|  |
| --- |
| «УТВЕРЖДАЮ»  Проректор по НИР  ТГПУ им. Л. Н. Толстого  К.А. Подрезов  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_2020 г. |

1. **ПАСПОРТ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

«Кибербезопасность и защита данных»

|  |  |  |
| --- | --- | --- |
| **Версия программы** | 2 |  |
| **Дата Версии** | 10**.**10**.**2020 |  |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Федеральное государственное бюджетное образовательное учреждение высшего образования "Тульский государственный педагогический университет им. Л.Н. Толстого" |
| 1.2 | Логотип образовательной организации | C:\Users\specdigec\Downloads\logo.png |
| 1.3 | Провайдер ИНН | **7107030811** |
| 1.4 | Ответственный за программу ФИО | **Богатырева Юлия Игоревна** |
| 1.5 | Ответственный должность | **заведующий кафедрой информатики и информационных технологий** |
| 1.6 | Ответственный Телефон | **+7(920)2767176** |
| 1.7 | Ответственный Е-mail | **bogatirevadj@yandex.ru** |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Кибербезопасность и защита данных |
| 2.2 | Ссылка на страницу программы | <http://cert.tsput.ru/course/view.php?id=4> |
| 2.3 | Формат обучения | Онлайн |
|  | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | Между организацией и Университетом 2035 настроена передача цифрового следа по REST API из LMS Moodle на стороне ОО в сторону Университета. Настроена бесшовная авторизация с использованием SSO Leader-id. |
| 2.4 | Уровень сложности | Базовый |
| 2.5 | Количество академических часов | **72** |
|  | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | 69 |
| 2.6 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | 15000     1. Информационная и веб-безопасность   Ссылка <https://www.specialist.ru/dictionary/definition/security-common>  Центр компьютерного обучения «Специалист» при МГТУ имени Н.Э. Баумана  Стоимость 47 890 рублей за 80 академических часов.  Без нормативно-правового обеспечения информационной безопасности и без построения модели угроз.Конец формы   1. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ЗАКОНА №187-ФЗ «О БЕЗОПАСНОСТИ КИИ РФ»  * 72 академических часа. Дистанционно, без отрыва от работы. * Стоимость курса повышения квалификации объёмом 72 часа: от 20 000 руб. за специалиста * Ссылка: <https://infobezopasnost.ru/informacionnaya-bezopasnost-kii/>   Курс направлен на изучение теоретических и прикладных вопросов организации безопасности значимых объектов критической информационной инфраструктуры (КИИ), категорирования объектов КИИ и построения систем защиты значимых объектов КИИ в соответствии с требованиями № 187- ФЗ от 26.07.2017. Подробнее: <https://infobezopasnost.ru/informacionnaya-bezopasnost-kii/>  Без нормативно-правового обеспечения информационной безопасности и без рассмотрения вопросов биометрических систем защиты данных.   1. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных (72 часа)   Тульский государственный университет   * Целью реализации программы является освоение специалистами актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации. * Форма обучения: Очная * Стоимость обучения: 25 000 рублей за 72 часа   Ссылка <http://itpk.tsu.tula.ru/programs.php>  Без дистанционного обучения и без рассмотрения вопросов работы с биометрическими системами идентификации. |
| 2.7 | Минимальное количество человек на курсе | 20 |
| 2.8 | Максимальное количество человек на курсе | 35 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 76 |
| 2.10 | Формы аттестации | тестирование |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Кибербезопасность и защита данных |

1. **Аннотация программы**

Целью реализации программы является совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации, необходимой для профессиональной деятельности в области обеспечения кибербезопасности и информационной безопасности.

Задачи курса:

- знакомство с законодательной и нормативно-правовой базой по информационной безопасности и кибербезопасности;

- изучение основных понятий кибербезопасности, информационной безопасности и защиты данных;

- получение навыков практического применения безопасного использования технических и программных средств защиты данных;

- формирование навыков защиты данных в условиях существования угроз их информационной безопасности для эксплуатации и сопровождения информационных систем и сервисов.

Объектами профессиональной деятельности являются:

- технологии обеспечения кибербезопасности и информационной безопасности информационных систем и сервисов, компьютерных систем и сетей;

- системы управления защитой данных в условиях существования угроз их информационной безопасности для эксплуатации и сопровождения информационных систем и сервисов.

Категории обучающихся: руководители и сотрудники организаций и предприятий, отвечающих за админист­рирование информационных систем и сетей, администраторы информационной безопас­ности, специалисты по защите информации, аналитики по вопросам компьютерной безо­пасности, пользователи компьютерных сетей и сервисов.

Лица, желающие освоить дополнительную профессиональную программу повышения квалификации, должны иметь высшее, среднее непрофильное или техническое образование.

1. **ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ**

|  |  |
| --- | --- |
|  | МИНПРОСВЕЩЕНИЯ РОССИИ  Федеральное государственное бюджетное образовательное учреждение  высшего образования  «Тульский государственный педагогический университет им. Л.Н. Толстого»  (ТГПУ им. Л.Н. Толстого) |

|  |  |
| --- | --- |
|  | «УТВЕРЖДАЮ»  Проректор по НИР  ТГПУ им. Л. Н. Толстого  К.А. Подрезов  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_2020 г. |

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ**

«Кибербезопасность и защита данных»

72 час.

Руководитель программы повышения квалификации:

Богатырева Юлия Игоревна, д.п.н., доцент, заведующий кафедрой информатики и информационных технологий

Тула, 2020

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

1. **Цель программы**

Целью реализации программы является совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации, необходимой для профессиональной деятельности в области обеспечения кибербезопасности и информационной безопасности.

**2.Планируемые результаты обучения:**

|  |  |
| --- | --- |
| **Результаты (освоенные профессиональные и общие компетенции)** | **Основные показатели оценки результата** |
| ПК 1. Проведение анализа безопасности компьютерных систем | способность оценивать и проводить анализ угроз и уровня безопасности компьютерных систем и сетей;  - знает основные понятия кибербезопасности, информационной безопасности и персональных данных; сущность и содержание понятия информационной безопасности, характеристики ее составляющих; правовые основы обеспечения кибербезопасности;  - описывает риски и угрозы персональных данных; эффективность защиты данных.  - владеет навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети. |
| СПК 1.1 Обслуживание средств защиты информации прикладного и системного программного обеспечения | способность обслуживать средства защиты информации в компьютерных системах и сетях;  - знает источники угроз информационной безопасности и меры по их предотвращению; особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения; уязвимости компьютерных систем и сетей; принципы работы и правила эксплуатации программно-аппаратных средств защиты данных;  - умеет ориентироваться в современных угрозах и факторах риска в условиях цифровой трансформации общества и государства;  - противодействует угрозам кибербезопасности с использованием аппаратных и программных средств защиты информации;  - работает с программным обеспечением с соблюдением действующих требований по защите информации;  - владеет навыками безопасного использования технических и программных средств защиты информации; навыками настройки программного обеспечения с соблюдением требований по защите информации; проверки функционирования встроенных средств защиты информации программного обеспечения; |
| СПК 1.2 Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей | способность разрабатывать требования и политику информационной безопасности компьютерных систем и сетей, в том числе биометрическими системами защиты данных;  - знает нормативные правовые акты в области защиты информации; организационные, технические и правовые меры по защите информации; основные понятия о биометрических системах защиты данных;  - формулирует принципы и строит модель угроз и нарушителей по методике ФСТЭК;  - умеет формулировать и проектировать политику информационной безопасности организации (предприятия);  - владеет навыками работы с биометрическими системами идентификации и аутентификации; навыками разработки модели угроз безопасности информации для политики безопасности; заданием требований к защите информации компьютерной системы в политике безопасности; |

2.1.Знание (осведомленность в областях)

2.1.1 основные понятия кибербезопасности, информационной безопасности и персональных данных;

2.1.2 сущность и содержание понятия информационной безопасности, характеристики ее составляющих;

2.1.3 источники угроз информационной безопасности и меры по их предотвращению;

2.1.4 особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения;

2.1.5 основные понятия о биометрических системах защиты данных;

2.1.6 уязвимости компьютерных систем и сетей;

2.1.7 правовые основы обеспечения кибербезопасности;

2.1.8 нормативные правовые акты в области защиты информации;

2.1.9 организационные, технические и правовые меры по защите информации;

2.1.10 принципы работы и правила эксплуатации программно-аппаратных средств защиты данных

2.2. Умение (способность к деятельности)

2.2.1 формулировать принципы и строить модель угроз и нарушителей по методике ФСТЭК;

2.2.2 описывать риски и угрозы персональных данных;

2.2.3 формулировать и проектировать политику информационной безопасности организации (предприятия);

2.2.4 ориентироваться в современных угрозах и факторах риска в условиях цифровой трансформации общества и государства;

2.2.5 противодействовать угрозам кибербезопасности с использованием аппаратных и программных средств защиты информации;

2.2.6 работать с программным обеспечением с соблюдением действующих требований по защите информации; - оценивать эффективность защиты данных.

2.3.Навыки (использование конкретных инструментов)

2.3.1 безопасного использования технических и программных средств защиты информации;

2.3.2 оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем;

2.3.3 работы с биометрическими системами идентификации и аутентификации;

2.3.4 настройки программного обеспечения с соблюдением требований по защите информации;

2.3.5 проверки функционирования встроенных средств защиты информации программного обеспечения;

2.3.6 определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети;

2.3.7 разработки модели угроз безопасности информации;

2.3.8 задание требований к защите информации компьютерной системы.

**3.Категория слушателей** (возможно заполнение не всех полей)

* 1. Высшее или среднее специальное
  2. Не требуется
  3. Для изучения программы желательно иметь основные знания в области информационных технологий, а также базовые знания из курса информатики и математики.
  4. Информатика, Информационные технологии

**4. Учебный план программы «Кибербезопасность и защита данных»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Основные понятия кибербезопасности и информационной безопасности | 12 | 1 |  | 11 |
| 2 | Правовые основы кибербезопасности | 12 | 1 |  | 11 |
| 3 | Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации | 12 | 1 | 2 | 9 |
| 4 | Аппаратные и программные средства защиты данных | 12 |  | 4 | 8 |
| 5 | Практические аспекты обеспечения защиты данных | 12 |  | 4 | 8 |
| 6 | Биометрические системы идентификации | 12 |  | 2 | 10 |
| **Итоговая аттестация** | | **72** | **тестирование** | | |
| **ИТОГО** | | **72** | **3** | **12** | **57** |

**5. Календарный план-график реализации образовательной программы**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Основные понятия кибербезопасности и информационной безопасности | 12 | 02.11.2020-05.11.2020 |
| 2 | Правовые основы кибербезопасности | 12 | 06.11.2020-10.11.2020 |
| 3 | Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации | 12 | 11.11.2020-14.11.2020 |
| 4 | Аппаратные и программные средства защиты данных | 12 | 16.11.2020-18.11.2020 |
| 5 | Практические аспекты обеспечения защиты данных | 12 | 19.11.2020-21.11.2020 |
| 6 | Биометрические системы идентификации | 12 | 23.11.2020-24.11.2020 |
| **Всего:** | | 72 | 25.11.2020 |

**6. Учебно-тематический план программы «Кибербезопасность и защита данных »**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Модуль 1. Основные понятия кибербезопасности и информационной безопасности | 12 | 1 |  | 11 | тест |
| 1.1 | Информатизация общества: социальные условия, предпосылки и последствия | 2 |  |  | 2 |  |
| 1.2 | Основные понятия информационной безопасности и защиты данных | 5 | 1 |  | 4 |  |
| 1.3 | Целостность, доступность и конфиденциальность информации | 5 |  |  | 5 |  |
| 2 | Модуль 2. Правовые основы кибербезопасности | 12 | 1 |  | 11 | тест |
| 2.1 | Нормативно-правовые акты в области обеспечения информационной безопасности и кибербезопасности | 7 | 1 |  | 6 |  |
| 2.2 | Виды защищаемой информации | 2 |  |  | 2 |  |
| 2.3 | Правовые основы защиты интеллектуальной собственности | 3 |  |  | 3 |  |
| 3 | Модуль 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации | 12 | 1 |  | 11 | тест |
| 3.1 | Понятие угрозы безопасности защищаемой информации | 5 | 1 |  | 4 |  |
| 3.2 | Классификация угроз безопасности информации | 4 |  | 2 | 2 | Выполнение практических заданий |
| 3.3 | Модель угроз информационной безопасности и политика информационной безопасности предприятия | 3 |  |  | 3 |  |
| 4 | Модуль 4. Аппаратные и программные средства защиты данных | 12 |  | 4 | 8 | Выполнение практических заданий |
| 5 | Модуль 5. Практические аспекты обеспечения защиты данных | 12 |  | 4 | 8 | Выполнение практических заданий |
| 6 | Модуль 6. Биометрические системы идентификации | 12 |  | 2 | 10 | Выполнение практических заданий |

**7. Учебная (рабочая) программа повышения квалификации «**Кибербезопасность и защита данных**»**

**Модуль 1. Основные понятия кибербезопасности и информационной безопасности**

Тема 1.1 Информатизация общества: социальные условия, предпосылки и последствия Цифровая трансформация: влияние ИТ на развитие общества. Вызовы современного информационного общества. Статистика потерь от утечки данных. Каналы утечек информации. Понятие информационной безопасности.

Тема 2.2 Основные понятия кибербезопасности и защиты данных. Цели, задачи, направления информационной безопасности. Понятия «кибербезопасности», «киберпространства», «киберпреступления», «кибервойна». Киберзащищенность объекта защиты.

Тема 2.3 Целостность, доступность и конфиденциальность информации. Уровни и принципы обеспечения информационной безопасности. Задачи кибербезопасности в современных условиях и информационных проблем цифровой экономики. Направления кибербезопасности. Проблемы и технологические решения. Субъекты и объекты критической инфраструктуры. Составляющие обеспечения информационной безопасности. Организационные, технические и правовые меры по защите информации.

**Модуль 2. Правовые основы кибербезопасности**

Тема 2.1 Нормативно-правовые акты в области обеспечения информационной безопасности и кибербезопасности

Конституция Российской Федерации. Конституционное право на поиск, получение и распространение информации. Уголовный Кодекс Российской Федерации. Ответственность за киберпреступления. Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 237 УК РФ). Понятие кибепреступлений. Статистика киберпреступлений в России и мире. Мошенничество с использованием электронных средств платежа. Классификация сведений, подлежащих защите. Закон РФ "Об информации, информационных технологиях и о защите информации". Доктрина информационной безопасности РФ. Концепция национальной безопасности РФ. Стратегия развития информационного общества в РФ. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 — 2030 годы». Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»). Федеральный закон Российской Федерации «О безопасности критической информационной инфраструктуры». Другие федеральные законы. ГОСТы в сфере защиты информации.

Тема 2.2 Виды защищаемой информации.

Классификация сведений, подлежащих защите. Общедоступная информация. Понятие государственной тайны. Сведения, составляющие коммерческую тайну. Служебная и профессиональные тайны. Основные отличия и характеристики. Персональные данные: понятия, особенности защиты. Классификация ИС персональных данных.

Тема 2.3 Правовые основы защиты интеллектуальной собственности.

Виды программного обеспечения. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo). Лицензионное ПО. Правовая охрана программ для ЭВМ и БД. Авторское право. Понятие и виды интеллектуальной собственности. Правовая охрана программ для ЭВМ и БД. Гражданский кодекс Российской Федерации (часть IV редакция от 01 января 2008 года). Раздел VII. Права на результаты интеллектуальной деятельности и средства индивидуализации

**Модуль 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации**

Тема 3.1. Понятие угроз кибербезопасности. Понятие угрозы безопасности защищаемой информации. Источники угроз информационной безопасности и меры по их предотвращению. Риски и угрозы персональным данным. Примеры атак на информационные системы. Нарушители информационной безопасности.

Тема 3.2 Классификация угроз безопасности информации. Общий анализ рисков. Внешние и внутренние угрозы кибербезопасности. Источники угроз информационной безопасности личности. Определение целей защиты данных на предприятии. Случайные угрозы. Угрозы доступности информации. Угрозы нарушения целостности информации. Угрозы конфиденциальности информации. Особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения. Определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети. Источники угроз безопасности информации (по рекомендациям ФСТЭК).

Тема 3.3. Разработка модели угроз безопасности информации. Задание требований к защите информации компьютерной системы. Модель угроз информационной безопасности. Преднамеренные угрозы. Определение угроз информационной безопасности и анализ рисков на предприятии. Построение модели угроз. Факторы, риски угроз информационным ресурсам. Виды угроз и типы атак. Анализ и оценивание угроз информационной безопасности личности в современном цифровом обществе. Принципы построения моделей угроз и нарушителей по методике ФСТЭК. Методика определения угроз безопасности информации в информационных системах (согласно методическим рекомендациям ФСТЭК). Политика информационной безопасности предприятия (организации). Уязвимости компьютерных систем и сетей.

**Модуль 4. Аппаратные и программные средства защиты данных**

Понятие и сущность защиты данных. Цели защиты данных. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. Кодирование информации. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Аппаратные средства. USB ключ защиты. Формальные средства защиты информации. Физические средства защиты информации. Аппаратные средства защиты информации. Принципы работы и правила эксплуатации программно-аппаратных средств защиты данных. Правила и принципы безопасного использования технических и программных средств защиты информации

**Модуль 5. Практические аспекты обеспечения защиты данных**

Восстановление и защита данных. Резервное копирование. Управление дисками. Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов. Парольная защита с помощью стандартных системных средств. Электронная подпись. Правовая основа использования и получения электронной подписи. Общие подходы к построению парольных систем. Выбор паролей. Хранение паролей. Безопасность мобильных устройств.

**Модуль 6. Биометрические системы идентификации**

Механизмы идентификации и аутентификации. Способы аутентификации. Понятие биометрической системы. Биометрическая идентификация. Виды биометрических систем. Группы биометрических параметров. Физиологические (статические) группы методов идентификации. Способы построения систем биометрической идентификации личности. Обзор готовых решений. Динамические (поведенческие) методы биометрической идентификации. Перспективы использования биометрических систем.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| 1.1 | 3.3 Модель угроз информационной безопасности и политика информационной безопасности предприятия | Построение модели угроз | Разработка/корректировка политики информационной безопасности или/и модели угроз информационной безопасности в соответствии с базовой моделью угроз ФСТЭК |
| 1.2 | Модуль 4. Аппаратные и программные средства защиты данных | Аппаратные средства защиты информации. Программные средства защиты данных. | Создание USB ключа для ограничения доступа к компьютеру средствами ОС WINDOWS |
| 1.3 | Модуль 5. Практические аспекты обеспечения защиты данных | Безопасность мобильных устройств | Данная работа состоит из 10 практических заданий, выполняемых на мобильном устройстве и позволяющих существенно повысить его уровень защищённости. |
| 1.4 | Модуль 6. Биометрические системы идентификации | Технологии биометрической идентификации | Формирование теоретических знаний и практических навыков анализа возможностей использования средств биометрической идентификации для защиты данных и идентификации пользователей систем при выполнении комплекса практических заданий. |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
|  | Тест входного контроля состоит из 10 вопросов  Примерные вопросы:  В качестве аутентификатора пользователя в сети Интернет могут использоваться:  - кардиограмма пользователя  - номер карточки пенсионного страхования  - результат работы генератора одноразовых паролей  - отпечаток пальца пользователя  К нормативно-правовой базе обеспечения информационной и кибербезопасности НЕ относят:  - Гражданский Кодекс РФ  - Уголовный Кодекс РФ  - Конституцию РФ  - Семейный Кодекс РФ |  | Тест итогового тестирования состоит из 10 вопросов  Примерные вопросы:  Штатный персонал организации и вспомогательный персонал (охрана) относят к категории источников угроз безопасности:  - стихийные  - антропогенные внутренние  - техногенные  - антропогенные внешние  Нарушитель информационной безопасности организации - это физическое лицо или логический объект, случайно или преднамеренно совершивший действия, следствием которых является … |
| 1 |  | Тест по Модулю 1 состоит из 10 вопросов  Примерные вопросы:  Какие из нижеперечисленных вызовов НЕ относятся к современным угрозам и факторам риска современного информационного общества  - тотальная доступность информации, в том числе запрещенная для распространения  - экспоненциальный рост объёмов информации, в том числе дезинформации  - аутентификация и идентификация личности в сети Интернет  - нарушение авторских прав и прав на охрану частной (личной) жизни |  |
| 2 |  | Тест по Модулю 2 состоит из 10 вопросов  Примерные вопросы:  В Доктрине информационной безопасности НЕ сформированы  - основные информационные угрозы  - принципы конфиденциальности и целостности информации  - направления обеспечения информационной безопасности  - понятие информационной инфраструктуры Российской Федерации  Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:  - обеспечение защиты информации от неограниченного доступа  - соблюдение конфиденциальности информации ограниченного доступа  - реализацию права на доступ к разрешенной информации  - возможность незамедлительного восстановления информации. |  |
| 3 |  | Тест по Модулю 3 состоит из 10 вопросов  В соответствии с Методикой определения угроз безопасности информации результаты оценки возможностей нарушителя, содержащие типы, виды и потенциал нарушителей, цели, которые могут преследовать нарушители каждого вида, а также возможные способы реализации угроз безопасности информации, образуют …  - модель угроз  - модель нарушителей  - виды нарушителей  - модель защиты данных  Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена, называют …  - утечка информации  - разглашение информации  - отказ программного обеспечения  - нарушение целостности информации |  |

**8.2.**  Оценка качества освоения программы включает текущую, промежуточную и итоговую аттестацию обучающихся.

Контрольно-проверочные занятия включают входной и текущий контроли, а также итоговую аттестацию обучающихся.

Входной контроль охватывает всех обучаемых и проводится в форме тестирования. Целью его является определение уровня знаний обучаемых для корректировки и адаптации учебного процесса под конкретные потребности обучаемых, с учётом уровня освоения учебного материала, изученного ими ранее в рамках получения базового образования или на курсах повышения квалификации.

Текущий контроль охватывает как можно большее число слушателей с обязательной оценкой их знаний, умений и навыков. Он призван стимулировать учебную работу слушателей и проводиться в форме, избранной преподавателем или предусмотренной рабочей программой.

Оценочные средства, включают типовые задания, выполняемые в ходе практических занятий и тесты, позволяющие оценить знания, умения и уровень приобретенных компетенций. В ходе тестирования используются современные способы и формы оценивания обучающихся, включая создание единой информационной среды с электронными формами контроля и оценки.

Программы текущего контроля и промежуточной аттестации максимально приближены к условиям (требованиям) их профессиональной деятельности.

Конкретные формы и процедуры входного и текущего контроля знаний по каждой теме разрабатываются учебным заведением самостоятельно и доводятся до сведения обучающихся в течение первого дня обучения.

Для проведения контрольно-проверочных занятий образовательным учреждением разработаны тестовые задания, включающие: организационно-методические указания по прохождению тестирования; вопросы для тестирования (не менее 20 вопросов для итогового теста).

Максимальное количество баллов, которое возможно набрать в результате тестирования, равняется 100. Для успешного прохождения тестирования и получения оценки «зачтено» необходимо набрать не менее 40 баллов. В остальных случаях предусматривается оценка «не зачтено». Оценка «зачтено» дифференцируется по 4-уровневой системе знаний в зависимости от количества набранных баллов.

В конце изучения каждого модуля слушатели, набравшие не менее 50% баллов за выполнение теста по теме и/или практических заданий, могут претендовать на получение зачета по модулю, для зачета по курсу необходимо успешно (не менее 50%) пройти итоговое тестирование по всему курсу.

При этом как в вопросах, так и в ответах учтена возможность многовариантности решений. Вопросы, предлагающие выбрать все правильные варианты ответа, имеют два и более верных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа. Ответ на вопрос считается правильным, если он является полным.

Тест включает в себя вопросы, направленные как на контроль знаний, так и на проверку полученных навыков работы. Во время тестирования запрещается пользоваться ка-кой-либо литературой или заранее подготовленными записями.

При проведении тестирования с использованием единой информационной среды с электронными формами контроля и оценки у каждого слушателя есть три попытки на прохождение тестирования. Время на одну попытку - 40 минут. По окончанию попытки слушатель может видеть результаты теста и полученные баллы через две минуты после отправки результатов. При этом имеется возможность просмотра отчета, показывающего ошибки при прохождении теста. Оценка выставляется по последней попытке.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей образовательной программы создаются фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить знания, умения и уровень приобретенных компетенций. Фонды оценочных средств разрабатываются и утверждаются образовательным учреждением самостоятельно.

Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы повышения квалификации и (или) отчисленным из организации, выдается справка об обучении или о периоде обучения, по установленному образцу.**.**

**8.3.**  **примеры контрольных заданий по модул**ю 6. 1 Изучите основные нормативные и справочные документы, регламентирующие работу с биометрическими системами идентификации/аутентификации, перечень их представьте в отчете; 2. рассмотрите и представьте в отчете критерии биометрической идентификации; 3. опишите порядок регистрации гражданина РФ через портал Госуслуг. Биометрическая идентификация пользователя в Единой биометрической системе. Укажите достоинства и недостатки данной системы. **.**

**8.4.**  Основными критериями оценки усвоения слушателями учебного материала при проведении текущего контроля в ходе практических занятий являются: полнота ответов на поставленные вопросы; правильность выполнения действий при отработки практических вопросов эксплуатации изучаемых средств защиты информации; соответствие содержания и объёма выполненного задания поставленной задаче; правильность оформления; правильное форматирование отрабатываемых документов; правильность оформления ссылок на правовые, нормативные и методические документы.

При этом для каждого критерия оценки каждого практического занятия определяются весовые коэффициенты, позволяющие в определённом конкретном случае получать наиболее объективные оценки выполненных слушателями заданий. **.**

**8.5.**  Тестирование по модулю 1-3. Выполнение практических заданий по модулю 4-6

Входное и итоговое тестирование. Рефлексия по каждому модулю**.**

**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** | Богатырева Юлия Игоревна | Заведующий кафедрой информатики и информационных технологий ФГБОУ ВО «Тульский государственный педагогический университет им. Л.Н. Толстого», доктор педагогических наук, доцент | https://tsput.ru/faculties\_and\_departments/departments/department\_of\_mathematics\_physics\_and\_informatio/informatic/zav.php |  | **да** |
| **2** | Гореликова Татьяна Владимировна | Ассистент кафедры информатики и информационных технологий ФГБОУ ВО «Тульский государственный педагогический университет им. Л.Н. Толстого» |  |  | **да** |
| 3 | Яковлева Надежда Александровна | Ассистент кафедры информатики и информационных технологий ФГБОУ ВО «Тульский государственный педагогический университет им. Л.Н. Толстого» | https://tsput.ru/faculties\_and\_departments/departments/department\_of\_mathematics\_physics\_and\_informatio/informatic/lecturer/120669/ |  |  |

**9.2.Учебно-методическое обеспечение и информационное сопровождение**

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки, материалы курса, учебная литература |
| Педагогические технологии на основе активизации и интенсификации деятельности слушателей, в частности: проблемное обучение, групповые технологии, информационные технологии обучения, включая дистанционные, интерактивные способы взаимодействия преподавателя и слушателей (в том числе дискуссии), личностно-ориентированная технология обучения, использование практико ориентированного подхода. | Основная литература:  1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учеб. пособие. -М.: Горячая линия-Телеком, 2006. - 352 с.  2. Девянин, П.Н. Теоретические основы компьютерной безопасности [Текст] / П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. – М.: «Радио и связь». – 2010. – 156 с.  3. Ковалев Д. В., Богданова Е. А. Информационная безопасность: учебное пособие Ростов-на-Дону: Издательство Южного федерального университета, 2016 <http://biblioclub.ru/index.php?page=book&id=493175>  4. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. Учебное пособие. - М.: Гелиос АРВ, 2006. – 143 с.  Дополнительная литература  1. Alpro. Современные тенденции и перспективы развития рынка биометрических систем. Новинки биометрических технологий [Электр. ресурс] URL <http://www.alpro.ru/upload/docs/Alpro-ZKTeco1606.pdf> (дата обращения 12.01.2020)  2. Google патентует систему сканирования радужной оболочки в контактных линзах [Электр. ресурс] URL http://www.oszone.net/27542/ (дата обращения 02.02.2020)  3. Основы информационной безопасности. Часть 2. Информация и средства её защиты. технологий [Электр. ресурс] https://habr.com/ru/company/vps\_house/blog/343498/(дата обращения 13.01.2020)  4. Скрипник Д. А. Обеспечение безопасности персональных данных: курс Москва: Интернет- Университет Информационных Технологий, 2011  <http://biblioclub.ru/index.php?page=book&id=234794>  5. Шилов А. К. Управление информационной безопасностью: учебное пособие Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2018 <http://biblioclub.ru/index.php?page=book&id=500065> |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Среда электронного обучения LMS Moodle <http://cert.tsput.ru/> | Официальный сайт ФГБОУ ВО «Тульский государственный педагогический университет им. Л.Н. Толстого» [www.tsput.ru](http://www.tsput.ru) |
| Федеральные законы, законодательные акты, руководящие документы в области ИБ: <http://docs.pravo.ru/> |
| Кибербезопасность [электронный ресурс] URL: <https://spravochnick.ru/informacionnaya_bezopasnost/kiberbezopasnost_i_informacionnaya_bezopasnost/> |
| Кияев В., Граничин О. Безопасность информационных систем: курс Москва: Национальный Открытый Университет «ИНТУИТ», 2016 http://biblioclub.ru/inde x.php? page=book&id=42903 2 |
| Энциклопедия информационной безопасности [Электронный ресурс]. - Информационная безопасность. - <http://www.wikisec.ru> |
| Лучшие антивирусы для Андроид – ТОП-10. [Электр. ресурс] <https://www.anti-malware.ru/compare/Best_antivirus_for_Android_TOP_10_2015_part_1> | Массачусетский Технологический институт. Курс лекций #6.858.: «Безопасность мобильных телефонов», часть 1. [Электр. ресурс] <https://habr.com/ru/company/ua-hosting/blog/432616/> |
| Gemalto: building trust in mobile apps. The consumer perspective. / Gemalto, July 2019 . [Электр. ресурс] <https://www.gemalto.com/brochures-site/download-site/Documents/tel-consumer-perspectives.pdf> |

**9.3.Материально-технические условия реализации программы**

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Практические занятия | Операционная система Microsoft Windows XP / Professional 7 / 8/ 10  Пакет прикладных программ Microsoft Office 2013/2016/2019  Браузеры Google Chrome, Яндекс, Opera. Свободно распространяемое ПО  Редактор диаграмм, схем, блок-схем, UML-схем Dia 0.97.2. Свободно распространяемое ПО  ОС Android или его эмулятор |
| Лекционные занятия | Операционная система Microsoft Windows XP / Professional 7 / 8/ 10  Пакет прикладных программ Microsoft Office 2013/2016/2019  Браузеры Google Chrome, Яндекс, Opera. Свободно распространяемое ПО |
| Самостоятельная работа | Операционная система Microsoft Windows XP / Professional 7 / 8/ 10  Пакет прикладных программ Microsoft Office 2013/2016/2019  Браузеры Google Chrome, Яндекс, Opera. Свободно распространяемое ПО |

1. **ПАСПОРТ КОМПЕТЕНЦИИ**

**Кибербезопасность и защита данных**

**ФГБОУ ВО "Тульский государственный педагогический университет им. Л.Н. Толстого"**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Обслуживание средств защиты информации прикладного и системного программного обеспечения | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональ ная |  | |
| профессиональная |  | |
| профессионально-специализированная | профессионально-специализированная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Под компетенцией понимается способность обслуживать средства защиты информации в компьютерных системах и сетях.  Слушатель должен:  знать:  - источники угроз информационной безопасности и меры по их предотвращению;  - особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения;  - уязвимости компьютерных систем и сетей;  - принципы работы и правила эксплуатации программно-аппаратных средств защиты данных.  Уметь:  - ориентироваться в современных угрозах и факторах риска в условиях цифровой трансформации общества и государства;  - противодействовать угрозам кибербезопасности с использованием аппаратных и программных средств защиты информации;  - работать с программным обеспечением с соблюдением действующих требований по защите информации;  владеть:  - навыками безопасного использования технических и программных средств защиты информации;  - навыками настройки программного обеспечения с соблюдением требований по защите информации;  - навыками проверки функционирования встроенных средств защиты информации программного обеспечения; | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень | Знает:  некоторые источники угроз информационной безопасности;  частично источники угроз информационной безопасности, связанные с эксплуатацией программного обеспечения;  Умеет:  интуитивно ориентироваться в современных угрозах и факторах риска в условиях цифровой трансформации общества и государства;  владеет:  навыками безопасного использования некоторых технических и программных средств защиты информации; |
|  | | Базовый уровень | Знает:  особенности источников угроз информационной безопасности, связанные с эксплуатацией программного обеспечения;  некоторые уязвимости компьютерных систем и сетей;  Умеет:  ориентироваться в современных угрозах и факторах риска в условиях цифровой трансформации общества и государства;  работать с программным обеспечением с соблюдением действующих требований по защите информации в условиях неопределенности;  владеет:  навыками безопасного использования некоторых технических и программных средств защиты информации в ситуациях повышенной сложности;  навыками настройки некоторого программного обеспечения с соблюдением требований по защите информации; |
|  | | Продвинутый | знает:  - источники угроз информационной безопасности и меры по их предотвращению в ситуациях повышенной сложности ;  - особенности источников угроз информационной безопасности, связанные с эксплуатацией программного обеспечения;  - уязвимости компьютерных систем и сетей в ситуациях повышенной сложности;  - принципы работы и правила эксплуатации программно-аппаратных средств защиты данных.  Умеет:  - работать с программным обеспечением с соблюдением действующих требований по защите информации;  владеет:  - навыками настройки программного обеспечения с соблюдением требований по защите информации; |
|  | | Профессиональный | знает:  - уязвимости компьютерных систем и сетей в ситуациях повышенной сложности;  Умеет:  - противодействовать угрозам кибербезопасности с использованием аппаратных и программных средств защиты информации для сложных проблем со многими взаимодействую-щими факторами;  владеет:  - навыками настройки программного обеспечения с соблюдением требований по защите информации для решения сложных проблем со многими факторами;  - навыками проверки функционирования встроенных средств защиты информации программного обеспечения. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенции цифровой грамотности | |
| 6. | Средства и технологии оценки | | Тестирование, выполнение практических заданий по программе | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Проведение анализа безопасности компьютерных систем | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональ ная |  | |
| профессиональная | профессиональная | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Под компетенцией понимается способность оценивать и проводить анализ угроз и уровня безопасности компьютерных систем и сетей  Слушатель должен:  знать:  - основные понятия кибербезопасности, информационной безопасности и персональных данных;  - сущность и содержание понятия информационной безопасности, характеристики ее составляющих;  - правовые основы обеспечения кибербезопасности;  Уметь:  - описывать риски и угрозы персональных данных;  - оценивать эффективность защиты данных.  владеть:  - навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем;  - навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень | Знает:  - некоторые понятия кибербезопасности, информационной безопасности;  Умеет:  - описывать на интуитивном уровне риски и угрозы персональных данных;  владеет:  - некоторыми навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; |
|  | | Базовый уровень | знает:  - основные понятия кибербезопасности, некоторые понятия информационной безопасности;  - сущность понятия информационной безопасности;  Умеет:  - описывать риски и угрозы персональных данных в ситуациях с элементами неопределённости ;  владеет:  - навыками оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем в сложных ситуациях; |
|  | | Продвинутый | знает:  - сущность и содержание понятия информационной безопасности;  - правовые основы обеспечения кибербезопасности;  Умеет:  - описывать риски и угрозы персональных данных в ситуациях повышенной сложности;  владеет:  - навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; |
|  | | Профессиональный | знает:  - сущность и содержание понятия кибербезопасности, информационной безопасности, характеристики ее составляющих;  Умеет:  - описывать риски и угрозы персональных данных для решения проблем со многими взаимодействую-щими факторами;  - оценивать эффективность защиты данных;  владеет:  - навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети, предлагает новые идеи и процессы; |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенции цифровой грамотности | |
| 6. | Средства и технологии оценки | | Тестирование, выполнение практических заданий по программе | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональ ная |  | |
| профессиональная |  | |
| профессионально-специализированная | Профессионально-специализированная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Под компетенцией понимается способность разрабатывать требования и политику информационной безопасности компьютерных систем и сетей, в том числе биометрическими системами защиты данных  Слушатель должен:  знать:  - нормативные правовые акты в области защиты информации;  - организационные, технические и правовые меры по защите информации;  - основные понятия о биометрических системах защиты данных;  Уметь:  - формулировать принципы и строить модель угроз и нарушителей по методике ФСТЭК;  - формулировать и проектировать политику информационной безопасности организации (предприятия);  владеть:  - навыками работы с биометрическими системами идентификации и аутентификации;  - навыками разработки модели угроз безопасности информации для политики безопасности;  - заданием требований к защите информации компьютерной системы в политике безопасности; | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень | знает:  - некоторые нормативные правовые акты в области защиты информации;  Умеет:  - частично формулировать угрозы информационной безопасности;  владеет:  - навыками практической работы с биометрическими системами идентификации; |
|  | | Базовый уровень | знает:  - нормативные правовые акты в области защиты информации;  Умеет:  - формулировать и проектировать политику информационной безопасности организации в ситуациях с элементами неопределённости;  владеет:  - навыками работы с биометрическими системами идентификации и аутентификации; |
|  | | Продвинутый | знает:  - основные понятия о биометрических системах защиты данных;  Умеет:  - формулировать и проектировать политику информационной безопасности организации в ситуациях повышенной сложности;  владеет:  - навыками задания требований к защите информации компьютерной системы в политике безопасности; |
|  | | Профессиональный | знает:  - организационные, технические и правовые меры по защите информации;  Умеет:  - формулировать принципы и строить модель угроз и нарушителей по методике ФСТЭК;  владеет:  - навыками разработки модели угроз безопасности информации для политики безопасности в ситуациях повышенной сложности. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенции цифровой грамотности | |
| 6. | Средства и технологии оценки | | Тестирование, выполнение практических заданий по программе | |

1. **ВОЗМОЖНЫЕ СЦЕНАРИИ ПРОФЕССИОНАЛЬНОЙ ТРАЕКТОРИИ ГРАЖДАН ПО ИТОГАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

**Сценарии профессиональной траектории граждан**

|  |  |
| --- | --- |
| **Цели получения персонального цифрового сертификата** | |
| **текущий статус** | **цель** |
| **Трудоустройство** | |
| состоящий на учете в Центре занятости | трудоустроенный |
| безработный |
| **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 |
| **Переход в новую сферу занятости** | |
| освоение новой сферы занятости | расширение кругозора |
| освоение смежных профессиональных областей | повышение уровня дохода, расширение профессиональной деятельности |

1. **ПРИЛОЖЕННЫЕ СКАН-КОПИИ**

* Утвержденная образовательная программа
* Утвержденный паспорт образовательной программы
* Рекомендательные письма от работодателей

Проректор по НИР \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ К.А. Подрезов

МП