1. **Паспорт Образовательной программы**

**«** Администрирование информационной безопасности **»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | 10.10.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Федеральное государственное бюджетное образовательное учреждение высшего образования "Пензенский государственный университет" |
| 1.2 | Логотип образовательной организации | C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.Word\LogPGU_simbioz2013 new.jpg |
| 1.3 | Провайдер ИНН | 5837003736 |
| 1.4 | Ответственный за программу ФИО | Лупанов Михаил Юрьевич |
| 1.5 | Ответственный должность | Доцент |
| 1.6 | Ответственный Телефон | 89603298384 |
| 1.7 | Ответственный Е-mail | lupanov@pnzgu.ru |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Администрирование информационной безопасности |
| 2.2 | Ссылка на страницу программы | <https://lk.pnzgu.ru/opop/spec/4255> |
| 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 | Наличие подтверждаем |
| 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) | Практикоориентированный характер образовательной программы 80% (58 час.) |
| 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 | 20000 руб.  Ссылки на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости:  <https://www.specialist.ru/course/m20744>  <https://www.specialist.ru/course/kl002104>  <https://www.academyit.ru/courses/20411/> |
| 2.7 | Минимальное количество человек на курсе | 100 |
| 2.8 | Максимальное количество человек на курсе | 200 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | При наличии |
| 2.10 | Формы аттестации | Зачет в виде теста |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | В соответствии с приложением |

1. **Аннотация программы**

Наиболее полное и содержательное описание программы, которое включает:

1) общую характеристику компетенций, качественное изменение которых осуществляется в результате обучения или которые формируются в результате освоения образовательной программы;

2) описание требований и рекомендаций для обучения по образовательной программе;

3) краткое описание результатов обучения в свободной форме, а также описание востребованности результатов обучения в профессиональной деятельности.

Ограничение по размеру: не менее 1000 символов -?

Общая характеристика компетенций, качественное изменение которых осуществляется в результате обучения

Общепрофессиональные компетенции цифровой экономики:

ОПК-1 - Управление информацией и данными.

Компетенция предполагает способность человека искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач.

Профессиональные компетенции цифровой экономики:

ПК-1 – способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций

Под данной компетенцией в рамках настоящей образовательной программы понимается умение обучающегося применять средства защиты, имеющиеся в автоматизированной системе, с целью противодействия угрозам информационной безопасности в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования и способность восстанавливать работоспособность средств защиты при возникновении нештатных ситуаций как техногенного, так и антропогенного характера.

ПК-2 – способность администрировать подсистему информационной безопасности автоматизированной системы.

Под данной компетенцией в рамках настоящей образовательной программы понимается готовность обучающегося выполнять действия по конфигурированию параметров компонентов подсистемы информационной безопасности автоматизированной системы в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования.

ПК-3 – способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы

Под данной компетенцией в рамках настоящей образовательной программы понимается готовность обучающегося выполнять действия по реализации и корректировке частных политик информационной безопасности, реализуемых в различных подсистемах автоматизированной системы в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования. Выполнять аудит информационной безопасности на основе данных мониторинга событий информационной безопасности.

Описание требований и рекомендаций для обучения по образовательнойпрограмме

Обучаемые до начала обучения (сотрудники государственных, муниципальных органов, органов местного самоуправления, организаций различных форм собственности, физические лица, организующие и (или) осуществляющие администрирование информационной безопасности, сотрудники департаментов (отделов, служб) IT и информационной безопасности, специалисты по защите информации) должны знать основы информационных технологий, иметь навыки работы на персональном компьютере под управлением ОС MS Windows, а также иметь навыки работы с антивирусными средствами Лаборатории Касперского.

Для просмотра методических видеоматериалов в режиме «оффлайн», для участия в лекционных и практических занятиях в режиме видеоконференций, а также для самостоятельного выполнения заданий обучаемые должны использовать персональные компьютеры, удовлетворяющие следующим требованиям:

* многоядерный процессор с поддержкой аппаратной виртуализации;
* объем оперативной памяти не менее 8 Гб;
* видеоадаптер с поддержкой HD-видео;
* веб-камера с микрофоном;
* сетевой адаптер, имеющий широкополосное подключение к сети Интернет.

На персональных компьютерах должно быть установлено следующее программное обеспечение:

* браузер с поддержкой просмотра видео (Mozilla Firefox, Google Chrome, MS Edge и т. п. последних версий);
* программа для записи видеоуроков (для преподавателя, например OBS);
* программа просмотра документов в формате PDF;
* программа виртуализации Oracle VirtualBox.

Для выполнения самостоятельных работ обучаемые могут использовать следующие дистрибутивы программных продуктов:

* дистрибутив клиентской операционной системы Windows уровня не ниже Professional и версии не ниже 7 для установки в виртуальную машину;
* дистрибутив серверной операционной системы Windows версии не ниже 2008 R2 для установки в виртуальную машину;
* дистрибутив Kaspersky Security Center для установки в виртуальную машину;
* дистрибутив Kaspersky Endpoint Security для установки в виртуальную машину;

В случае недоступности указанных дистрибутивов обучаемые должны иметь установленную на персональный компьютер операционную систему Windows уровня не ниже Professional и версии не ниже 7 с правами локального администратора.

Краткое описание результатов обучения

В результате освоения программы обучающийся:

должен уметь:

* управлять процессом обеспечения антивирусной безопасности автоматизированных систем для реагирования на инциденты информационной безопасности;
* настраивать права доступа пользователей к объектам при использовании механизмов групп безопасности и наследования прав;
* создавать и редактировать объекты в Microsoft AD; создавать, редактировать групповые политики и управлять ими;
* использовать языки сценариев для автоматизации задач администрирования информационной безопасности;

должен знать:

* архитектуру и основные компоненты средств обеспечения антивирусной безопасности;
* принципы управления антивирусной безопасностью автоматизированной системы;
* механизмы реализации разграничения доступа в файловых системах;
* понятия группы безопасности, отношения доверия и групповой политики;

Знания, умения и навыки, полученные в результате обучения, могут быть востребованы во всех сферах цифровой экономики при выполнении должностных обязанностей по администрированию информационной безопасности.

1. ШАБЛОН ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ (ДПО)

Титульный лист программы

Название организации

Дополнительная профессиональная программа повышения квалификации

« Администрирование информационной безопасности »

72 час.

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

актуализация профессиональных компетенций у обучаемых, связанных с администрированием информационной безопасности в области цифровой экономики

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1 Понятие политики информационной безопасности.

2.1.2 Методы разграничения доступа к ресурсам в многопользовательской среде.

2.1.3 Основы аудита информационной безопасности.

2.1.4 Методы и средства противодействия вредоносным программам и компьютерным вирусам.

2.2. Умение (способность к деятельности)

2.2.1. Реализация политик управления доступом к общим ресурсам.

2.2.2 Использование механизма управление групповыми политиками для создания единой среды настроек пользователей и компьютеров.

2.2.3 Настройка сбора событий аудита информационной безопасности и выявление фактов нарушений информационной безопасности путем анализа аудита.

2.2.4 Реализация политики антивирусной защиты в корпоративной среде.

2.3.Навыки (использование конкретных инструментов)

2.3.1 Настройка прав доступа к объектам файловой системы NTFS для пользователей и групп безопасности в ОС Windows.

2.3.2 Управление локальными политиками в ОС Windows и групповыми политиками в Mictosoft Active Directory.

2.3.3 Настройка сбора и отображения событий аудита информационной безопасности в ОС Windows.

2.3.4 Использование сценариев PowerShell для управления пользователями и группами безопасности в Mictosoft Active Directory.

2.3.5 Реализация политики антивирусной защиты с помощью антивирусного пакета Kaspersky Endpoint Security и с сетевым центром управления Kaspersky Security Center.

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

* 1. Образование: высшее
  2. Квалификация
  3. Наличие опыта профессиональной деятельности: не требуется
  4. Предварительное освоение иных дисциплин/курсов /модулей: не требуется

**4.Учебный план программы «…..наименование программы….»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Администрирование Microsoft AD | 50 | 8 | 20 | 22 |
| 2 | Администрирование подсистемы антивирусной безопасности. | 20 | 4 | 8 | 8 |
| **Итоговая аттестация** | |  | **Указывается вид (экзамен, зачёт, реферат и т.д.)** | | |
| Компьютерное тестирование | | 2 | зачет | | |

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | Администрирование Microsoft AD | 50 | 2.11.2020 - 9.11.2020 |
| **2** | Администрирование подсистемы антивирусной безопасности. | 20 | 10.11.2020 - 13.11.2020 |
| 3 | Итоговая аттестация | 2 | 14.11.2020 |
| **Всего:** | | 72 | 2.11.2020-15.11.2020 |

**6.Учебно-тематический план программы «**  Администрирование информационной безопасности **»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Администрирование Microsoft AD | 50 | 8 | 20 | 22 |  |
| 1.1 | Инфраструктура Microsoft AD | 10 | 2 | 4 | 4 | тест |
| 1.2 | Управление полномочиями в AD | 14 | 2 | 6 | 6 | Проверка заданий |
| 1.3 | Управление групповыми политиками | 16 | 2 | 6 | 8 | Проверка заданий |
| 1.4 | Использование Microsoft PowerShell для администрирования системы | 10 | 2 | 4 | 4 | Проверка заданий |
| 2 | Администрирование подсистемы антивирусной безопасности | 20 | 4 | 8 | 8 |  |
| 2.1 | Архитектура и основные компоненты подсистемы антивирусной безопасности | 10 | 2 | 4 | 4 | тест |
| 2.2 | Управление подсистемой антивирусной безопасности | 10 | 2 | 4 | 4 | Проверка заданий |

**7. Учебная (рабочая) программа повышения квалификации «**  Администрирование информационной безопасности  **»**

**Модуль 1.** Администрирование Microsoft AD **(** 50 **час.)**

**Тема 1.1** Инфраструктура Microsoft AD **(** 10 **час)**

Понятия домена, дерева доменов, леса доменов. Схема AD, объекты схемы и их атрибуты. Доступ к службе каталогов AD, репликация AD. Отношения доверия между доменами. Организационные единицы AD. Планирование организационных единиц в AD. Служба имен в АD. Обеспечение безопасности в AD. Планирование организационных единиц в AD. Реализация структуры AD средствами графических оснасток и консольных утилит.

**Тема 1.2** Управление полномочиями в AD (14 час)

Управление доступом к файлам и принтерам в AD на уровне сети (общие ресурсы) и на уровне файловой системы NTFS. Группы безопасности в AD. Типы групп и их область действия. Сайты AD и их назначение. Планирование групп безопасности. Разграничение прав доступа к ресурсам.

Тема 1.3 Управление групповыми политиками (16 час.)

Понятие групповой политики. Обработка ГП компьютеров и пользователей. Шаблоны безопасности и их применение. Стартовые политики. Средства управления политиками. Управление фильтрами безопасности и порядком выполнения ГП. Создание и применение следующих политик: политика учетных записей; политика аудита; политика ограниченного использования программ..

Тема 1.4 Использование Microsoft PowerShell для администрирования системы (10 час.)

Управление правами доступа. Управление процессами. Управление пользователями и группами. Управление групповыми политиками. Автоматизация задач управления AD с помощью сценариев PowerShell.

**Модуль 2.** Администрирование подсистемы антивирусной безопасности **(**20 **час.)**

**Тема 2.1.** Архитектура и основные компоненты подсистемы антивирусной безопасности (10 час.)

Классификация методов и средств обеспечения антивирусной безопасности. Архитектура и основные компоненты подсистемы антивирусной безопасности с сетевым центром управления. Процессы управления подсистемой антивирусной безопасности. Развертывание подсистемы антивирусной безопасности.

Тема 2.2. (10 час.)

Управление антивирусной безопасностью с применением политик и задач. Настройка уведомлений о событиях антивирусной безопасности. Настройка реагирования на инциденты информационной безопасности с моделированием вирусных атак. Разделение полномочий по управлению антивирусной безопасностью. Обеспечение отказоустойчивости подсистемы антивирусной безопасности.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1.1** | Тема 1.1 | Планирование организационных единиц | Для заданной структуры организации выполнить планирование организационных единиц Microsoft AD. |
| **1.2** | Тема 1.2 | Разграничение доступа к объектам файловой системы | Для заданного списка служебных полномочий к набору файловых объектов создать группы безопасности и выполнить разграничение доступа |
| 1.3 | Тема 1.3 | Управление политикой ограниченного использования программ | По заданным требованиям создать политику ограниченного использования программ и проверить ее работу |
| 1.4 | Тема 1.3 | Управление политикой аудита событий информационной безопасности | Настроить групповую политику аудита безопасности объектов файловой системы для заданных файлов и папок |
| 1.5 | Тема 1.3 | Просмотр и анализ событий аудита информационной безопасности | Создать фильтр в журнале безопасности для просмотра критических событий аудита |
| 1.6 | Тема 1.4 | Создание сценариев управленияинформационной безопасностью на языке PowerShell | Создать сценарии на языке PowerShell для выполнения заданного действия (добавление учетных записей пользователей по текстовому списку, блокировка учетных записей по списку, удаление учетных записей по списку, перемещение учетных записей из одной организационной единицы в другую по списку) |
| 2.1 | Тема 2.1 | Развертывание подсистемы антивирусной безопасности с сетевым центром управления | Выполнить установку и настройку компонентов подсистемы антивирусной безопасности. Настроить взаимодействие антивирусных средств и сетевого центра управления. Обеспечить совместимость центра управления антивирусной безопасностью и различных версий антивирусных средств. |
| 2.2 | Тема 2.2 | Управление подсистемой антивирусной безопасности с сетевым центром управления | Настроить групповые политики и задачи для различных версий антивирусных средств. Обеспечить совместимость политик и задач, созданных для различных версий антивирусных средств. Настроить оповещение и реагирование на инциденты |
| 2.3 | Тема 2.2 | Разграничение полномочий по управлению подсистемой антивирусной безопасности и обеспечение отказоустойчивости. | Создать иерархию серверов подсистемы антивирусной безопасности. Создать различных пользователей подсистемы антивирусной безопасности и разделить полномочия по управлению. Настроить резервирование получения обновления антивирусных баз, управления и восстановление работоспособности при возникновении нештатных ситуаций. |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1**.1 | Каково назначение операционной системы? | Каково назначение организационных единиц в Microsoft AD? | На какие объекты Microsoft AD можно назначить групповую политику? |
| 1.2 | Что такое файл? | Назовите виды доверия между доменами в Microsoft AD | Укажите последовательность применения групповых политик в Microsoft AD |
| 2.1 | Программа, предназначенная для осуществления несанкционированного доступа к информации и или деструктивного воздействия на информацию или ресурсы информационной системы, называется… вредоносная; проприетарная; сертифицированная. | Агент администрирования центра управления антивирусной безопасностью …  осуществляет взаимодействие между сервером администрирования и антивирусными средствами, установленными на сетевом узле.  предоставляет пользовательский интерфейс к административным службам сервера администрирования и агента администрирования.  осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими. | Сервер администрирования сетевого центра управления антивирусной безопасностью…  осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.  осуществляет взаимодействие между сервером администрирования и антивирусными средствами, установленными на сетевом узле.  предоставляет пользовательский интерфейс к административным службам сервера администрирования и агента администрирования. |
| 2.2 | Набор клиентских компьютеров, объединенных по какому-либо признаку, с целью управления компьютерами как единым целым называется …  группой администрирования.  профилем администрирования.  задачей администрирования. | При отсутствии политики для автономного пользователя в случае разрыва соединения между сервером администрирования и клиентским компьютером, на клиентском компьютере …  действует активная политика.  действует политика более высокого уровня иерархии.  не действует ни одна политика. | Если в активной политике не установлен запрет на изменение параметров программы, то на каждом клиентском компьютере антивирусная программа использует …  локальное значение параметра.  значение параметра активной политики.  значение параметра политики для автономного пользователя. |

**8.2.**

Входное тестирование:

Не зачтено - менее 60% правильных ответов;

Зачтено - 60% и более правильных ответов.

Зачет по входному тестированию служит допуском к освоению материалов модуля.

Промежуточное тестирование:

Не зачтено - менее 60% правильных ответов;

Зачтено - 60% и более правильных ответов.

Практикоориетированное задание:

Отлично - Отчет содержит все необходимые разделы, соответствует заданию, оформлен с соблюдением заданных требований. Материал представлен адекватно, в доходчивой форме, с преобладанием графических образов и применением современных ИТ. Отчет представлен в установленные сроки. Замечания по отчету отработаны правильно.

Хорошо - Отчет содержит все необходимые разделы, соответствует заданию, оформлен с соблюдением заданных требований. Материал представлен адекватно, в доходчивой форме. Отчет представлен в установленные сроки.

Удовлетворительно - Отчет содержит все необходимые разделы. Материал представлен адекватно.

Неудовлетворительно - Отчет отсутствует, или в отчете представлены не все разделы, или материал разделов не отражает результатов выполнения заданий.

Итоговое тестирование:

Не зачтено - менее 75% правильных ответов;

Зачтено - 75% и более правильных ответов.

Зачет (итоговая аттестация) выставляется, если

- зачтены результаты промежуточного тестирования по всем модулям;

- все практиокоориентированные задания выполнены с оценкой не ниже «удовлетворительно»;

- зачтены результаты итогового теста.

**.**

**8.3.**  Пример контрольного задания:

Перечислите обязанности администратора информационной безопасности по управлению антивирусной безопасностью автоматизированной системы. **.**

**8.4.**  Примеры тестов и практикоориентированных заданий:

1) Консоль администрирования сетевого центра управления…

- предоставляет пользовательский интерфейс к административным службам сервера администрирования и агента администрирования.

- осуществляет взаимодействие между сервером администрирования и антивирусными программами, установленными на сетевом узле.

- осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.

2) Агент администрирования сетевого центра управления …

- осуществляет взаимодействие между сервером администрирования и антивирусными программами, установленными на сетевом узле.

- предоставляет пользовательский интерфейс к административным службам сервера администрирования и агента администрирования.

- осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.

3) Сервер администрирования сетевого центра управления …

- осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.

- осуществляет взаимодействие между сервером администрирования и антивирусными программами, установленными на сетевом узле.

- предоставляет пользовательский интерфейс к административным службам сервера администрирования и агента администрирования.

4) Укажите правильный порядок применения груповых политик в Microsoft AD:

- локальная политика -> политика сайта -> политика домена -> политика подразделения

- локальная политика -> политика подразделения -> политика домена -> политика сайта

- политика сайта -> политика домена -> политика подразделения -> локальная политика

Для заданного списка служебных полномочий к набору файловых объектов создать группы безопасности и выполнить разграничение доступа.

Выполнить установку и настройку компонентов подсистемы антивирусной безопасности. Настроить взаимодействие антивирусных средств и сетевого центра управления. Обеспечить совместимость центра управления антивирусной безопасностью и различных версий антивирусных средств **.**

**8.5.**  Процедура аттестации состоит из

- тестирования по каждому модулю;

- проверки практико-ориентированных заданий по каждой теме каждого модуля;

- итогового теста.  
 **.**

**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** | Зефиров Сергей Львович | Пензенский государственный университет, Заведующий кафедрой «Информационная безопасность систем и технологий», к.т.н., доцент | <https://lk.pnzgu.ru/portfolio/1538270> |  | Согласие есть |
| **2** | Лупанов Михаил Юрьевич | Пензенский государственный университет, доцент кафедры «Информационная безопасность систем и технологий», к.т.н., доцент | <https://lk.pnzgu.ru/portfolio/16997969> |  | Согласие есть |
| 3 | Липилин Олег Владимирович | Пензенский государственный университет, доцент кафедры «Информационная безопасность систем и технологий», к.т.н., доцент | <https://lk.pnzgu.ru/portfolio/31494833> |  | Согласие есть |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Методы: | Основная литература: |
| - объяснительно-иллюстративный | Староверова, Н.А. Операционные системы : учебник / Н.А. Староверова. — Санкт-Петербург : Лань, 2019. — 308 с |
| - репродуктивный | Коробко, И.В. PowerShell как средство автоматического администрирования / И.В. Коробко. — Москва : ДМК Пресс, 2012. — 224 с. |
| - частично-поисковый | Программно-аппаратные средства защиты информации: учебное пособие/ Прокушев Я.Е. – СПб.: ООО Издательский центр «Интермедия», 2017. – 168 с |
| Форма: | Методические разработки и материалы курса: |
| - дистанционная | http://moodle.pnzgu.ru/enrol/index.php?id=61129 |
| Технологии: |  |
| - видеоурок |  |
| - видеоконференция |  |
| - практикоориентированное задание |  |
| - тестирование |  |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Электронные образовательные ресурсы ЭИОС ПГУ http://moodle.pnzgu.ru/enrol/index.php?id=61129 | PowerShell [электронный ресурс]: Материал из Microsoft Docs. – Режим доступа: https://docs.microsoft.com/ru-ru/powershell/scripting/overview?view=powershell-6, свободный. – Загл. с экрана |
|  | База знаний по продуктам [электронный ресурс]. – Режим доступа: https://support.kaspersky.ru/#s\_tab4, свободный. – Загл. с экрана |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекции | Персональный компьютер со следующим оборудованием:  - видеоадаптер с поддержкой HD-видео;  - веб-камера с микрофоном;  - устройство воспроизведения звука (колонки/наушники);  - сетевой адаптер, имеющий широкополосное подключение к сети Интернет; и программным обеспечением:  - программа просмотра документов в формате PDF (любая);  - интернет-браузер с поддержкой просмотра видео (Mozilla Firefox, Google Chrome, MS Edge и т. п. последних версий). |
| Практические занятия | Персональный компьютер со следующим оборудованием:  - видеоадаптер с поддержкой HD-видео;  - веб-камера с микрофоном;  - устройство воспроизведения звука (колонки/наушники);  - сетевой адаптер, имеющий широкополосное подключение к сети Интернет; и программным обеспечением:  - интернет-браузер с поддержкой просмотра видео (Mozilla Firefox, Google Chrome, MS Edge и т. п. последних версий);  - программа для проведения видеоконференций Zoom. |
| Самостоятельная работа | Персональный компьютер со следующим оборудованием:  -многоядерный процессор с поддержкой аппаратной виртуализации;  - объем оперативной памяти не менее 8 Гб;  и программным обеспечением:  - операционная система MS Windows версии не ниже 7 и уровня не ниже Professional;  - программа виртуализации Oracle VirtualBox;  - дистрибутив клиентской операционной системы Windows уровня не ниже Professional и версии не ниже 7 для установки в виртуальную машину (желательно, но не обязательно);  - дистрибутив серверной операционной системы Windows версии не ниже 2008 R2 для установки в виртуальную машину (желательно, но не обязательно);  - дистрибутив Kaspersky Security Center для установки в виртуальную машину (желательно, но не обязательно);  - дистрибутив Kaspersky Endpoint Security для установки в виртуальную машину(желательно, но не обязательно). |

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

Описание перечня профессиональных компетенций, качественное изменение которых осуществляется в результате обучения.

Планируемые результаты обучения должны быть определены в виде знаний, умений, навыков и (или) опыта деятельности, характеризующих формирование/развитие компетенции(-й) в области цифровой экономики и представлены в виде Паспорта компетенций в машиночитаемом текстовом формате. Структура паспорта представлена в приложении.

ПАСПОРТ КОМПЕТЕНЦИИ ОПК-1

(Администрирование информационной безопасности)

(Федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный университет»)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Управление информацией и данными | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная | общепрофессиональная | |
| профессиональная |  | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Компетенция предполагает способность человека искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач.  Слушатель должен:  Знать:  - состав и функциональное назначение подсистемы информационной безопасности ОС Windows;  - состав и функциональное назначение антивирусных средств  Уметь:  - управлять правами доступа к информационным объектам ОС Windows;  - осуществлять аудит доступа к информационным объектам ОС Windows;  - управлять групповыми политиками информационной безопасности ОС Windows;  - устанавливать антивирусные средства на персональный компьютер;  - осуществлять аудит событий антивирусной защиты;  - управлять политиками антивирусной защиты;  Владеть:  - инструментальными средствами ОС Windows для разграничения прав доступа, управления групповыми политиками и настройки и просмотра событий аудита информационной безопасности;  - навыками установки антивирусных средств;  - инструментальными средствами настройки аудита и политики антивирусной защиты. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знает:  О средствах разграничения доступа, используемых при передаче и хранении информации. О необходимости обязательной проверки всех полученных данных антивирусными средствами  Умеет:  Пользоваться средствами операционных систем для передачи и хранения информации. Пользоваться антивирусными средствами для проверки полученных данных.  Владеет:  Начальными навыками управления ОС Windows. Навыками по использованию предварительно настроенных антивирусных средств |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | Знает:  Состав и назначение средств разграничения доступа операционных систем. Состав и назначение антивирусных средств.  Умеет:  Выполнять действия по разграничению прав доступа к хранимой информации. Выполнять установку антивирусных средств на рабочее место.  Владеет:  Интсрументальными средствами ОС Windows для разграничения прав доступа. Навыками установки антивирусных средств в конфигурации «по умолчанию» |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает:  Функциональные возможности средств разграничения доступа операционных систем. Функциональные возможности антивирусных средств  Умеет:  Выполнять аудит событий доступа к информации в журнале безопасности ОС Windows. Выполнять аудит событий в журнале антивирусных средств.  Владеет:  Средствами настройки и просмотра аудита ОС Windows. Средствами настройки и просмотра аудита антивирусных средств. |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | Знает:  Понятие групповых политик безопасности.  Умеет:  Выполнять управление политиками безопасности ОС Windows и антивирусных средств.  Владеет:  Инструментальными средствами настройки политик безопасности ОС Windows и антивирусных средств. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | |  | |
| 6. | Средства и технологии оценки | | тесты | |

ПАСПОРТ КОМПЕТЕНЦИИ ПК-1

(Администрирование информационной безопасности)

(Федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный университет»)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная |  | |
| профессиональная | профессиональная | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Компетенция предполагает способность человека применять средства защиты, имеющиеся в автоматизированной системе, с целью противодействия угрозам информационной безопасности в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования и способность восстанавливать работоспособность средств защиты при возникновении нештатных ситуаций как техногенного, так и антропогенного характера.  Слушатель должен:  Знать:  - принципы применения антивирусных средств, их недостатки и ограничения;  - особенности функционирования отдельных подсистем антивирусных средств;  порядок восстановления работоспособности антивирусных средств;  Уметь:  - применять средства управления для определения значений параметров антивирусных средств;  - конфигурировать параметры антивирусных средств, обеспечивающие компенсацию различных угроз безопасности и восстановление работоспособности;  - учитывать изменения в требованиях информационной безопасности и условиях применения антивирусных средств, появления новых угроз  Владеть:  - навыками обеспечения информационной безопасности путем использования антивирусных средств;  - навыками навыками обеспечения отказоустойчивости антивирусных средств;  - навыками управления антивирусными средствами в сетевой среде;  - навыками автоматизизации управления антивирусными средствами, включая восстановление работоспособности. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знает:  о возможности и необходимости применения антивирусных средств защиты информации, имеет представление о возможностях антивирусной системы по обеспечению информационной безопасности  Умеет:  использовать некоторые средства управления, применяемые для конфигурирования антивирусных средств  Владеет:  начальными навыками использования антивирусных средств для защиты информации на отдельном рабочем месте |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | Знает:  основные принципы применения антивирусных средств; общий порядок (алгоритм) их применения и восстановления работоспособности  Умеет:  применять средства управления для определения значений параметров антивирусных средств; определять значения параметров с учетом требований информационной безопасности  Владеет:  навыками обеспечения информационной безопасности на отдельном рабочем месте с использованием антивирусных средств; навыками определения режимов работы антивирусных средств, базовыми навыками обеспечения отказоустойчивости антивирусных средств |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает:  особенности применения антивирусных средств, обеспечивающие их эффективное применение; недостатки и ограничения антивирусных средств при их применении  Умеет:  конфигурировать параметры антивирусных средств, обеспечивающие их эффективное применение; определять оптимальные значения параметров с учетом всех условий применения антивирусных средств  Владеет:  навыками использования и антивирусных средств в сетевой среде с централизованным управлением с учетом требований их эффективного функционирования; навыками обеспечения отказоустойсивости антивирусных средств, функционирующих в сетевой среде с единым центром управления |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | Знает:  особенности применения антивирусных средств, обеспечивающие реализацию наборов требований и политик безопасности; особенности функционирования отдельных подсистем и восстановления работоспособности  Умеет:  конфигурировать параметры антивирусных средств, обеспечивающие компенсацию различных угроз безопасности и восстановление работоспособности; учитывать изменения в требованиях информационной безопасноси и условиях применения антивирусных средств, появления новых угроз  Владеет:  навыками применения антивирусных средств посредством созданиях сложных конфигураций; навыками использования функциональных возможностей антивирусных средств, позволяющих автоматизировать управление антивирусных средств, включая восстановление работоспособности |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | ОПК-1, ПК-3  Компетенция ОПК-1 является общепрофессиональной компетенцией цифровой экономики и владение этой компетенцией необходимо для овладевания всеми профессиональными компетенциями данной программы.  Необходимость владения компетенцией ПК-3 обусловлена тем, что для эффективного применения антивирусных средств и восстановления их работоспособности при возникновении нештатных ситуаций требуются знания и навыки создания частных политик информационной безопасности в части антивирусной защиты | |
| 6. | Средства и технологии оценки | | Тесты, практикоориентированные задания | |

ПАСПОРТ КОМПЕТЕНЦИИ ПК-2

(Администрирование информационной безопасности)

(Федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный университет»)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | способность администрировать подсистему информационной безопасности автоматизированной системы | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная |  | |
| профессиональная | профессиональная | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Компетенция предполагает способность человека выполнять действия по конфигурированию параметров компонентов подсистемы информационной безопасности автоматизированной системы в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования  Слушатель должен:  Знать:  - методы и средства обеспечения информационной безопасности операционных систем;  - особенности применения средств и методов обеспечения информационной безопасности операционной системы в соответствии с требованиями эксплуатационной документации и нормативных документов;  - влияние параметров средств и методов обеспечения информационной безопасности операционной системы на реализацию наборов требований и политик безопасности;  Уметь:  - использовать средства управления конфигурацией компонентов подсистемы информационной безопасности операционной системы;  - определять параметры конфигурации компонентов подсистемы информационной безопасности операционной системы;  - формулировать требования информационной безопасности к компонентам подсистемы информационной безопасности операционной системы;  Владеть:  - навыками конфигурирования подсистемы информационной безопасности операционной системы в соответствии с требованиями по информационной безопасности;  - навыками автоматизации управления конфигурацией подсистемы информационной безопасности операционной системы. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знает:  типовые методы и средства обеспечения информационной безопасности операционной системы  Умеет:  использовать средства управления конфигурацией компонентов подсистемы информационной безопасности операционной системы  Владеет:  начальными навыками конфигурирования подсистемы информационной безопасности операционной системы |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | Знает:  основные принципы применения средств и методов обеспечения информационной безопасности операционных систем  Умеет:  использовать средства управления конфигурацией компонентов подсистемы информационной безопасности операционной системы в соответствии с требованиями эксплуатационной документации  Владеет:  навыками конфигурирования компонентов подсистемы информационной безопасности операционной системы в соответствии с требованиями по информационной безопасности |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает:  особенности применения средств и методов обеспечения информационной безопасности операционной системы в соответствии с требованиями эксплуатационной документации и нормативных документов  Умеет:  определять параметры конфигурации компонентов подсистемы информационной безопасности операционной системы в соответствии с требованиями эксплуатационной документации и требованиями нормативных документов  Владеет:  навыками конфигурирования программных компонентов подсистемы информационной безопасности операционной системы в соответствии с требованиями по информационной безопасности и особенностями их функционирования |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | Знает:  влияние параметров средств и методов обеспечения информационной безопасности операционной системы на реализацию наборов требований и политик безопасности  Умеет:  формулировать требования информационной безопасности к компонентам подсистемы информационной безопасности операционной системы на основе анализа событий информационной безопасности и функционирования системы  Владеет:  навыками использования функциональных возможностей компонентов подсистемы информационной безопасности операционной системы, позволяющих автоматизировать функции администрирования и восстановления работоспособности |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | ОПК-1, ПК-3  Компетенция ОПК-1 является общепрофессиональной компетенцией цифровой экономики и владение этой компетенцией необходимо для овладевания всеми профессиональными компетенциями данной программы.  Необходимость владения компетенцией ПК-3 обусловлена тем, что для эффективного администрирования подсистемы информационной безопасности требуются знания и навыки создания частных политик информационной безопасности в части антивирусной защиты | |
| 6. | Средства и технологии оценки | | Тесты, практикоориентированные задания | |

ПАСПОРТ КОМПЕТЕНЦИИ ПК-3

(Администрирование информационной безопасности)

(Федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный университет»)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная |  | |
| профессиональная | профессиональная | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Компетенция предполагает способность человека выполнять действия по реализации и корректировке частных политик информационной безопасности, реализуемых в различных подсистемах автоматизированной системы в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования. Выполнять аудит информационной безопасности на основе данных мониторинга событий информационной безопасности.  Слушатель должен:  Знать:  - функциональные возможности операционных систем и антивирусных средств, необходимые для реализации частных политик информационной безопасности;  - возможности операционных систем и антивирусных средств по аудиту информационной безопасности;  - язык сценариев PowerShell в объеме, достаточном для реализации частных политик информационной безопасности в операционных системах;  Уметь:  - применять средства управления операционных систем и антивирусных средств для реализации частых политик информационной безопасности;  - использовать язык сценариев для автоматизации работ по реализации частных политик информационной безопасности;  Владеть:  - инструментальными средствами управления групповыми политиками в ОС Windows;  - навыками управления журналами регистрации событий в операционных системах и антивирусных средствах, в том числе фильтрацией событий по выбранным критериям;  - навыками настройки реагирования на инциденты информационной безопасности в антивирусных средствах. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знает:  о возможности реализации частных политик информационной безопасности в автоматизированной системе средствами операционных систем, имеет представления о средствах мониторинга и аудита  Умеет:  использовать антивирусные средства защиты с политиками, предоставленными по-умолчанию  Владеет:  начальными навыками реализации некоторых частных политик информационной безопасности на отдельном рабочем месте |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | Знает:  функциональные возможности операционных систем и антивирусных средств, необходимые для реализации частных политик информационной безопасности, а также возможности по мониторингу и аудиту информационной безопасности  Умеет:  применять средства управления операционных систем и антивирусных средств для реализации частых политик информационной безопасности на отдельном рабочем месте  Владеет:  инструментальными средствами управления групповыми политиками в ОС Windows; базовыми навыками управления журналами регистрации событий в операционных системах и антивирусных средствах, в том числе фильтрацией событий по некоторым критериям, на отдельном рабочем месте |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает:  функциональные возможности операционных систем и антивирусных средств, необходимые для реализации частных политик информационной безопасности, а также возможности по мониторингу и аудиту информационной безопасности применительно к группам рабочих мест, функционирующих в сетевой среде с централизованным управлением  Умеет:  применять средства управления операционных систем и антивирусных средств для реализации частых политик информационной безопасности применительно к группам рабочих мест, функционирующих в сетевой среде с централизованным управлением  Владеет:  навыками управления журналами регистрации событий в операционных системах и антивирусных средствах, в том числе фильтрацией событий по всем возможным критериям, применительно к группам рабочих мест, функционирующих в сетевой среде с централизованным управлением |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | Знает:  язык сценариев PowerShell в объеме, достаточном для реализации частных политик информационной безопасности в операционных системах  Умеет:  использовать язык сценариев для автоматизации работ по реализации частных политик информационной безопасности  Владеет:  навыками настройки реагирования на инциденты информационной безопасности в антивирусных средствах |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | ОПК-1, ПК-1, ПК-2  Компетенция ОПК-1 является общепрофессиональной компетенцией цифровой экономики и владение этой компетенцией необходимо для овладевания всеми профессиональными компетенциями данной программы.  Необходимость владения компетенциями ПК-1 и ПК-2 обусловлена тем, что для реализации частных политик информационной безопасности автоматизированной системы, а также выполнения мониторинга и аудита информационной безопасности требуются знания и навыки администрирования и эффективного использования подсистемы информационной безопасности автоматизированной системы, включая навыки настройки и использования подсистем информационной безопасности операционной системы и антивирусных средств. | |
| 6. | Средства и технологии оценки | | Тесты, практикоориентированные задания | |

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

**V.Рекомендаций к программе от работодателей**: наличие не менее двух писем и/или подтверждения на цифровой платформе Государственной системы предоставления ПЦС от работодателей о рекомендации образовательной программы для реализации в рамках Государственной системы предоставления ПЦС на формирование у трудоспособного населения компетенций цифровой экономики с указанием востребованности результатов освоения программы в сфере деятельности соответствующих компаний и готовности к рассмотрению заявок наиболее успешно освоивших образовательную программу граждан на прохождение стажировки и (или) собеседования на предмет трудоустройства путем проставления отметки в профиле программы

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

Сценарии профессиональной траектории граждан

|  |  |
| --- | --- |
| Цели получения персонального цифрового сертификата | |
| текущий статус | цель |
| Развитие компетенций в текущей сфере занятости | |
| работающий по найму в организации, на  предприятии | сохранение текущего рабочего места |
| работающий по найму в организации, на  предприятии | развитие профессиональных качеств |
| работающий по найму в организации, на  предприятии | повышение заработной платы |
| работающий по найму в организации, на  предприятии | смена работы без изменения сферы  профессиональной деятельности |
| Переход в новую сферу занятости | |
| освоение новой сферы занятости | самозанятый, ИП/бизнесмен, |
| освоение смежных профессиональных  областей | повышение уровня дохода, расширение  профессиональной деятельности |

**VII.Дополнительная информация**

**VIII.Приложенные Скан-копии**

Утвержденной рабочей программа (подпись, печать, в формате pdf)