Волгоградский государственный университет

УТВЕРЖДАЮ

Директор института
дополнительного образования

А.А. Суслов

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

РАБОЧАЯ ПРОГРАММА

дополнительной образовательной программы

повышения квалификации

 **«Цифровые технологии безопасной среды и обработки, защиты персональных данных»**

учебной дисциплины

«Информационные технологии»

наименование дисциплины, модуля

09.03.02 Информационные системы и технологии

код, наименование

Руководитель программы

Ассистент кафедры

информационных систем

и компьютерного моделирования Корнаухова М.А.

Волгоград – 2020

**Структура рабочей программы:**

**Раздел 1.** Общая характеристика программы

* 1. Цель реализации программы
	2. Характеристика новой квалификации. Виды профессиональной деятельности, трудовых функций и (или) уровней квалификации.
	3. Планируемые результаты обучения
	4. Требования к уровню подготовки поступающего на обучение.

**Раздел 2.** Содержание программы

2.1.Учебно-тематический план

2.3. Лекции (темы), перечень семинарских (лабораторных, практических) занятий

2.4. Оценка качества освоения программы

Раздел 3. Организационно-педагогические условия реализации программы

##### 3.1. Кадровые условия

3.2. Условия функционирования электронной информационно-образовательной среды (при реализации программ с использованием дистанционных образовательных технологий)

3.3. Виды самостоятельной работы слушателей (СРС)

3.4. Требования и методические рекомендации по подготовке к семинарским занятиям

**Раздел 4.** Материально-технические требования программы

**Раздел 5.** Информационно-методические требования программы

5.1. Рекомендуемая литература

5.1.1. Основная литература

5.1.2. Дополнительная литература

5.1.3. Электронная информационно-образовательная среда

**Срок обучения:** 72 часа.

**Режим занятий:** не более 6 часов в день.

**Категория слушателей**: допускаются лица, имеющие или получающие среднее профессиональное и (или) высшее образование.

**Форма обучения:** очно-заочная с использованием дистанционных образовательных технологий и электронного обучения.

**РАЗДЕЛ 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

* 1. ***Цель реализации программы***

**Цель преподавания программы** «Цифровые технологии безопасной среды и обработки, защиты персональных данных» целью обучения является обучение основам цифровой грамотности и защиты персональных данных; обеспечение содействия жителям в освоении ключевых компетенций цифровой экономики; увеличение числа граждан, обладающих цифровыми навыками.

Данная образовательная программа разработана в соответствии с:

- требованиями Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. № 499;

- приказу Минобрнауки России от 29 марта 2019 № 178;

- глобальной технологической повестки (прогноз научно-технического развития Российской Федерации до 2030 года);

- потребностям реального сектора экономики;

- квалификационными требованиями, указанных в квалификационных справочниках по соответствующим должностям, профессиям и специальностям;

 - интересами различных целевых аудиторий, в том числе граждан предпенсионного и пенсионного возраста, трудовых мигрантов, инвалидов, осуществляющих свою деятельность на территории Российской Федерации.

* 1. ***Характеристика новой квалификации. Виды профессиональной деятельности, трудовых функций и (или) уровней квалификации.***

Целью реализации программы повышения квалификации «Цифровые технологии безопасной среды и обработки, защиты персональных данных»является совершенствование знаний в области современных информационных технологий и защиты персональных данных.

* 1. ***Планируемые результаты обучения***

В результате изучения программы «Цифровые технологии безопасной среды и обработки, защиты персональных данных» слушатель должен **овладеть понятиями:**

* об информационной безопасности и законодательстве в сфере защиты личной информации и ответственности граждан по предоставлению личной информации;
* основные особенности современного состояния организационно-правового обеспечения защиты персональных данных в информационных системах персональных данных;
* проблемы охраны конфиденциальности персональных данных лиц в Российской Федерации;
* требования и рекомендации по обеспечению безопасности информации в информационных системах персональных данных;
* о глобальной информационной сети Интернет, программах- браузерах и электронной почты, безопасность в сети Интернет;о средствах сетевых коммуникаций для социального взаимодействия в сети Интернет и об основах сетевого этикета.
* о средствах сетевой консультационной поддержки пользователей электронных государственных услуг;
* о составе электронных региональных и муниципальных государственных услуг населению и их нормативном правовом статусе;
* об облачных технологиях и безопасном доступе к личному кабинету пользователя.
* создание безопасной интернет-страницы, принципы создания Landing Page, анатомия лендинга: функциональные элементы

***Требования к уровню подготовки поступающего на обучение***

Наличие или получение высшего и/или среднего профессионального образования.

### **РАЗДЕЛ 2. СОДЕРЖАНИЕ ПРОГРАММЫ**

### ***2.1. Учебно-тематический план***

| № | Наименование разделов и тем | Общая трудоемкость, часов | Всего, часов | в т.ч. | Самостоятельная работа (СРС), часов | Формы контроля |
| --- | --- | --- | --- | --- | --- | --- |
| лекции | Семинарские занятия  |
| **I. Модуль 1. Создание безопасной среды и защита персональных данных** | **8** | **6** | **2** | **4** | **2** | зачет |
| **1.1** | **Компьютерная безопасность.** Основы информационной безопасности и персонифицированной опрос работы с коммуникационными сервисами. Спам и кибермошенничество. Защита от спама. Защита информации. | 4 | 3 | 1 | 2 | 1 | опрос |
| **1.2** | **Компьютерные вирусы.**Антивирусная защита. Антивирусные программы. | 4 | 3 | 1 | 2 | 1 | опрос |
| **II. Модуль 2. Обеспечение и оценка эффективности системы защиты информационных систем персональных данных.** | **20** | **14** | **3** | **11** | **6** | зачет |
| **2.1** | **Модель угроз для информационных систем персональных данных**. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Модель злоумышленника информационных систем персональных данных. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.. | 7 | 5 | 1 | 4 | 2 | опрос |
| **2.2.** | **Организация и обеспечение режимов защиты персональных данных.** Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий. | 7 | 5 | 1 | 4 | 2 | опрос |
| **2.3** | **Оценка эффективности систем защиты информационных систем персональных данных.** Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации. Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства контроля. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган. | 6 | 4 | 1 | 3 | 2 | опрос |
| **III. Модуль 3. Жизнь в информационном обществе.** | **16** | **13** | **3** | **10** | **3** | зачет |
| 3.1 | Новостные сайты. Сайты газет и журналов. Корпоративные сайты. | 5 | 4 | 1 | 3 | 1 | опрос |
| 3.2 | Использование возможностей Интернета в различных сферах жизни (образование / обучение, работа, здоровье, путешествия). Регистрация на сайтах. | 5 | 4 | 1 | 3 | 1 | опрос |
| 3.3 | Приобретение товаров и услуг через Интернет. Обзор Интернет-магазинов. Оплата услуг. Основные меры предосторожности. Общение в социальных сетях, форумы | 6 | 5 | 1 | 4 | 1 | опрос |
| **IV. Модуль 4. Создание безопасной интернет-страницы. Cоздание Landing Page.** | **26** | **19** | **6** | **13** | **7** | зачет |
| 4.1 | Понимание принципов Landing Page. | 5 | 3 | 1 | 2 | 2 | опрос |
| 4.2 | Этапы создания Landing Page | 5 | 4 | 1 | 3 | 1 | опрос |
| 4.3 | Анатомия лендинга: функциональные элементы | 5 | 4 | 1 | 3 | 1 | опрос |
| 4.4 | Принципы дизайна лендинга | 4 | 3 | 1 | 2 | 1 |  |
| 4.5 | Описание конструкторов | 4 | 3 | 1 | 2 | 1 |  |
| 4.6 | Как увеличить эффективность лендинга | 3 | 2 | 1 | 1 | 1 |  |
| Итоговая аттестация | **2** | **2** | **-** | **2** | - | **зачет** |
|  |  **ВСЕГО:** | **72** | **54** | **14** | **40** | **18** |  |

***2.2. Содержание разделов***

***Модуль 1. Создание безопасной среды и защита персональных данных***

Блок содержит темы о способах обеспечения информационной безопасности при работе на компьютере, в том числе о мерах предосторожности при работе в сети Интернет.

1.1. Компьютерная безопасность. Основы информационной безопасности и персонифицированной работы с коммуникационными сервисами. Спам и кибермошенничество. Защита от спама.

1.2. Антивирусная защита. Обзор наиболее популярного антивирусного программного обеспечения. Классификация компьютерных угроз. Вирусы, черви, трояны. Клавиатурный шпион. Рекламные системы.

***Модуль 2. Обеспечение и оценка эффективности системы защиты информационных систем персональных данных.***

2.1. Модель угроз для информационных систем персональных данных. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Модель злоумышленника информационных систем персональных данных. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.

2.2. Организация и обеспечение режимов защиты персональных данных. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.

2.3. Оценка эффективности систем защиты информационных систем персональных данных. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации. Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства контроля. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

***Блок 3. Жизнь в информационном обществе***

Блок посвящен описанию современных тенденций в мире информационных технологий в части использования гражданами возможностей компьютерных устройств и Интернета в различных сферах жизни.

3.1. Новостные сайты. Сайты газет и журналов. Корпоративные сайты. Обзор. Принцип работы.

3.2. Использование возможностей Интернета в различных сферах жизни (образование/обучение, работа, здоровье, путешествия). Регистрация на сайтах.

Путешествия (бронирование билетов и гостиниц через Интернет). Образование. Работа. Здоровье (электронная регистратура).

3.3. Основные аспекты приобретения товаров и услуг через Интернет. Обзор Интернет-магазинов, оплата товаров и услуг через Интернет и с использованием банковских карт. Основы безопасной работы при оплате товаров и услуг. Безопасность при регистрации в сетевом сервисе. Общение в социальных сетях. Форумы. Средства общения (в онлайн конференциях, чатах, форумах и в социальных сетях «Одноклассники», «Твиттер», «Вконтакте»). Поиск людей. Отправка сообщений.

***Модуль 4. Создание безопасной интернет-страницы. Cоздание Landing Page.***

Понимание принципов Landing Page. Этапы создания Landing Page. Анатомия лендинга: функциональные элементы. Принципы дизайна лендинга. Описание конструкторов. Как увеличить эффективность лендинга.

***2.3. Лекции (темы), перечень семинарских (лабораторных, практических) занятий***

***Модуль 1. Создание безопасной среды и защита персональных данных***

**Тема 1.** Компьютерная безопасность. Основы информационной безопасности и персонифицированной работы с коммуникационными сервисами.

**Тема 2.** Спам и кибермошенничество. Защита от спама. Защита информации.

**Тема 3.** Антивирусная защита. Обзор наиболее популярного антивирусного программного обеспечения. Классификация компьютерных угроз. Вирусы, черви, трояны. Клавиатурный шпион. Рекламные системы.

**Тема 4.** Личное информационное пространство: регистрация в сетевом сервисе (логин и пароль), личные данные, законодательство в сфере защиты личной информации и ответственность граждан по предоставлению личной информации.

| **Номер занятия** | **Тема практического занятия**  | **Методические рекомендации** |
| --- | --- | --- |
| 1 | 2 | 3 |
| Практическая работа 1 | «Антивирусы» - защита от вредоносных программ и спама. Что такое СПАМ и как с ним бороться. Основные меры обеспечения безопасности при осуществлении оплаты товаров и услуг через Интернет. | – ознакомиться с темой занятия;– прочитать конспект лекции по изучаемой теме;– просмотреть перечень научных источников, выбрав несколько из них для углубленного изучения данной темы; |
| Практическая работа 2 | Регистрация и работа в бесплатном сервисе на компьютере и мобильном устройстве |

***Модуль 2. Обеспечение и оценка эффективности системы защиты информационных систем персональных данных.***

**Тема 5.** Модель угроз для информационных систем персональных данных. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.

**Тема 6.** Организация и обеспечение режимов защиты персональных данных. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных..

**Тема 7.** Оценка эффективности систем защиты информационных систем персональных данных. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации. М

| **Номер занятия** | **Тема практического занятия**  | **Методические рекомендации** |
| --- | --- | --- |
| 1 | 2 | 3 |
| Практическая работа 3 | Модель угроз для информационных систем персональных данных. | – ознакомиться с темой занятия;– прочитать конспект лекции по изучаемой теме;– просмотреть перечень научных источников, выбрав несколько из них для углубленного изучения данной темы; |
| Практическая работа 4 | Организация и обеспечение режимов защиты персональных данных. |
| Практическая работа 5 | Оценка эффективности систем защиты информационных систем персональных данных |

***Блок 3. Жизнь в информационном обществе***

**Тема 8*.*** Основы сетевого этикета. Возможности общения в сетях: чаты, конференции, форумы, социальные сервисы. «Живое общение». Использование возможностей Интернета в различных сферах жизни.

| **Номер занятия** | **Тема практического занятия**  | **Методические рекомендации** |
| --- | --- | --- |
| 1 | 2 | 3 |
| Практическая работа 6 | Обзор Интернет-магазинов, оплата товаров и услуг через Интернет и с использованием банковских карт. Основы безопасной работы при оплате товаров и услуг | – ознакомиться с темой занятия;– прочитать конспект лекции по изучаемой теме;– просмотреть перечень научных источников, выбрав несколько из них для углубленного изучения данной темы; |
| Практическая работа 7 | Общение в социальных сетях. Форумы. Средства общения. |
| Практическая работа 8 | Регистрация, использование электронных учебных материалов по курсу. Тренинг по компьютерному тестированию для слушателей курса. |

***Модуль 4. Создание безопасной интернет-страницы. Cоздание Landing Page.***

**Тема 9**. Понимание принципов Landing Page.

**Тема 10.** Этапы создания Landing Page.

**Тема 11**. Анатомия лендинга: функциональные элементы.

**Тема 12.** Принципы дизайна лендинга.

**Тема 13**. Описание конструкторов.

**Тема 14.** Как увеличить эффективность лендинга.

| **Номер занятия** | **Тема практического занятия**  | **Методические рекомендации** |
| --- | --- | --- |
| 1 | 2 | 3 |
| Практическая работа 9 | Знакомство с конструкторами. | – ознакомиться с темой занятия;– прочитать конспект лекции по изучаемой теме;– просмотреть перечень научных источников, выбрав несколько из них для углубленного изучения данной темы; |
| Практическая работа 10 | Разработка и создание Landing Page. |

***2.4. Оценка качества освоения программы***

**Формы аттестации.**

В период обучения контроль знаний ведется непрерывно в виде текущей и итоговой форм контроля работы слушателей. Текущий контроль формирования компетенций проводится во время опроса в учебной аудитории во время семинаров. Итоговый контроль степени усвоения материала курса осуществляется во время зачета/экзамена. Основным подходом при составлении контрольных заданий является компетентностный подход, так как он позволяет отслеживать процесс усвоения слушателями содержания изучаемых тем.

Структура и содержание зачетных заданий, а также применение четких критериев оценки качества выполняемых заданий позволяет достаточно объективно оценивать уровень сформированности компетенций. Зачет проходит в форме письменной работы

.

 **Вопросы к модулям 1 и 2.**

1) Определение персональных данных (ПДн) и информационной системы персональных данных.

2) Нормативно-правовая база в сфере защиты и обработки ПДн (№ 149-ФЗ, № 152ФЗ).

3) Категории персональных данных.

4) Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5) Уровни защищённости информационных систем персональных данных.

6) Процесс подготовки пакета документов к аккредитации ИСПДн: обязательство о неразглашении информации, содержащей ПДн; согласие на обработку ПДн; перечень ИСПДн.

7) Процесс подготовки пакета документов к аккредитации ИСПДн: перечень ПДн, обрабатываемых и хранящихся в ИСПДн; положение об обработки ПДн работников; акт определения уровня защищённости ИСПДн.

8) Принципы обеспечения безопасности ПДн.

9) Обезличивание ПДн. Абсолютное обезличивание и относительное обезличивание.

10) Нормативно-правовая база в области обезличивания ПДн (Приказ Роскомнадзора от 5 сентября 2013 г. №996 «Об утверждении требований и методов по обезличиванию ПДн»).

11) Свойства обезличенных данных.

12) Свойства методов обезличивания.

13) Методы обезличивания персональных данных. Сравнительный анализ методов обезличивания

По итогам освоения программы обучающиеся проходят **итоговое тестирование.**

**Примерное задание для тестирования (модуль 3)**

|  |  |
| --- | --- |
| **Вопрос** | **Варианты ответов** |
| Что такое государственная услуга в электронном виде? | * Информационно-консультационный сайт по часто задаваемым вопросам граждан
* Сайт для регистрации обращений и заявок граждан с предоставлением материалов или выполнения действий по запросу
* Электронный форум пользователей государственных услуг населению
 |
| Какое первое действие требуется выполнить пользователю для обращения к государственной услуге? | * Поиск и выбор государственной услуги
* Регистрация на сайте государственных услуг
* Создание личного кабинета
 |
| Какой статус по защите личных данных имеет ресурс «личный кабинет» пользователя? | * Это персональные данные и они подлежат защите со стороны держателя портала государственных услуг
* Это личное информационное пространство и пользователь может его открыть для входа других пользователям
* Это открытые данные пользователя для всех желающих
 |
| Каков статус общественного форума на портале государственных услуг? | * Это персональные данные и они подлежат защите со стороны держателя портала государственных услуг
* Это информационное пространство и любые пользователи могут его посещать без регистрации на портале государственных услуг
* Это открытые данные пользователя для всех зарегистрированных желающих
 |
| Какие виды доступ к государственным услугам предусмотрены? | * Только через специальные пункты доступа
* С компьютера, подключенного к Интернету
* С любого устройства, имеющего доступ в Интернет
 |
| Каково назначение электронной карты пользователя государственных услуг? | * Это личная карта для регистрации и удалённого обслуживания персоны на сайте государственных услуг
* Это личная карта для электронных платежей
* Это карта для хранения информации из личного кабинета
 |
| Что позволяет выполнить электронная почта пользователя при работе на сайте государственных услуг? | * Получить доступ к услуге на сайте
* Получить доступ к личному кабинету через посылку электронного письма
* Получить ответ на запрос на сайте государственных услуг
 |
| Какие из перечисленных сервисов являются госуслугой? | * Форум на сайте государственных услуг – заказ справок
* Заказ оформления паспорта
* Оплата услуг ЖКХ
* Электронная очередь
* Электронная приёмная
* Оформление собственности
* Оформление электронного билета
* Оформление пенсионного свидетельства
* Сдача ЕГЭ в электронной форме
 |
| Для защиты данных какие рекомендации нужно использовать при выборе пароля? | * Пароль должен включать только буквы и не более 4
* Пароль должен состоять из 4 букв и 4 цифр
* Пароль должен включать буквы, цифры и символы, всего не менее 8
 |
| Какие из перечисленных имен являются именами файлов? | * free@gmail.com
* free.doc
* [www.free.org](http://www.free.org)
 |
| Какие из перечисленных имен являются ящиком электронной почты? | * free@gmail.com
* free.doc
* [www.free.org](http://www.free.org)
 |
| Какие из перечисленных сайтов являются поисковыми системами? | * Edu.ru
* Yandex.ru
* Mail.ru
* Rabota.ru
 |
| Какими услугами вы уже пользуетесь, используя подключение к Интернету? | * Найти нужную информацию
* Послать и получить электронное письмо
* Выйти в коллекцию электронных книг
* Сделать заказ в Интернет-магазине
* Выйти на видео связь с друзьями
* Зарегистрироваться в очереди
* Получить консультацию юриста
* Заказать документы
* Оплатить ЖКХ через пластиковую карту
* Купить электронный билет на транспорт
* Оплатить телефон
* Смотреть ТВ каналы
* Заказать доставку продуктов или лекарств
* Получить консультацию социального работника
* Обучаться в электронном курсе
 |

##### **РАЗДЕЛ 3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ**

***3.1. Кадровые условия***

Реализация программы осуществляется высококвалифицированным преподавательским составом и практиками, имеющими опыт педагогической и/или практической работы в профессиональной деятельности.

***3.2. Условия функционирования электронной информационно-образовательной среды***

***3.3. Виды самостоятельной работы слушателей (СРС)***

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Вид срс** | **Трудоемкость, ч.** |
|  | Работа с литературой | 6 |
|  | Подготовка к практическим работам | 6 |
|  | Выполнение домашних заданий | 6 |
| Итого | 18 |

Самостоятельная работа слушателя (СРС) представляет собой завершающий этап изучения слушателем курсов теоретических и специальных программ и должна быть выполнена как самостоятельное и завершенное исследование поставленной проблемы, имеющей практическую значимость. СРС должна быть посвящена исследованию одной проблемы. Целью написания СРС является формирование и развитие у слушателей навыков логического мышления, выявления и анализа проблем, постановки целей и задач и выработки рекомендаций по решению проблем.

***3.4. Требования и методические рекомендации по подготовке к семинарским занятиям***

В процессе подготовке к семинарскому занятию рекомендуется:

– ознакомиться с темой занятия;

– прочитать конспект лекции по изучаемой теме;

– просмотреть перечень научных источников, выбрав несколько из них для углубленного изучения данной темы;

– ознакомиться с позицией авторов изучаемых произведений, законспектировать основные положения их концепций;

– подготовить план вопросы, ответы на которые планируется получить в результате обучения;

– выучить определения понятий, составляющих основу данной темы.

##### РАЗДЕЛ 4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ПРОГРАММЫ

Здания и помещения Волгоградского государственного университета обеспечивают стабильную работу программно-технического комплекса, систем связи и других технических компонентов, систем энерго-, водо- и теплоснабжения, кондиционирования воздуха, противопожарных систем, обеспечивают защищенность персонала. Здания и помещения соответствуют требованиям санитарных норм, установленным действующим законодательством.

В наличии имеется учебно-материальная база в местах проведения обучения, аудиторный фонд, оснащен средствами обучения: информационными образовательными технологиями; исчерпывающим набором дидактических, учебно-методических материалов, изучение которых предусмотрено программой, из расчета по одному комплекту на каждого слушателя; библиотекой с необходимым количеством учебной, методической литературы и другой печатной продукцией на каждого слушателя, читальным залом, а также помещениями для самостоятельной работы слушателей.

Материально-технические условия, созданные в институте дополнительного образования, позволяют успешно использовать компьютерное оборудование и внедрять в образовательный процесс информационно-коммуникационные технологии. Вся имеющаяся в аудиториях компьютерная техника и проекционное оборудование находятся в рабочем состоянии. Качественные характеристики аудиторий, их техническая оснащённость, благоприятная образовательная атмосфера позволяют организовывать обучение, которое гарантирует не только его качество, но и наличие среды, создающей условия для оптимальной организации образовательного процесса.

На занятиях программы широко представлена визуальная информация, как в компьютерном, так и в ручном вариантах. Все лекционные курсы представлены в системе видеопрезентации, на практических занятиях используются учебные фильмы и видеокейсы. Все это позволяет расширить объем передаваемой информации, вырабатывает у слушателей навыки овладения технологией визуализации.

Изучение дисциплины лицами с ограниченными возможностями здоровья и инвалидов обеспечивается посредством доступа к учебно-методическим материалам по дисциплине, размещенным в системе электронных ресурсов Moodle. Основной формой, применяемой при реализации дистанционных образовательных технологий, является индивидуальная форма обучения. С этой целью, разрабатываются индивидуальные графики для каждого обучающегося, в которых уточняются методы и темпы учебной деятельности, при необходимости вносятся корректировки в деятельность обучающегося и преподавателя. Индивидуальные задания подбираются в адаптивных к ограничениям здоровья формах (письменно или устно, в форме презентации). Наряду с этим, ведущим преподавателем осуществляются индивидуальные консультации обучающегося посредством on-line и off-line технологий (очно, в часы консультаций, по электронной почте, а также с использованием программ Skype, Wiber, а также возможностей социальных сетей). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Организационно-техническое обеспечение занятий Обучение рекомендуется проводить в помещении, оборудованном компьютерными местами для 1-2 обучающихся и одним компьютерным местом педагога, флэш-картами не менее одной на двух обучающихся, проектором и экраном или интерактивной доской для коллективной работы с учебными материалами. Должен быть обеспечен доступ в Интернет (стационарное подключение или мобильный доступ через мобильный модем).

Для проведения занятий предусмотрены две модели оборудования.

Модель «Компьютерный класс с выходом в Интернет» и модель «Мобильный телефон с подключением к Интернету». Выбор модели определяется условиями коммуникационного обслуживания в населенном пункте. Для каждого занятия предусмотрены два варианта практических (диагностических) заданий соответственно для работы на компьютере и работы с мобильным телефоном.

Для лекций возможны следующие формы организации занятия:

- коллективный просмотр видеозаписи через Интернет или на носителе на компьютере педагога через проектор,

- индивидуальный просмотр видеозаписи в локальной сети класса или автономно с носителя на компьютерах слушателей с наушниками,

- выступление педагога с предоставленной ему презентацией, которая доступна всем слушателям.

Для практической работы возможны следующие формы организации занятий:

- коллективное выполнение учебной практической работы на компьютере или мобильном телефоне педагога с анализом хода работы с использованием проектора и экрана, поочередное выполнение этапов работы слушателями на компьютере педагога,

- выполнение работы в парах за одним компьютером с контролем со стороны педагога,

- персональная работа с заданием за компьютером или мобильным телефоном слушателем с контролем со стороны педагога.

Педагог должен быть обеспечен: флэш-картами, корпоративной сим-картой и мобильным телефоном, корпоративной электронной почтой на сайте курса, блогом и правами модератора на форуме курса.

**РАЗДЕЛ 5. ИНФОРМАЦИОННО-МЕТОДИЧЕСКИЕ ТРЕБОВАНИЯ ПРОГРАММЫ**

* 1. Обеспеченность информационными ресурсами и программными продуктами, используемыми в программе.

Microsoft Office

Acrobat Professional 9/0 WIN

Google Chrom

Kaspersky Endpoint Security

* 1. Каждому слушателю программы выдается удостоверение, по которому он может пройти в университет, а также пользоваться абонементом, залом периодики, читальным залом.

Слушатели имеют доступ к ссылкам на интернет – сайты, в том числе на сайт электронной библиотеки ВолГУ и на сайты, находящиеся в свободном доступе.

***Учебно-методические пособия***

|  |  |  |
| --- | --- | --- |
|  | **Название, автор** | **Год выпуска** |
| 1. | Пушкарёва Т. П. Основы компьютерной обработки информации [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по направлениям подготовки: 22.03.01 "Материаловедение и технологии материалов", 29.03.04 "Технология художественной обработки материалов", 22.04.01 "Материаловедение и технология" / Т. П. Пушкарёва ; М-во образования и науки Российской Федерации, Сибирский федеральный ун-т, [Политехнический ин-т]. - Красноярск : СФУ, 2016. - 179 с. : ил., табл., цв. ил.; 21 см. - (Материаловедение и технологии материалов).; ISBN 978-5-7638-3492-5 | 2016 ЭБС  |

1. Рекомендуемая литература:
	1. ***Основная литература****.*

|  |  |  |
| --- | --- | --- |
|  | Название, автор | Фонд |
|  | Башлы, П.Н. Информационная безопасность и защита информации: Учебник 1./ П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – М.: РИОР, 2013. – 222 с.  | 2019URL:http://znanium.com/bookread.php?book=405000 |
|  | Борисова И.В.Цифровые методы обработки информации/БорисоваИ.В. - Новосиб.: НГТУ, 2014. - 139 с.: ISBN 978-5-7782-2448-3 | 2014URL: <http://znanium.com/bookread2.php?book=546207&spec=1> |
|  | Горелов, Н. А.   Развитие информационного общества: цифровая экономика : учебное пособие для вузов / Н. А. Горелов, О. Н. Кораблева. — Москва : Издательство Юрайт, 2019. — 241 с. — (Университеты России). — ISBN 978-5-534-10039-6. | 2019URL:<https://biblio-online.ru/viewer/razvitie-informacionnogo-obschestva-cifrovaya-ekonomika-429156?share_image_id=> |
|  |  |  |

***4.2. Дополнительная литература.***

|  |  |  |
| --- | --- | --- |
|  | Название, автор | Фонд |
|  | Трайнер В.А.Электронно-образовательные ресурсы в развитии информационного общества (обобщение и практика) / Трайнев В.А. - М.:Дашков и К, 2018. - 256 с.: ISBN 978-5-394-02464-1 | 2018URL: http://znanium.com/catalog/product/513047 |
|  |  |  |

***4.3.******Электронные образовательные ресурсы***

|  |  |
| --- | --- |
| Э1 | Образовательный портал «УМНИК»: http://new.volsu.ru/umnik |
| Э2 | Федеральный образовательный портал. Библиотека. Единое окно доступа к образовательным ресурсам: http://window.edu.ru/library |
| Э6 | Научная электронная библиотека: http://elibrary.ru |

***4.4. Перечень информационных технологий, программного обеспечения и информационных справочных систем***

Информационно-правовая система «КонсультантПлюс» http://www.consultant.ru/