1. **Паспорт Образовательной программы**

**«Основы информационной безопасности. Начальный уровень»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | **06.10.2020** |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | АНО ДПО «Центральный учебный центр» |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 7719435821 |
| 1.4 | Ответственный за программу ФИО | Безценная Юлия Евгеньевна |
| 1.5 | Ответственный должность | Руководитель по направлению «Цифровая экономика» |
| 1.6 | Ответственный Телефон | 89600567469 |
| 1.7 | Ответственный Е-mail | bezcennaja@mail.ru |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Основы информационной безопасности. Начальный уровень. |
| 2.2 | Ссылка на страницу программы | https://kursi.pro/product/osnovy-informacionnoy-bezopasnosti-nachalnyy-uroven |
| 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 | <https://online.kursi.pro/account/login> |
| 2.4 | Уровень сложности | Начальный |
| 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) | Практические занятия: 33  Самостоятельная работа: 32 |
| 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 | 10000 руб.  1) <https://www.specialist.ru/course/setibez>  2) <https://edu.softline.com/vendors/softline/osnovy-informacionnoj-bezopasnosti/>  3) https://academy.ru/catalog/security/IS-1.0.html |
| 2.7 | Минимальное количество человек на курсе | 100 |
| 2.8 | Максимальное количество человек на курсе | 999 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 47 |
| 2.10 | Формы аттестации | Удостоверение |
|  | 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**

В результате освоения Программы слушатель должен:

**знать:** виды мошенничества в интернете и способы борьбы с ними; как работают вирусы и как бороться с ними; основные типы алгоритмов (работы с различными структурами данных, базовые алгоритмы на графах, алгоритмы организации перебора и динамического программирования, целочисленной арифметики, моделирования, компьютерной геометрии); понятие сложности алгоритмов при решении задач; методы современных технологий программирования, отладки и тестирования программ;

**уметь:** защищать свои данные и свое личное информационное пространство; распознавать виды мошенничества в интернете и противостоять им; находить слабые места в программах и системах, чтобы защитить их от угроз; составлять алгоритмические конструкции для различных исполнителей;

**иметь навыки:** записи символов и ключевых слов языка программирования; записи числовых и логических констант, определения и описания переменных; описания типа и размерности массивов; составления математической модели, алгоритма и программы для решения задач.

К освоению программы допускаются физические лица, имеющие или получающие высшее образование или среднее профессиональное образование.

Результатами подготовки по Программе является повышение уровня профессиональной квалификации слушателей за счет освоения ими способов доступа к конфиденциальной информации и технологиям ее защиты, используя базовые алгоритмы шифрования информации и защиты каналов связи; способов предотвращения утечек данных в информационном поле (веб-сайтов, сетевых сервисов, криптографических шифров и современных операционных систем).

1. **Дополнительная образовательная программа**

**Автономная некоммерческая организация дополнительного профессионального образования**

**«Центральный учебный центр»**

**(АНО ДПО «ЦУЦ»)**

|  |  |
| --- | --- |
|  | **УТВЕРЖДЕНО**  Директор  АНО ДПО «ЦУЦ» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Т.Р. Мустаев/  Приказ № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

**Дополнительная профессиональная программа**

**повышения квалификации**

**«Основы информационной безопасности. Начальный уровень»**

|  |
| --- |
| (наименование программы) |

72 часа

|  |
| --- |
| дополнительное профессиональное образование |
| (подвид дополнительного образования) |

г. Москва 2020

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Целью подготовки слушателей является повышение квалификации заинтересованных лиц в условиях инновационного процесса цифровизации различных сфер жизни за счет освоения способов доступа к конфиденциальной информации и технологиям ее защиты, используя базовые алгоритмы шифрования информации и защиты каналов связи в информационном поле (веб-сайтов, сетевых сервисов, криптографических шифров и современных операционных систем).

**2.Планируемые результаты обучения:**

2.1. Знание (осведомленность в областях)

2.1.1. виды мошенничества в интернете и способы борьбы с ними;

2.1.2. как работают вирусы и как с ними бороться;

2.1.3. основные типы алгоритмов (работы с различными структурами данных, базовые алгоритмы на графах, алгоритмы организации перебора и динамического программирования, целочисленной арифметики, моделирования, компьютерной геометрии);

2.1.4. понятие сложности алгоритмов при решении задач;

2.1.5. методы современных технологий программирования, отладки и тестирования программ.

2.2. Умение (способность к деятельности)

2.2.1. защищать свои данные и своё личное информационное пространство;

2.2.2. распознавать виды мошенничества в интернете и противостоять им;

2.2.3. находить слабые места в программах и системах, чтобы защитить их от угроз;

2.2.4. создавать алгоритмические конструкции для различных исполнителей.

2.3. Навыки (использование конкретных инструментов)

2.3.1. записи символов и ключевых слов языка программирования;

2.3.2. записи числовых и логических констант, определения и описания переменных;

2.3.3. описание типа и размерности массивов;

2.3.4. составление математической модели, алгоритма и программы для решения задач.

**3.Категория слушателей**

* 1. Образование: высшее или среднее профессиональное

**4.Учебный план программы «Основы информационной безопасности. Начальный уровень»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Введение в информационную безопасность | 4 | 1 | 2 | 1 |
| 1.1. | Что такое информационная безопасность и где она применяется; основные составляющие информационной безопасности; определение угроз. | 4 | 1 | 2 | 1 |
| 2 | Современное применение средств криптографической защиты информации | 6 | 1 | 3 | 2 |
| 2.2. | История появления; простейшие шифры (скитала, атбаш, шифры простой замены, шифры сдвига, шифр Полибия, шифр Виженера и т.д.). | 6 | 1 | 3 | 2 |
| 3 | Cтеганография | 8 | 1 | 4 | 3 |
| 3.1. | Появление, значимость; классическая стеганография; цифровая стеганография: как спрятать информацию, передаваемую на электронных носителях. | 4 | 1 | 2 | 1 |
| 3.2. | Практический блок с задачами на сокрытие информации в тексте (несколько форматов), звуке (спектр, специализированное ПО), видео (вариативные варианты); примеры сетевой стеганографии. | 4 |  | 2 | 2 |
| 4 | Сетевые технологии | 8 | 1 | 4 | 3 |
| 4.1. | Что такое сеть и из чего она состоит; определение модели OSI.; стек протоколов TCP/IP. | 4 | 1 | 2 | 1 |
| 4.2. | Примеры атак на канальном уровне; примеры атак на транспортном уровне; примеры атак на сетевом уровне. | 4 |  | 2 | 2 |
| 5 | Операционные системы | 6 | 1 | 2 | 3 |
| 5.1. | Обзор архитектуры систем Linux; уязвимости в современных ОС; Построение защищённой системы. | 6 | 1 | 2 | 3 |
| 6 | Современные уязвимости | 8 |  | 4 | 4 |
| 6.1. | АСУТП; Блокчейн; Облачные сервисы. | 8 |  | 4 | 4 |
| 7 | Основы сетевого взаимодействия | 8 |  | 4 | 4 |
| 7.1. | модель OSI; Построение дерева атаки; технологии защиты от сетевых атак; Построение защищённой сети. | 8 |  | 4 | 4 |
| 8. | Аудит информационной безопасности | 10 |  | 4 | 6 |
| 8.1. | Аудит защищённости сетевых служб; Аудит сервисов операционных систем | 10 |  | 4 | 6 |
| 9. | Технологии защиты от атак | 12 |  | 6 | 6 |
| 9.1. | Проведение атаки на существующую инфраструктуру; Отражение атаки на построенной архитектуре. | 12 |  | 6 | 6 |
| **Итоговая аттестация** | | **2** | **Зачёт** | | |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1. | Введение в информационную безопасность | 4 | 01.10.2020-02.10.2020 |
| 2. | Современное применение средств криптографической защиты информации | 6 | 03.10.2020-04.10.2020 |
| 3. | Cтеганография | 8 | 05.10.2020-07.10.2020 |
| 4. | Сетевые технологии | 8 | 08.10.2020-10.10.2020 |
| 5. | Операционные системы | 6 | 11.10.2020-12.10.2020 |
| 6. | Современные уязвимости | 8 | 13.10.2020-15.10.2020 |
| 7. | Основы сетевого взаимодействия | 8 | 16.10.2020-18.10.2020 |
| 8. | Аудит информационной безопасности | 10 | 19.10.2020-21.10.2020 |
| 9. | Технологии защиты от атак | 12 | 22.10.2020-24.10.2020 |
| 10. | Итоговая аттестация | 2 |  |
| **Всего:** | | **72** |  |

**6.Учебно-тематический план программы «Основы информационной безопасности. Начальный уровень»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Введение в информационную безопасность | 4 | 1 | 2 | 1 | Самоконтроль |
| 1.1. | что такое информационная безопасность и где она применяется; основные составляющие информационной безопасности; определение угроз. | 4 | 1 | 2 | 1 | Самоконтроль |
| 2 | Современное применение средств криптографической защиты информации | 6 | 1 | 3 | 2 | Самоконтроль |
| 2.2. | История появления; простейшие шифры (скитала, атбаш, шифры простой замены, шифры сдвига, шифр Полибия, шифр Виженера и т.д.). | 6 | 1 | 3 | 2 | Самоконтроль |
| 3 | Cтеганография | 8 | 1 | 4 | 3 | Самоконтроль |
| 3.1. | Появление, значимость; классическая стеганография; цифровая стеганография: как спрятать информацию, передаваемую на электронных носителях. | 4 | 1 | 2 | 1 | Самоконтроль |
| 3.2. | Практический блок с задачами на сокрытие информации в тексте (несколько форматов), звуке (спектр, специализированное ПО), видео (вариативные варианты); примеры сетевой стеганографии. | 4 |  | 2 | 2 | Самоконтроль |
| 4 | Сетевые технологии | 8 | 1 | 4 | 3 | Самоконтроль |
| 4.1. | Что такое сеть и из чего она состоит; определение модели OSI.; стек протоколов TCP/IP. | 4 | 1 | 2 | 1 | Самоконтроль |
| 4.2. | Примеры атак на канальном уровне; примеры атак на транспортном уровне; примеры атак на сетевом уровне. | 4 |  | 2 | 2 | Самоконтроль |
| 5 | Операционные системы | 6 | 1 | 2 | 3 | Самоконтроль |
| 5.1. | Обзор архитектуры систем Linux; уязвимости в современных ОС; Построение защищённой системы. | 6 | 1 | 2 | 3 | Самоконтроль |
| 6 | Современные уязвимости | 8 |  | 4 | 4 | Самоконтроль |
| 6.1. | АСУТП; Блокчейн; Облачные сервисы. | 8 |  | 4 | 4 | Самоконтроль |
| 7 | Основы сетевого взаимодействия | 8 |  | 4 | 4 | Самоконтроль |
| 7.1. | модель OSI; Построение дерева атаки; технологии защиты от сетевых атак; Построение защищённой сети. | 8 |  | 4 | 4 | Самоконтроль |
| 8. | Аудит информационной безопасности | 10 |  | 4 | 6 | Самоконтроль |
| 8.1. | Аудит защищённости сетевых служб; Аудит сервисов операционных систем | 10 |  | 4 | 6 | Самоконтроль |
| 9. | Технологии защиты от атак | 12 |  | 6 | 6 | Самоконтроль |
| 9.1. | Проведение атаки на существующую инфраструктуру; Отражение атаки на построенной архитектуре. | 12 |  | 6 | 6 | Самоконтроль |
| 10 | Итоговая аттестация | 2 |  |  |  | Текущий контроль |

**7. Учебная (рабочая) программа повышения квалификации «Основы информационной безопасности. Начальный уровень»**

**Модуль 1. Введение в информационную безопасность (4 час.)**

Что такое информационная безопасность и где она применяется.

**Модуль 2. Современное применение средств криптографической защиты информации (6 час.)**

История появления средств криптографии, а также возможности их применения.

**Модуль 3. Cтеганография (8 час.)**

Появление, значимость; классическая стеганография; цифровая стеганография: как спрятать информацию, передаваемую на электронных носителях.

**Модуль 4. Сетевые технологии (8 час.)**

Что такое сеть и из чего она состоит; определение модели OSI.; стек протоколов TCP/IP.

**Модуль 5. Операционные системы (6 час.)**

Обзор архитектуры систем Linux

**Модуль 6. Современные уязвимости (8 час.)**

Что такое информационная безопасность и где она применяется.

**Модуль 7. Основы сетевого взаимодействия (8 час.)**

Что такое информационная безопасность и где она применяется.

**Модуль 8. Аудит информационной безопасности (10 час.)**

Что такое информационная безопасность и где она применяется.

**Модуль 9. Технологии защиты от атак (12 час.)**

Что такое информационная безопасность и где она применяется.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование практического занятия** | **Описание** |
| **1.** | Введение в информационную безопасность | Основные составляющие информационной безопасности; определение угроз |
| **2.** | Современное применение средств криптографической защиты информации | Простейшие шифры (скитала, атбаш, шифры простой замены, шифры сдвига, шифр Полибия, шифр Виженера и т.д.). |
| **3.** | Cтеганография | Практический блок с задачами на сокрытие информации в тексте (несколько форматов), звуке (спектр, специализированное ПО), видео (вариативные варианты); примеры сетевой стеганографии. |
| **4.** | Сетевые технологии | Примеры атак на канальном уровне; примеры атак на транспортном уровне; примеры атак на сетевом уровне. |
| **5.** | Операционные системы | Уязвимости в современных ОС; Построение защищённой системы. |
| **6.** | Современные уязвимости | АСУТП; Блокчейн; Облачные сервисы. |
| **7.** | Основы сетевого взаимодействия | Модель OSI; Построение дерева атаки; технологии защиты от сетевых атак; Построение защищённой сети. |
| **8.** | Аудит информационной безопасности | Аудит защищённости сетевых служб; Аудит сервисов операционных систем |
| **9.** | Технологии защиты от атак | Проведение атаки на существующую инфраструктуру; Отражение атаки на построенной архитектуре. |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования**

|  |  |  |
| --- | --- | --- |
| **№** | **Вопросы входного тестирования** | **Вопросы итогового тестирования** |
| 1. | Под информационной безопасностью понимается…  А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.  Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия  В) нет правильного ответа | Охарактеризуйте технологии IPS/IDS,WAF,SIEM,IRP; перечислите способы настройки этих систем. |
| 2. | Защита информации – это..  А) комплекс мероприятий, направленных на обеспечение информационной безопасности.  Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей  В) небольшая программа для выполнения определенной задачи | 1. Перечислите методы обнаружения атак и типичные ошибки, допускаемые злоумышленниками |
| 3. | От чего зависит информационная безопасность?  А) от компьютеров  Б) от поддерживающей инфраструктуры  В) от информации | Перечислите способы обнаружения типичных ошибок, допускаемых злоумышленниками |
| 4. | Основные составляющие информационной безопасности:  А) целостность  Б) достоверность  В) конфиденциальность | Что такое Модель OSI |
| 5. | Доступность – это…  А) возможность за приемлемое время получить требуемую информационную услугу.  Б) логическая независимость  В) нет правильного ответа | Как построить дерево атаки |
| 6. | Целостность – это..  А) целостность информации  Б) непротиворечивость информации  В) защищенность от разрушения | Что из себя представляет программа WireShark |
| 7. | Конфиденциальность – это..  А) защита от несанкционированного доступа к информации  Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов  В) описание процедур | Сделать обзор по последним новостям в сфере информационной безопасности по конкретному инциденту, указав кто подвергся атаке, тип атаки, нанесенный ущерб, дата атаки |
| 8. | Целостность можно подразделить:  А) статическую  Б) динамичную  В) структурную | Провести атаку на сервис (веб-сайт), расписать шаги, ход атаки, добыть критические данные, составить отчет |
| 9. | Угроза – это…  А) потенциальная возможность определенным образом нарушить информационную безопасность  Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных  В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа |  |
| 10. | Атака – это…  А) попытка реализации угрозы  Б) потенциальная возможность определенным образом нарушить информационную безопасность  В) программы, предназначенные для поиска необходимых программ. |  |

**8.2.**  **Описание показателей и критериев оценивания, шкалы оценивания.**

Контроль знаний, полученных слушателями при освоении разделов (модулей) Программы, осуществляется в следующих формах:

- контроль знаний (входное тестирование) – оценивает уровня знаний слушателя, необходимых для освоения разделов Программы;

- итоговая аттестация – завершает изучение всей Программы. Итоговая аттестация проводится в форме выполнения заданий контрольного теста, демонстрирующего освоение слушателем всех изученных разделов Программы.

**8.3.**  **Примеры контрольных заданий по модулям или всей образовательной программе.**

Программой предусмотрена итоговая оценка знаний, которая осуществляется посредством итогового тестирования. Слушатели, ответившие верно более, чем на 80% вопросов, считаются успешно прошедшими Программу.

**8.4.** Программой предусмотрено решение индивидуальных обучающих задач по выбранному слушателем направлению.

**8.5.** Слушатели, успешно выполнившие все элементы учебного плана, допускаются к итоговой аттестации. Итоговая аттестация по Программе проводится в форме выбора варианта ответа на вопросы контрольного теста. Программа считается успешно пройденной если Слушатель набирает 80% правильных результатов.

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть Программы и (или) отчисленным с АНО ДПО «ЦУЦ», выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому АНО ДПО «ЦУЦ».

**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 | Сабиров Тимур Марсович | АНО ДПО «ЦУЦ», преподаватель-методист |  |  | Да |
| 2 | Потопахин Виталий Валерьевич | АНО ДПО «ЦУЦ», Методист по информатике и искусственному интеллекту высшей квалификационной категории. Лауреат премии правительства РФ. | https://www.dvhab.ru/sections/trainer/potopahin-vitaliy-valeryevich |  | Да |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| **Методы, формы и технологии** | **Методические разработки,**  **материалы курса, учебная литература** |
| Данная программа предполагает использование активного метода обучения | Спицын, В. Г. Информационная безопасность вычислительной техники: учебное пособие / В. Г. Спицын. — Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 148 c. — ISBN 978-5-4332-0020-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/13936.html |
| Очная групповая онлайн форма обучения, когда каждый ее участник имеет возможность высказать свое мнение или предложить свое решение всем остальным участникам, услышать их мнение и вместе со всеми выработать единое для этой творческой группы решение. | Национальная система раннего предупреждения о компьютерном нападении Number: 815 Author: Петренко С. А., Ступин Д. Д. Publishing House: ООО «ИД «Афина» - 2017. – 440 с. |
| Технологии:  Обучение производится с помощью учебной платформы Uchi.pro (лекционный материал), Zoom (практические работы), YouTube (вебинары) | Петров, В.Ю. Информатика. Алгоритмизация и программирование. Учебное пособие. Часть 1 [Электронный ресурс]: учеб. пособие — Электрон. дан. — Санкт-Петербург: НИУ ИТМО, 2016. — 91 с. — Режим доступа: https://e.lanbook.com/book/91533 |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| **Электронные**  **образовательные ресурсы** | **Электронные**  **информационные ресурсы** |
| https://academiait.ru/course/informatsionnaya-bezopasnost-2/ | Кубенский, А.А. Функциональное программирование [Электронный ресурс]: учеб.-метод. пособие — Электрон. дан. — Санкт-Петербург : НИУ ИТМО, 2010. — 251 с. — Режим доступа: https://e.lanbook.com/book/40771 |
| https://www.edx.org/learn/cybersecurity | Тюгашев, А.А. Основы программирования. Часть I [Электронный ресурс] : учебное пособие / А.А. Тюгашев. — Электрон. дан. — Санкт-Петербург : НИУ ИТМО, 2016. — 160 с. — Режим доступа: https://e.lanbook.com/book/91469 |
| https://www.cyberdegrees.org/resources/free-online-courses/#Popular\_Cyber\_Security\_MOOCs | Фарафонов, А. С. Программирование на языке высокого уровня: методические указания к проведению лабораторных работ по курсу «Программирование» / А. С. Фарафонов. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2013. — 32 c.— Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/22912.html |
| https://school.codeby.net/ |  |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекционные занятия | * Компьютер с выходом в интернет, минимальные требования: 1600 МГц процессор, 4 Гб RAM, 50 Гб места на жестком диске (или флэш-карты, карты памяти или внешнего жесткого диска, * VGA и разрешение экрана 1024x768, CD/DVD-дисковод или USB-порт для запуска программы установки. |
| Практические занятия |
| Самостоятельная работа |

**III. Паспорт компетенций (Приложение 2)**

**ПАСПОРТ КОМПЕТЕНЦИИ**

**Дополнительная профессиональная программа**

**(программа повышения квалификации)**

**«Основы информационной безопасности. Начальный уровень»**

**Автономная некоммерческая организация дополнительного профессионального образования**

**«Центральный учебный центр»**

**(АНО ДПО «ЦУЦ»)**

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Наименование компетенции | **ПК-1.** Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. | |
| 2 | Указание типа компетенции | Профессиональная | |
| 3 | Определение, содержание и основные сущностные характеристики компетенции | Под компетенцией ПК-1 понимается Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.  Слушатель должен:  **Знать:**  - архитектуру и пользовательские интерфейсы операционных систем;  -порядок обеспечения безопасности информации при эксплуатации операционных систем;  -источники угроз информационной безопасности и меры по их предотвращению;  - сущность и содержание понятия информационной безопасности, характеристика ее составляющих;  - типовые средства защиты информации в операционных системах;  - программно-аппаратные средства и методы защиты информации;  **Уметь:**  - применять программно-аппаратные средства защиты информации в операционных системах;  - применять антивирусные средства защиты информации в операционных системах;  - проводит мониторинг, анализ и сравнение эффективности программно-аппаратные средства защиты информации в операционных системах;  - контролировать целостность подсистем защиты информации операционных систем;  -устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации.  **Владеть:**  Навыками ввода в эксплуатацию программно-аппаратных средств защиты информации в операционных системах;  Навыками проверки корректности работы программно-аппаратных средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;  Навыками обслуживания программно-аппаратных средств защиты информации в операционных системах. | |
| 4 | Дескриптор знаний, умений и навыков по уровням | Уровни сформированности компетенции обучающегося | Индикаторы |
|  |  | Начальный уровень | Знать: о мерах по поддержанию в работоспособном состоянии СЗИ.  Уметь: определять условия функционирования СЗИ.  Владеть: базовыми навыками работы с СЗИ. |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Перечислены основы для формирования компетенции ПК-1:  Для формирования данной компетенции необходимо обладать следующими компетенциями на начальном уровне:  ОК-5, ОК-8, ОПК-4, ОПК-7 | |
| 6 | Средства и технологии оценки | итоговая аттестация | |

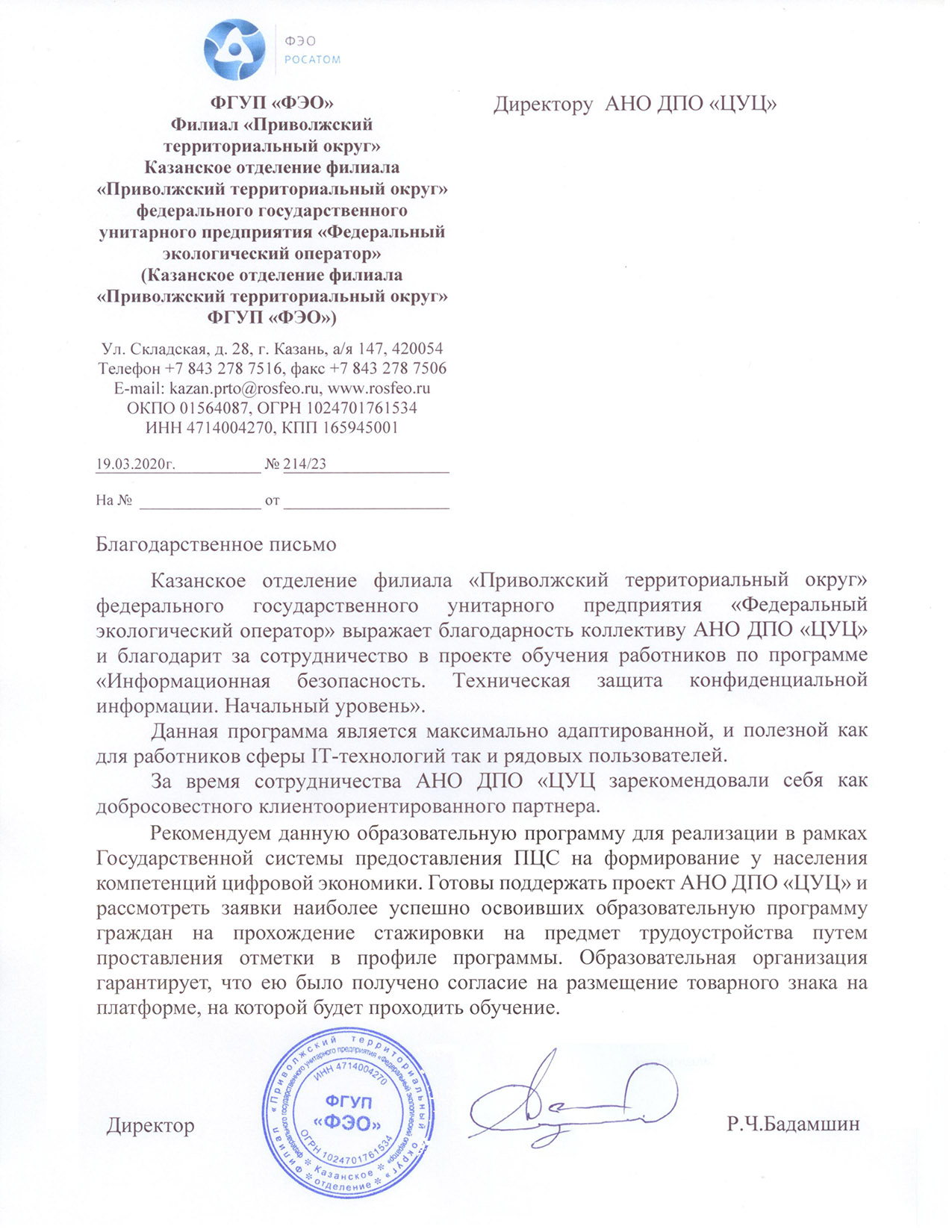
|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Наименование компетенции | **ОПК-4.** Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации. | |
| 2 | Указание типа компетенции | Общепрофессиональная | |
| 3 | Определение, содержание и основные сущностные характеристики компетенции | Под компетенцией понимается способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.  У выпускника должны быть сформированы следующие компетенции на базовом уровне:  **Знать:** аспекты применения информационных технологий с позиций научно-исследовательской и правовой деятельностей; типовые алгоритмы обработки данных; структуры данных, используемые для представления типовых информационных объектов  **Уметь:** применять математические методы для решения задач с использованием стандартных программных средств  **Владеть:** навыками применения стандартных программных средств; компьютером как средством управления информацией | |
| 4 | Дескриптор знаний, умений и навыков по уровням | Уровни сформированности компетенции обучающегося | Индикаторы |
|  |  | Начальный уровень | **Знать:** аспекты применения информационных технологий с позиций научно-исследовательской и правовой деятельностей; типовые алгоритмы обработки данных; структуры данных, используемые для представления типовых информационных объектов  **Уметь:** применять математические методы для решения задач с использованием стандартных программных средств  **Владеть:** навыками применения стандартных программных средств; компьютером как средством управления информацией |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Перечислены основы для формирования компетенции ОПК-4:  Для формирования данной компетенции необходимо обладать следующими компетенциями на начальном уровне: ОК-5, ОК-8, ОПК-7 | |
| 6 | Средства и технологии оценки | итоговая аттестация | |

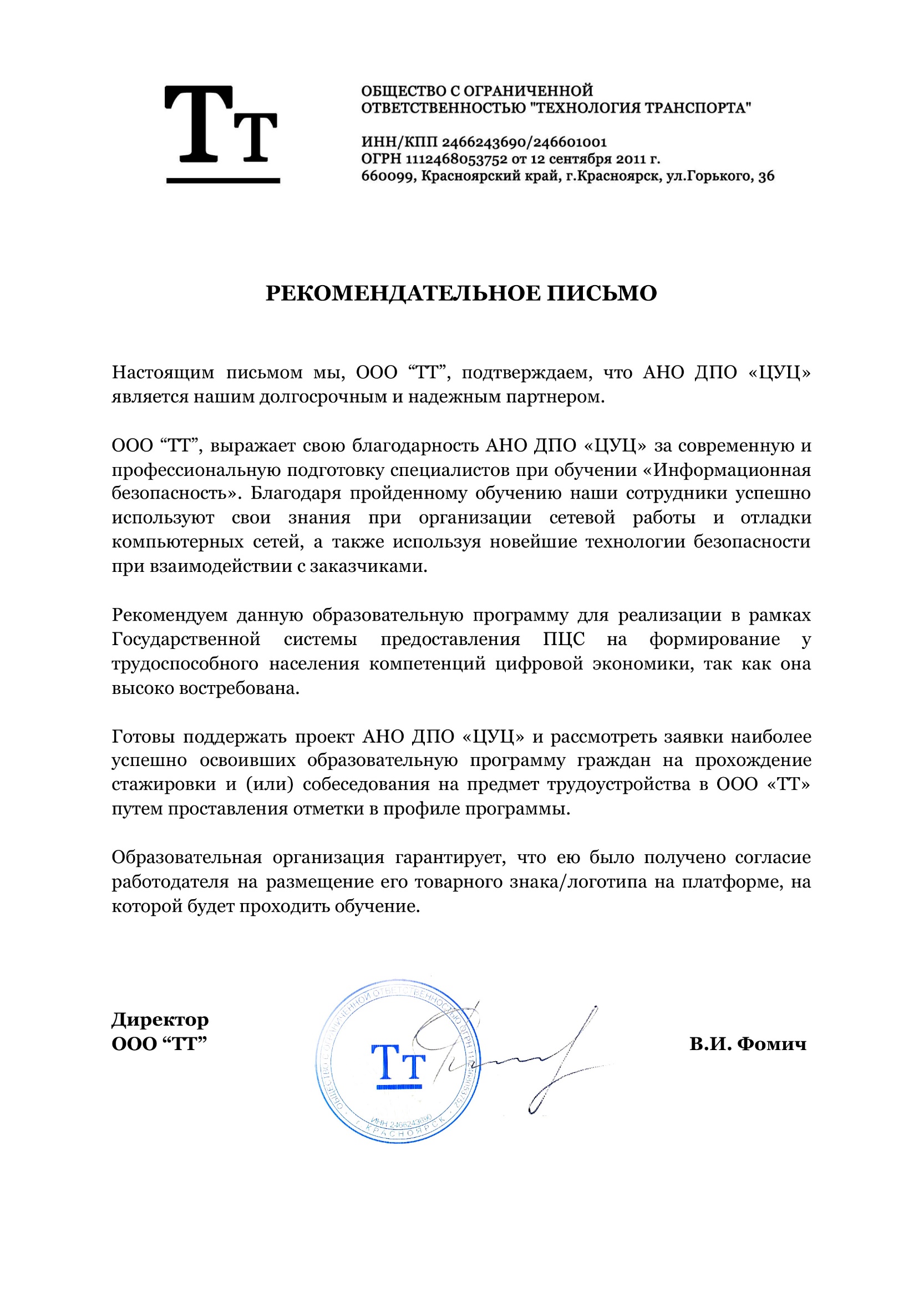
|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Наименование компетенции | **ОПК-7.** Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты | |
| 2 | Указание типа компетенции | Общепрофессиональная | |
| 3 | Определение, содержание и основные сущностные характеристики компетенции | Под компетенцией понимается способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.  У выпускника должны быть сформированы следующие компетенции на базовом уровне:  **Знать:** основные угрозы безопасности информации и модели нарушителя в информационных системах; методики анализа рисков; программные средства анализа и управления рисками.  **Уметь:** проводить классификацию критичных информационных ресурсов; анализировать и оценивать информационные риски; разрабатывать модели угроз и нарушителей информационной безопасности  **Владеть:** методами оценки информационных рисков. | |
| 4 | Дескриптор знаний, умений и навыков по уровням | Уровни сформированности компетенции обучающегося | Индикаторы |
|  |  | Начальный уровень | **Знать:** основные угрозы безопасности информации и модели нарушителя в информационных системах; методики анализа рисков; программные средства анализа и управления рисками.  **Уметь:** проводить классификацию критичных информационных ресурсов; анализировать и оценивать информационные риски; разрабатывать модели угроз и нарушителей информационной безопасности  **Владеть:** методами оценки информационных рисков. |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Для формирования данной компетенции необходимо обладать следующими компетенциями на начальном уровне:  ОК-5, ОК-8, ОПК-4 | |
| 6 | Средства и технологии оценки | итоговая аттестация | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Наименование компетенции | **ОК-5.** Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | |
| 2 | Указание типа компетенции | Общекультурная | |
| 3 | Определение, содержание и основные сущностные характеристики компетенции | Под компетенцией понимается способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.  У выпускника должны быть сформированы следующие компетенции на базовом уровне:  **Уметь:** Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом криптографических средств защиты информации; Применять отечественные и зарубежные стандарты в области компьютерной безопасности с использованием криптографических средств обеспечения информационной безопасности.  **Владеть:** Профессиональной терминологией и методами теоретического обоснования в выборе криптографических средств обеспечения информационной безопасности; методологическим и принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты с использованием криптографических средств обеспечения информационной безопасности. | |
| 4 | Дескриптор знаний, умений и навыков по уровням | Уровни сформированности компетенции обучающегося | Индикаторы |
|  |  | Начальный уровень | **Уметь:** Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом криптографических средств защиты информации; Применять отечественные и зарубежные стандарты в области компьютерной безопасности с использованием криптографических средств обеспечения информационной безопасности.  **Владеть:** Профессиональной терминологией и методами теоретического обоснования в выборе криптографических средств обеспечения информационной безопасности; методологическим и принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты с использованием криптографических средств обеспечения информационной безопасности. |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Перечислены основы для формирования компетенции ОК-5:  Для формирования данной компетенции необходимо обладать следующими компетенциями на начальном уровне: ОК-8, ОПК-4, ОПК-7. | |
| 6 | Средства и технологии оценки | итоговая аттестация | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Наименование компетенции | **ОК-8**. Способность к самоорганизации и самообразованию. | |
| 2 | Указание типа компетенции | Общекультурная | |
| 3 | Определение, содержание и основные сущностные характеристики компетенции | Под компетенцией понимается способность к самоорганизации и самообразованию.  У выпускника должны быть сформированы следующие компетенции на базовом уровне:  **Знать**: содержание процессов самоорганизации и самообразования, их особенности и технологии реализации, исходя из целей совершенствования  **Уметь:** планировать цели и устанавливать приоритеты при осуществлении деятельности;  **Владеть:** технологиями организации процесса самообразования и самоорганизации | |
| 4 | Дескриптор знаний, умений и навыков по уровням | Уровни сформированности компетенции обучающегося | Индикаторы |
|  |  | Начальный уровень | **Знать**: содержание процессов самоорганизации и самообразования, их особенности и технологии реализации, исходя из целей совершенствования  **Уметь:** планировать цели и устанавливать приоритеты при осуществлении деятельности;  **Владеть:** технологиями организации процесса самообразования и самоорганизации |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Перечислены основы для формирования компетенции ОК-8:  Для формирования данной компетенции необходимо обладать следующими компетенциями на начальном уровне: ОК-5, ОПК-4, ОПК-7. | |
| 6 | Средства и технологии оценки | итоговая аттестация | |

**IV. Рекомендации к программе от работодателей**





****

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

|  |  |
| --- | --- |
| **Цели получения персонального цифрового сертификата** | |
| **текущий статус** | **цель** |
| **Трудоустройство** | |
| Стоящий на учете в Центре занятости | Освоение программы подразумевает несколько вариантов трудоустройства:  Разработчик по направлению Информационная безопасность.  Аналитик Информационной безопасности. Знания и навыки, полученные на курсе, позволяют основы и составляющие инфраструктуры, обеспечивающей безопасность в компании.  Самозанятый (фриланс) – удаленная разработка ПО, обеспечивающего защиту персональных компьютеров и серверов. |
| Безработный |
| Безработный по состоянию здоровья |
| **Развитие компетенций в текущей сфере занятости** | |
| Работающий по найму в организации, на предприятии | Сохранение текущего рабочего места: развитие новых навыков в области информационной безопасности и понимание новейших принципов атак и информационных угроз, а также способов предотвращения и борьбы с ними позволит работающим по найму сотрудникам актуализировать знания по разработке, освоить новый стек технологий и соответствовать требованиям цифровой экономики к кадрам. |
| Работающий по найму в организации, на предприятии | Разработчикам и системным администраторам новый стек технологий позволит адаптировать инфраструктуру, обеспечивающую информационную безопасность с применением новейших антивирусных решений. Следовательно, позволит повысить защищенность информационных данных компании. |
| Работающий по найму в организации, на предприятии | Повышение заработной платы: развитие компетенций по новому стеку технологий, повышение универсальных, общепрофессиональных и профессиональных компетенций обеспечивает сотруднику его профессиональный рост. Исходя из этого, специалист, прошедший обучение «дорожает» на рынке труда и может рассчитывать на увеличение заработной платы на текущем предприятии. |
| Работающий по найму в организации, на предприятии | Смена работы без изменения сферы профессиональной деятельности: переход в более крупную компанию или компанию, расположенную в другом регионе или внутри компании с повышением заработной платы. |
| Временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.) | Прохождение обучения по программе способствует сохранению и развитию квалификации. Обеспечивает возможность соответствовать должностным требованиям в условиях быстро меняющейся цифровой среды. |
| **Переход в новую сферу занятости** | |
| Освоение новой сферы занятости | Прохождение обучения по программе способствует расширению кругозора. Самозанятым гражданам освоение нового стека технологий даст возможность выполнять заказы по разработке и тестированию ПО, обеспечивающего информационную безопасность. |
| Освоение смежных профессиональных областей | Освоить дополнительные профессиональные навыки:  Системным администраторам освоение нового стека технологий позволит обеспечить более качественную защиту информационной инфраструктуры на предприятии. |

**VIII. Приложенные Скан-копии**

<https://kursi.pro/storage/files/dpp-osnovy-inf-bezopasnosti.pdf>