявления уязвимостей в АС и СВТ;
- программные средства криптографической защиты информации;
- программные средства защиты среды виртуализации.

Технические средства обучения:

- компьютеры INTEL CELERON с лицензионным программным обеспечением;
- мультимедиапроектор Acer XI230;
- экран PAPER LUMA 127\*16;
- периферийные устройства:
- принтер SAMSUNG ML 1210;
- сканер EPSON 1210

#### 3.2. Информационное обеспечение обучения

##### Электронный ресурс

1. Мэтиз Эрик. Изучаем Python. Программирование игр, визуализация данных, веб-приложения [Электронный ресурс]: Мэтиз Эрик. - 2-е изд. - СПб.: Питер, 2017. — 496 с.: ил. <http://ibooks.ru/>

2. Хортон, А. Разработка веб-приложений в ReactJS [Электронный ресурс] / А. Хортон, Р. Вайс ; пер. с англ. Рагимова Р.Н. — М.: ДМК Пресс, 2016. — 254 с. <https://e.lanbook.com/>

3. Заяц, А. М. Проектирование и разработка WEB-приложений. Введение в frontend и backend разработку на JavaScript и node.js [Электронный ресурс]: учебное пособие / А. М. Заяц, Н. П. Васильев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 120 с. <https://e.lanbook.com/>

4. Гумерова, Л. З. Основы web-программирования [Электронный ресурс]: учебное пособие / Л. З. Гумерова. — Красноярск : Научно-инновационный центр, 2019. — 104 с. <http://www.iprbookshop.ru/>

5. Фролов, А. Б. Основы web-дизайна. Разработка, создание и сопровождение web-сайтов [Электронный ресурс]: учебное пособие для СПО / А. Б. Фролов, И. А. Нагаева, И. А. Кузнецов. — Саратов : Профобразование, 2020. — 244 с. <http://www.iprbookshop.ru/>

#### 4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Формы и методы текущего контроля успеваемости студентов, промежуточной аттестации по профессиональному модулю доводятся до сведения студентов до начала обучения по образовательной программе среднего профессионального образования – программе подготовки специалистов среднего звена.

Текущий контроль успеваемости студентов проводится в процессе обучения и осуществляется в виде оценки выполнения и защиты практических работ, контрольных работ, устных и письменных опросов, оценки выполнения самостоятельной работы студентов, оценки выполнения курсового проекта.

Обучение по профессиональному модулю завершается промежуточной аттестацией в форме экзамена (квалификационного), который проводит экзаменационная комиссия. В ее состав входят представители работодателя.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

<p>ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.</p>	<p>Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.</p>	<p>Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.</p>	<p>Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.</p>	<p>Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<ul style="list-style-type: none"> <li>– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;</li> <li>- адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач</li> </ul>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p> <p>Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам</p> <p>Экзамен квалификационный</p>
ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	<ul style="list-style-type: none"> <li>- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач</li> </ul>	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	<ul style="list-style-type: none"> <li>- демонстрация ответственности за принятые решения</li> <li>- обоснованность самоанализа и коррекция результатов собственной работы;</li> </ul>	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	<ul style="list-style-type: none"> <li>- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;</li> <li>- обоснованность анализа работы членов команды (подчиненных)</li> </ul>	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	<ul style="list-style-type: none"> <li>- грамотность устной и письменной речи,</li> <li>- ясность формулирования и изложения мыслей</li> </ul>	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	<ul style="list-style-type: none"> <li>- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,</li> </ul>	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно	<ul style="list-style-type: none"> <li>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;</li> </ul>	

действовать в чрезвычайных ситуациях.	- знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	