# I. Паспорт Образовательной программы

**«Кибербезопасность и кибергигиена: Level 0.»**

|  |  |
| --- | --- |
| **Версия программы** | 1 |
| **Дата Версии** | 07.09.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | ФГБОУ ВО «Магнитогорский государственный  технический университет им. Г.И. Носова» |
| 1.2 | Логотип образовательной организации | M:\2 Документы по КПК\2020-2021 учебный год\Цифровая экономика\logo_mgtu.jpg |
| 1.3 | Провайдер ИНН | 7414002238 |
| 1.4 | Ответственный за программу  ФИО | Георгиевских Наталья Валерьевна |
| 1.5 | Ответственный должность | Специалист по информационно-аналитической  работе ИДПО «Горизонт» |
| 1.6 | Ответственный Телефон | +79123163253 |
| 1.7 | Ответственный Е-mail | [georgievskih95@gmail.com](mailto:georgievskih95@gmail.com) |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Кибербезопасность и кибергигиена: Level 0. |
| 2.2 | Ссылка на страницу программы | [http://idpo.magtu.ru/index.php/component/jshoppin](http://idpo.magtu.ru/index.php/component/jshopping/product/view/79/745?Itemid=0)  [g/product/view/79/745?Itemid=0](http://idpo.magtu.ru/index.php/component/jshopping/product/view/79/745?Itemid=0) |
| 2.3 | Формат обучения | Онлайн |
| 2.4 | 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 | Кус размещен на платформе MOODLE портала дистанционной подготовки ИДПО «Горизонт» ФГБОУ ВО «Магнитогорского государственного технического университета им. Г.И. Носова»  <http://m.idpo.magtu.ru/> |
| 2.5 | Уровень сложности | Начальный |
| 2.6 | Количество академических часов | 72 |
| 2.7 | 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) | 36 |
| 2.8 | 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 | 30000  <https://academy.ithub.ru/course/osnkiber>  <http://www.fa.ru/fil/tula/dpo/ppk/Pages/Kiber.aspx>  <https://www.rea.ru/ru/org/managements/Centr-kompetencijj-cifrovojj-ehkonomiki/Pages/kiberbezopasnost.aspx> |
| 2.9 | Минимальное количество  человек на курсе | 1 |
| 2.10 | Максимальное количество  человек на курсе | 200 |
| 2.11 | Данные о количестве слушателей, ранее успешно  прошедших обучение по образовательной программе |  |
| 2.13 | Формы аттестации | Разработка проекта |
| 2.13 | 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**

По окончанию изучения курса «Кибербезопасность и кибергигиена: Level 0.» у слушателя будут сформированы следующие компетенции:

* + Управление информацией и данными.
  + Критическое мышление в цифровой среде.
  + Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защите интересов личности, общества и государства, соблюдать нормы профессиональной этики.
  + 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 объектов защиты.

Для обучения по данной программе слушатель должен:

Знать:

* + Понятия Интернет, браузер, Play Маркет/App Store.
  + Основные возможности программ Word, PowerPoint, Excel.
  + Основы работы на компьютере и его функциональные возможности.
  + Основные возможности цифровых технологий.
  + Основы работы с мобильным устройством. Уметь:
  + Использовать возможности цифровых технологий.
  + Скачивать приложения с Play Маркет (App Store).
  + Создавать и редактировать документы в программах MS Word, MS Exsel. Владеть:
  + Цифровыми технологиями для возможности повсеместного использования.

С использованием цифровых технологий изменяются повседневная жизнь человека, производственные отношения, структура экономики и образование, а также возникают новые требования к коммуникациям. Все большее число граждан РФ признает необходимость обладания цифровыми компетенциями, однако уровень использования персональных компьютеров и информационно-телекоммуникационной сети «Интернет» в России все еще ниже, чем в Европе, и существует серьезный разрыв в цифровых навыках между отдельными группами населения. Применение цифровых технологий без владения навыками обеспечения кибербезопасности и кибергигиены это как езда на машине без применения тормозов. Поэтому всем людям, живущим в эпоху цифровизации, такие навыки необходимы как в повседневной жизни, так и в профессиональной деятельности. Обучение на программе «Кибербезопасность и кибергигиена: Level 0» позволит слушателю освоить основные подходы по обеспечению кибербезопасности и основные правила кибергигиены. На информационных лекциях слушатель узнает о видах информации подлежащей защите, о способах и средствах ее защиты, на видео лекция познакомиться с

техническими средствами защиты информации, а на практических занятиях с элементами геймификации сможет отточить полученные знания, принимая участие в визуальной новелле с реконструкцией моделей ролевого поведения в предложенных сценарных условиях по тематике программы. В результате освоения программы слушатель построит дерево атак с учетом вероятности возникновения угроз на основе статистики за 2020 год по данным «Лаборатории Касперского».



# ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

**1. Цель программы**

С использованием цифровых технологий изменяются повседневная жизнь человека, производственные отношения, структура экономики и образование, а также возникают новые требования к коммуникациям. Все большее число граждан РФ признает необходимость обладания цифровыми компетенциями, однако уровень использования персональных компьютеров и информационно-телекоммуникационной сети «Интернет» в России все еще ниже, чем в Европе, и существует серьезный разрыв в цифровых навыках между отдельными группами населения.

Целью программы является:

1. Повышение профессионального уровня слушателей для приобретения дополнительных компетенций, позволяющих решать человеку поставленные задачи или достигать заданного результата деятельности в условиях глобальной цифровизации общественных и бизнес-процессов.
2. Получение новой компетенции, необходимой для профессиональной деятельности в сфере цифровой экономики в условиях нарастающих угроз безопасности информации.

# Планируемые результаты обучения:

Программа разработана с учетом требований:

профессионального стандарта: проф. стандарт " Специалист по защите информации в автоматизированных системах ", от 15.09.2016 № 522н; ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).

и квалификационных требований: нац. программа «Цифровая экономика РФ», распоряжение от 28 июля 2017 г. № 1632-р; фед. проект «Кадры для цифровой экономики», протокол №6 от 27 декабря 2018 г.

По окончании обучения планируется достижение слушателями следующих результатов по реализации обобщенной трудовой функции: Обслуживание систем защиты информации в автоматизированных системах, 5 уровень квалификации.

В результате освоения программы у слушателей должны быть сформированы следующие **компетенции**:

|  |  |  |
| --- | --- | --- |
| ***Управление информацией и данными*** | | |
| *Трудовые действия* | *Необходимые умения* | *Необходимые знания* |
| * Поиск и анализ необходимых источников информации и данных. * Передача информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными. * Эффективно использовать полученную информацию для решения задач. * Организовать процедуру обработки и хранения | * Использовать специальные сервисы и алгоритмы для поиска и анализа информационного пространства. * Воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств. * Пользоваться   информационными нормативно-правовыми базами данных.   * Уметь различать виды информации, такие как конфиденциальная | * Алгоритмы анализа информационного пространства. * Основные цифровые средства передачи информации. * Методы обработки текстовой и графической информации. * Основы цифровой грамотности. * Правовые основания обработки и хранения персональных данных. * Понятия конфиденциальной информации и коммерческой тайны. |
| персональных данных в соответствии с  требованиями законодательства. | информация, коммерческая тайна и персональные данные. | - Основы законодательства РФ в области  информационной безопасности. |
| ***Критическое мышление в цифровой среде*** | | |
| *Трудовые действия* | *Необходимые умения* | *Необходимые знания* |
| - Проведение критической оценки информации и ее достоверности. | - Умение строить логические умозаключения на основании поступающих информации и данных. | * Основные принципы построения логических умозаключений на основании поступающих информации и данных. * Основы деловой коммуникации. * Методы обработки текстовой и графической информации. * Основы цифровой грамотности. |
| ***Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защите интересов личности,***  ***общества и государства, соблюдать нормы профессиональной этики*** | | |
| *Трудовые действия* | *Необходимые умения* | *Необходимые знания* |
| * Информирование персонала об угрозах безопасности информации. * Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации. * Информирование персонала об   ответственности за не санкционированное разглашение различных видов тайн. | * Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации. * Уметь осуществлять поиск новой методической документации по регламентации мероприятий и оказанию услуг в области защиты информации. | * Нормативные правовые акты в области защиты информации. * Организационные меры по защите информации. * Основы деловой коммуникации. * Методы обработки текстовой и графической информации. * Основы цифровой грамотности. |
| ***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 объектов защиты*** | | |
| *Трудовые действия* | *Необходимые умения* | *Необходимые знания* |
| - Ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации  автоматизированных | * Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации. * Конфигурировать | * Понятие угрозы информационной безопасности. * Классификацию угроз информационной безопасности. |
| систем.  - Ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем. | параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией. | * Нормативные правовые акты в области защиты информации. * Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях. * Организационные меры по защите информации. * Особенности применения программных и программно- аппаратных средств защиты информации в   автоматизированных системах.   * Технические средства защиты информации. * Методы обработки текстовой и графической информации. * Основы цифровой грамотности. |

# Категория слушателей

* 1. Образование: среднее профессиональное и (или) высшее образование
  2. Квалификация: требования к квалификации не предъявляются
  3. Наличие опыта профессиональной деятельности: требования к опыту профессиональной деятельности не предъявляются
  4. Предварительное освоение иных дисциплин/курсов /модулей: освоение иных дисциплин/курсов/модулей не требуется

# Учебный план программы «Кибербезопасность и кибергигиена: Level 0»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Кибербезопасность и кибергигиена | 64 | 20 | 36 | 8 |
| **Итоговая аттестация** | | 8 | Разработка проекта | | |
| **Итого** | | 72 | 20 | 36 | 8 |

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

**«Кибербезопасность и кибергигиена: Level 0»**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Наименование учебных модулей/темы** | **Трудоёмкость**  **(час)** | **Сроки**  **обучения** |
| 1. | Кибербезопасность и кибергигиена | 64 | C 01.11.2020 по  15.11.2020 |
| 1.1 | Кибербезопасность как один из ключевых  факторов устойчивого развития цифровой экономики. | 3 | 1.11.2020 |
| 1.2 | Кибергигиена: все о защите персональных  данных. | 10 | с 01.11.2020 по  03.11.2020 |
| 1.3 | Цифровые права граждан*.* | 4 | с 03.11.2020 по  04.11.2020 |
| 1.4 | Законодательство РФ в области конфиденциальной информации и  коммерческой тайны. Ответственность. | 4 | с 04.11.2020 по  05.11.2020 |
| 1.5 | Понятие организационной защиты  информации. | 8 | с 05.11.2020 по  06.11.2020 |
| 1.6 | Источники и классификация угроз  информационной безопасности. | 11 | с 07.11.2020 по  08.11.2020 |
| 1.7 | Основные средства и способы обеспечения информационной безопасности, принципы  построения систем защиты информации. | 10 | с 09.11.2020 по  10.11.2020 |
| 1.8 | Основные принципы создания системы  управления информационной безопасностью. | 7 | с 11.11.2020 по  12.11.2020 |
| 1.9 | Применение политик информационной  безопасности. | 7 | с 13.11.2020 по  14.11.2020 |
|  | Итоговая аттестация | 8 | 15.11.2020 |
| **Всего:** | | 72 |  |

1. **Учебно-тематический план программы «Кибербезопасность и кибергигиена: Level 0»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/**  **п** | **Модуль / Тема** | **Всего**  **, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекци и** | **практически е занятия** | **самостоятел ьная работа** |
| 1. | Кибербезопаснос ть и кибергигиена | 64 | 20 | 36 | 8 |  |
| 1.1 | Кибербезопаснос ть как один из ключевых факторов устойчивого развития цифровой  экономики. | 3 | 1 | 1 | 1 | тестирование |
| 1.2 | Кибергигиена: все о защите персональных  данных. | 10 | 4 | 5 | 1 | тестирование |
| 1.3 | Цифровые права  граждан*.* | 4 | 1 | 2 | 1 | тестирование |
| 1.4 | Законодательство  РФ в области конфиденциально й информации и коммерческой тайны.  Ответственность. | 4 | 1 | 2 | 1 | тестирование |
|  |  |  |  |  |
| 1.5 | Понятие организационной защиты  информации. | 8 | 2 | 5 | 1 | задание |
| 1.6 | Источники и классификация угроз  информационной безопасности. | 11 | 4 | 6 | 1 | тестирование |
| 1.7 | Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты  информации. | 10 | 4 | 6 |  | тестирование |
| 1.8 | Основные принципы создания системы управления  информационной безопасностью. | 7 | 1 | 5 | 1 | задание |
| 1.9 | Применение политик информационной  безопасности. | 7 | 2 | 4 | 1 | тестирование |
|  | Итоговая  аттестация | 8 |  |  |  |  |
|  | Итого | 72 | 20 | 36 | 8 |  |

1. **Учебная (рабочая) программа повышения квалификации**

**«Кибербезопасность и кибергигиена: Level 0»**

## Модуль 1. Кибербезопасность и кибергигиена

***Тема 1.1 Кибербезопасность как один из ключевых факторов устойчивого развития цифровой экономики (3 часа).***

*Понятие кибербезопасности. 9 органов власти и организаций, выступающих в роли регуляторов в сфере информационной безопасности РФ. Понятие критической информационной инфраструктуры (КИИ). Баланс между государственными требованиями к защищенности критической информационной инфраструктуры и темпами развития цифровых технологий. Статистика кибератак за последние годы. Причины роста кибератак во время пандемии*

## Тема 1.2. Кибергигиена: все о защите персональных данных (10 часов).

*Понятие персональных данных (ПДн). Правовые основания обработки ПДн. Проблема обработки и защиты персональных данных в России и мире. Функции регуляторов в области защиты ПДн. GDPR – европейский регламент защиты ПДн. Основные этапы обработки ПДн. Федеральный закон №152 - ФЗ «О персональных данных». Правила личной кибергигиены.*

## Тема 1.3. Цифровые права граждан (4 часа).

*Закон о цифровых правах. Основы законодательства РФ в области информационной безопасности. Доктрина и стратегия информационной безопасности РФ. Понятие и виды защищаемой информации. Основы международного законодательства в области защиты информации*

## Тема 1.4 Законодательство РФ в области конфиденциальной информации и коммерческой тайны. Ответственность (4 часа).

*Понятие конфиденциальной информации и коммерческой тайны. Указ президента*

*№188 «Об утверждении перечня сведений конфиденциального характера». Федеральный закон N 98-ФЗ "О коммерческой тайне". Понятие врачебной тайны. Ответственности за не санкционированное разглашение различных видов тайн*

## Тема 1.5. Понятие организационной защиты информации (8 часов).

*Понятие угрозы информационной безопасности. Классификация угроз информационной безопасности. Банк угроз ФСТЭК России. Анализ степени опасности угроз. Статистика реализации различных видов угроз. Анализ и оценка угроз информационной безопасности объекта цифровизации. Порядок проведения оценки опасности угрозы*

## Тема 1.6 Источники и классификация угроз информационной безопасности (11 часов).

*Методы и средства защиты информации. Основные принципы построения систем защиты информации. Обзор программно-аппаратных средств защиты информации. Обзор технических средств защиты информации. Анализ существующих методов и средств, применяемых для защиты информации. Электронная цифровая подпись и особенности ее применения. Защита информации в Интернете.*

## Тема 1.7. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации (10 часов).

*Методы и средства защиты информации. Основные принципы построения систем защиты информации. Обзор программно-аппаратных средств защиты информации. Обзор технических средств защиты информации. Анализ существующих методов и средств, применяемых для защиты информации. Электронная цифровая подпись и особенности ее применения. Защита информации в Интернете.*

## Тема 1.8 Основные принципы создания системы управления информационной безопасностью (7 часов).

*Понятие системы управления информационной безопасностью (СУИБ). Основные принципы создания СУИБ. Структура системы управления информационной безопасностью. Этапы построения системы защиты информации. Понятие аудита информационной безопасности. Основные задачи аудита информационной безопасности. Применение и назначение DLP и SIEM систем.*

## Тема 1.9 Применение политик информационной безопасности (7 часов).

*Политика безопасности как основа организации обеспечения защиты информации.*

*Комплект типовых документов по информационной безопасности организации.*

# Описание практико-ориентированных заданий и кейсов

|  |  |  |  |
| --- | --- | --- | --- |
| **№ темы**  **/модуля** | **Название модулья/темы** | **Наименование практического**  **занятия** | **Описание** |
| 1.1 | Кибербезопасность как один из ключевых факторов устойчивого развития цифровой экономики. | Практическая работа  № 1. Кибербезопасность как один из ключевых факторов устойчивого развития цифровой экономики. | Подготовить письменный ответ на вопрос: «Каким наиболее важным, с вашей точки зрения, аспектам кибербезопасности уделяется должное внимание со стороны государства, а каким необходимо уделять больше внимания». Дайте развернутый ответ и поясните  почему вы так считаете. |
| 1.2 | Кибергигиена: все о защите персональных данных. | Практическая работа  №2. Кибергигиена: все о защите персональных данных. | Проведите критический анализ того как вы организуете работу с личными персональными данными (в случае самозанятости) / Проведите критический анализ того как обрабатываются персональные данные в организации, в которой вы работаете. Оформить ответ в  виде схемы: Должно быть организовано/Реальное  положение организации |
|  |
| 1.3 | Цифровые права граждан*.* | Практическая работа  №3. Цифровые права граждан*.* | Подготовить письменный ответ на вопрос: «Какими я обладаю цифровыми правами  как гражданин РФ» |
| 1.4 | Законодательство РФ в области конфиденциальной информации и коммерческой тайны. Ответственность. | Практическая работа  №4. Законодательство РФ в области конфиденциальной информации и коммерческой тайны | Провести сравнительный анализ видов тайн с указанием ответственности за их разглашение. Ответ оформить в виде сводной таблицы в MS Word. |
| 1.5 | Понятие организационной защиты информации. | Практическая работа  №5. Понятие организационной защиты информации. | Разработайте схему деятельности должностных лиц для обеспечения информационной безопасности вашей организации / Разработайте схему для обеспечения информационной безопасности вашего вида  деятельности (в случае самозанятости) |
| 1.6 | Источники и классификация угроз информационной безопасности. | Практическая работа  №6. Источники и классификация угроз информационной безопасности | Постройте гистограмму выявленных угроз по основным типам на основе статистики за 2018-2020 год по данным «Лаборатории Касперского». 2.  Проанализируйте угрозы приведенные в банке угроз ФСТЭК России. |
| 1.7 | Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. | Практическая работа  №7. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. | Найдите информацию и технические характеристики для сертифицированных ФСТЭК России средств защиты информации:   * одно программно- аппаратное средство защиты информации от несанкционированного доступа; * одно программное средство защиты информации от вирусов; * одно техническое средство защиты информации от утечки по акустическому каналу; * одно техническое средство защиты информации от утечки по электромагнитному   каналу. |
| 1.8 | Основные принципы создания системы управления информационной безопасностью. | Практическая работа  №8. Основные принципы создания системы управления информационной безопасностью. | Найдите описание и функционал одной DLP и одной SIEM системы.  Оформите ответ в виде сравнительной таблицы для двух систем. |
| 1.9 | Применение политик информационной безопасности. | Практическая работа  №9. Применение политик информационной безопасности. | Разработайте парольную политику для своей организации. |

1. **Оценочные материалы по образовательной программе**
   1. **Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1** | 1. Вы используете почтовый ящик на обще доступом почтовом сервисе (mail.ru и другие) в рабочих целях?   а) Только для отправки срочных и важных писем.  б) Если в письме нет конфиденциальной информации.  **в) Пишу деловые письма только с рабочей почты.**  г) Да, только информацию предварительно архивирую с паролем.   1. Вам нужно отойти «на пару минут» – налить кофе или перекусить. Что вы точно сделаете, прежде чем уйти?   а) Спрошу, не принести ли чего-нибудь коллегам.  **б) Заблокирую компьютер.**  в) Закрою и сохраню все документы, с которыми работал(а).  г) Напишу в общем чате, что отлучусь ненадолго   1. Вам позвонили из федеральной налоговой службы и попросили   сообщить некоторую | 1. Что из перечисленного может являться объектом КИИ?   Выберите один или несколько ответов:   * 1. Мясоперерабатывающий комбинат   2. **Больница**   3. **Банк**   4. **Карьер**   5. **Научно-**   **исследовательский институт**   * 1. Торговая точка   2. **Атомная электростанция**   3. **Металлургический комбинат**  1. Вам нужно отойти «на пару минут» – налить кофе или перекусить. Что вы точно сделаете, прежде чем уйти?   д) Спрошу, не принести ли чего-нибудь коллегам.  **е) Заблокирую компьютер.**  ж) Закрою и сохраню все документы, с которыми работал(а).  з) Напишу в общем чате, что отлучусь ненадолго   1. Попытка реализации угрозы – …   а) взлом **б) атака** в) хакинг  г) нападение | 1. Когда и где началась первая промышленная революция?   Выберите один ответ:   * 1. **Процесс начался в Англии в 1740–1780-х годах**   2. Процесс начался в США в 1860–1880-х годах   3. Процесс начался в России в 1860–1880-х годах   4. Процесс начался в США в 1740–1780-х годах   5. Процесс начался в Англии в 1860–1880-х годах  1. Когда и где началась вторая промышленная революция?   Выберите один ответ:  a. Процесс начался в Англии в 1740–1780-х годах  b. В 1710–1770-х годах технологическая революция быстро охватила Западную Европу, США, Российскую империю и Японию  c. Процесс начался в  США в 1740–1780-х  годах |
|  | информацию о сотрудниках организации, что вы сделаете?  а) Скажете, что у вас нет такой информации.  б) Попросите, чтобы они приехали лично.  **в) Предложите им сделать запрос на официальном бланке и прислать на e-mail компании.**  г) Положите трубку, не вступая в разговор.   1. Совокупность целенаправленных действий по обеспечению безопасности данных это   **защита информации**   1. Попытка реализации угрозы – …   а) взлом **б) атака** в) хакинг  г) нападение | 1. Выберите термин соответствующий определению: Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с   целью защиты информации.   * 1. Организационно- планирующие документы   2. **Объект защиты информации**   3. Субъект защиты информации:   4. Защищаемый объект информатизации   5. Что из перечисленного можно отнести к объектам защиты информации:   1. **выделенное помещение** 2. **охраняемая территория** 3. человек, обладающий информацией 4. **информация и (или) информационные ресурсы объекта информатизации** 5. **здание (сооружение**) | **d. В 1860–1870-х годах технологическая революция быстро охватила Западную Европу, США,**  **Российскую империю и Японию**   1. Когда и где началась третья промышленная революция?   Выберите один ответ:   * 1. Началась в 1960-х гг в США   2. **Началась в 1960-х гг в странах Европы**   3. Началась в 1920-х гг в странах Европы   4. Началась в 1860-х гг в странах Европы   5. Началась в 1960-х гг в России  1. Когда и где началась четвертая промышленная революция?   Выберите один ответ:   * 1. Началась в 2010 году в России.   2. Началась в 2016 году в Швейцарии.   3. **Началась в 2012 году в Германии.**   4. Началась в 1960 гг. в странах Европы.   5. Началась в 2000 году в США.   5. Что из перечисленного может являться объектом КИИ?  Выберите один или несколько ответов: a.  Мясоперерабатывающий комбинат   1. **Больница** 2. **Банк** 3. **Карьер** 4. **Научно-**   **исследовательский институт**   1. Торговая точка 2. **Атомная**   **электростанция** |
|  |  |  | **h. Металлургический**  **комбинат** |

* 1. **описание показателей и критериев оценивания, шкалы оценивания.**

Шкала оценивания входного контроля

|  |  |
| --- | --- |
| Оценка | Результат |
| Ниже 50% | Слушатель не может начать изучению по новому модулю,  рекомендуется изучить текущий модуль еще раз. |
| 50-99% | Слушатель может начать изучение по новому модулю, но  необходимо снова изучить темы, по которым вышло 0 баллов |
| 100% | Слушатель готов к прохождению нового модуля |

Шкала оценивания промежуточного контроля

|  |  |
| --- | --- |
| Оценка | Результат |
| Ниже 50% | Слушателю стоит внимательнее изучать материалы по  текущему модулю |
| 50-99% | Слушатель хорошо справляется и изучением текущего модуля,  но стоит обратить внимание на вопросы с оценкой 0 баллов |
| 100% | Слушатель отлично справляется с изучением текущего модуля |

Шкала оценивания итогового контроля

|  |  |
| --- | --- |
| Оценка | Результат |
| <50% | незачет |
| >=50% | зачет |

# примеры контрольных заданий по модулям или всей образовательной программе.

Пример задания для итоговой аттестации выполнения проекта

Постройте дерево атак с учетом вероятности возникновения угроз на основе статистики за 2020 год по данным «Лаборатории Касперского»

# тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий.

* 1. **описание процедуры оценивания результатов обучения.**

Для оценки результатов обучения слушателям предлагается выполнить проект, пример задания для проекта представлен в пункте 8.3

Оценка итоговой аттестации:

|  |  |  |
| --- | --- | --- |
| Критерий оценивания | Количество  баллов | Характеристика |
| Программное обеспечение, в котором выполнен проект | 0 | Скриншот рисунка на бумаге |
| 1 | Microsoft Word (или другие схожие по функционалу  программы) |
| 2 | Microsoft Visio (или другие схожие по функционалу  программы) |

|  |  |  |
| --- | --- | --- |
| Стиль оформления дерева атак | 0 | Описан в виде не систематизированного текста |
| 2 | Оформлен в виде концептуальной диаграммы  (дерева) |
| Выбор угроз | 0 | Выбраны не актуальные угрозы |
| 1 | Выбраны частично актуальные угрозы |
| 2 | Выбраны актуальные угрозы |
| Использование данных  «Лаборатории Касперского» за 2020 год | 0 | Не использованы |
| 2 | Использованы |

Шкала оценки:

|  |  |
| --- | --- |
| Количество набранных баллов | Результат |
| 0-4 | незачет |
| 5-8 | зачет |

# Организационно-педагогические условия реализации программы

* 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 полученно м согласии на обработку персональ**  **ных данных** |
| **1** | Михайлов а Ульяна Владимир овна | ФГБОУ ВО  «МГТУ им. Г.И.  Носова» к.т.н., доцент по системам и методам защиты информации  , доцент кафедры информатик и и информацио нной безопасност и | [https://www.magtu.ru/st](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/mihajlova-ulyana-vladimirovna.html) [aff/personalnye-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/mihajlova-ulyana-vladimirovna.html) [stranitsy-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/mihajlova-ulyana-vladimirovna.html) [prepodavatelej/item/mih](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/mihajlova-ulyana-vladimirovna.html) [ajlova-ulyana-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/mihajlova-ulyana-vladimirovna.html) [vladimirovna.html](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/mihajlova-ulyana-vladimirovna.html) |  | **+** |
| **2** | Афанасьев | ФГБОУ ВО | [https://www.magtu.ru/st](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/afanaseva-margarita-vladimirovna.html) |  | **+** |
|  | а | «МГТУ им. | [aff/personalnye-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/afanaseva-margarita-vladimirovna.html) |  |
|  | Маргарита | Г.И. | [stranitsy-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/afanaseva-margarita-vladimirovna.html) |  |
|  | Владимир | Носова» | [prepodavatelej/item/afa](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/afanaseva-margarita-vladimirovna.html) |  |
|  | овна | старший | [naseva-margarita-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/afanaseva-margarita-vladimirovna.html) |  |
|  |  | преподавате | [vladimirovna.html](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/afanaseva-margarita-vladimirovna.html) |  |
|  |  | ль кафедры |  |  |
|  |  | информатик |  |  |
|  |  | и и |  |  |
|  |  | информацио |  |  |
|  |  | нной |  |  |
|  |  | безопасност |  |  |
|  |  | и |  |  |
|  | Лукьянов | ФГБОУ ВО | [https://www.magtu.ru/st](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/lukyanov-georgij-igorevich.html) |  | **+** |
| Георгий | «МГТУ им. | [aff/personalnye-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/lukyanov-georgij-igorevich.html) |  |
| Игоревич | Г.И. | [stranitsy-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/lukyanov-georgij-igorevich.html) |  |
|  | Носова» | [prepodavatelej/item/luk](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/lukyanov-georgij-igorevich.html) |  |
|  | старший | [yanov-georgij-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/lukyanov-georgij-igorevich.html) |  |
|  | преподавате | [igorevich.html](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/lukyanov-georgij-igorevich.html) |  |
|  | ль кафедры |  |  |
|  | информатик |  |  |
|  | и и |  |  |
|  | информацио |  |  |
|  | нной |  |  |
|  | безопасност |  |  |
|  | и |  |  |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки, материалы курса,  учебная литература |
| дистанционные образовательные  технологии с элементами геймификации | <http://m.idpo.magtu.ru/course/view.php?id=198> |
| 1. Раздельно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками самостоятельной работы, практических работ и тестированием по каждой теме содержания курса, а именно кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании. 2. Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических практических самостоятельных работ, анализ ошибок,   совместный поиск вариантов рационального решения проблемы. |  |
| 1. Контекстное обучение – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками организации обеспечения безопасности информации, обучающийся приобретет способность участвовать в разработке защищенных организационных систем по профилю своей профессиональной деятельности. 2. Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации. 3. Игровые технологии – формы учебных занятий с использованием предложенных сценарных условий с использованием игровых технологий, а именно ролевая игра – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.   Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. |  |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
|  | Мазнин Д. Н., Баранкова И.И., Михайлова У.В. и др. Организация обработки и защиты ПДн в вузе: учебное пособие – Магнитогорск: ФГБОУ ВО "Магнитогорский государственный технический университет им. Г. И. Носова". Текст: электронный. Текст: электронный. - URL: <https://magtu.informsystema.ru/> (дата  обращения: 15.02.2020). |
|  | 1. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-  М, 2019. - 400 с. - (Высшее образование). - DOI: |
|  | https://doi.org/10.12737/1759-3. - ISBN 978-5-16- 106478-8. - Текст: электронный. - URL: <https://new.znanium.com/catalog/product/1018901>  (дата обращения: 26.02.2019). |
|  | 2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. — Москва : ИД  «ФОРУМ» : ИНФРА-М, 2019. — 592 с.: ISBN  978-5-16-106148-0. - Текст: электронный. - URL:  <https://new.znanium.com/catalog/product/996789> (дата обращения: 15.02.2020). |
|  | 3. Внуков, А.А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. —  URL: <https://urait.ru/bcode/422772>(дата обращения: 15.02.2020). |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекция | Компьютер с доступом в Интернет |
| Практическая работа | Компьютер с доступом в Интернет, Microsoft PowerPoint, Microsoft Word, Microsoft Excel, Microsoft Visio (или другие схожие по функционалу  программы) |
| Самостоятельная работа | Компьютер с доступом в Интернет, Microsoft PowerPoint, Microsoft Word, Microsoft Excel, Microsoft Visio (или другие схожие по функционалу  программы) |

ПАСПОРТ КОМПЕТЕНЦИИ

Кибербезопасность и кибергигиена: Level 0.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова»

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Наименование компетенции | Управление информацией и данными | |
| 2 | Указание типа компетенции | общепрофессиональная | |
| 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:   * Современные стандарты информационного взаимодействия систем.   Уметь:   * Выявлять информационные потребности автоматизируемых подразделений.   Владеть:   * Навыком организации сбора данных о запросах и потребностях заказчика.   Навыком обработки результатов с применением современных информационных технологий и технических средств | |
| 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 средства обработки текстовой и числовой информации.  Умеет искать нужные источники информации и данные.  Владеет инструментами поиска информации |
|  |  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знает основы цифровой грамотности.  Умеет анализировать найденную информацию. Владеет навыком  использования информационных ресурсов |
|  |  |  |  |
|  |  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает алгоритмы анализа информационного пространства.  Умеет передавать информацию с помощью цифровых средств.  Владеет навыком эффективного использования полученной информации для решения простых задач |
|  |  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно  влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает современные стандарты информационного взаимодействия систем. Умеет организовать процедуру обработки и хранения персональных данных в соответствии с требованиями законодательства.  Владеет навыком эффективного использования полученной информации для создания новых решения сложных задач в условиях неопределенности. |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной  компетенции | Способность использовать возможности компьютера и цифровой среды | |
| 6 | Средства и технологии оценки | Практические задания и тесты | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. | | Наименование компетенции | | Критическое мышление в цифровой среде | | |
| 2. | | Указание типа компетенции | | профессиональная | | |
| 3. | | Определение, | | Под компетенцией понимается способность к поиску | | |
|  | | содержание и | | новых решений в условиях цифровизации | | |
|  | | основные сущностные | |  | | |
|  | | характеристики | | Слушатель должен | | |
|  | | компетенции | | Знать:  Специфические особенности функционирования подразделений, подлежащих автоматизации  Уметь: | | |
|  | |  | | Проверять (верифицировать) архитектуру | | |
|  | |  | | информационной системы | | |
|  | |  | | Владеть: | | |
|  | |  | | Навыком осуществления экспертной поддержки анализа требований.  Навыком написания экспертных заключений по вариантам | | |
|  | |  | | архитектуры информационной 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 архитектуры информационных систем Умеет оценивать информацию.  Владеет инструментарием для сбора и обработки информации | |
|  | |  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, | Знает особенности функционирования IoT- систем.  Умеет проверять (верифицировать) архитектуру типовой IoT- системы  Владеет | |
|  | |  | | сложности.) |  | |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает инструменты для анализа функционирования IoT-систем.  Умеет осуществлять экспертную поддержку анализа требований.  Владеет навыком верификации архитектуры IoT- системы. | |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает специфические особенности функционирования подразделений, подлежащих автоматизации.  Умеет верифицировать архитектуру IoT- системы в условиях неопределенности. Владеет навыком оказания экспертной поддержки анализа требований. | |
| 5. | | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Способность использовать возможности компьютера | | |
| 6. | | Средства и технологии оценки | | Практические задания | | |
| 1 | Наименование компетенции | | Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защите  интересов личности, общества и государства, соблюдать нормы профессиональной этики. | | | |
| 2 | Указание типа компетенции | | профессиональная | | | |
| 3 | Определение, содержание и основные сущностные характеристики компетенции | | Компетенция предполагает осознание важности и необходимости обеспечения информационной безопасности в организации или на предприятии, а так же способность донести эту информацию до других людей.  Знать:   * Нормативные правовые акты в области защиты информации. * Организационные меры по защите информации. * Основы деловой коммуникации. * Методы обработки текстовой и графической информации. * Основы цифровой грамотности. Уметь: * Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации. * Уметь осуществлять поиск новой методической документации по регламентации мероприятий и оказанию услуг в области защиты информации   Владеть:   * Навыком информирования персонала об угрозах безопасности информации. * Навыком информирования персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации. * Навыком информирования персонала об ответственности за не санкционированное разглашение   различных видов тайн.. | | | |
| 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 нормативные правовые акты в области защиты информации.  Владеет основами деловой коммуникации,- методами обработки текстовой и графической информации. |
|  |  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | | | Знает способы оформления документации по регламентации мероприятий и оказанию услуг в области защиты информации.  Умеет читать  документацию по регламентации мероприятий и оказанию услуг в области защиты информации.  Владеет навыком анализа информации |
|  |  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | | | Знает перечень организационных мер по защите информации.  Умеет оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации  Владеет навыком использования полученной информации |
|  |  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно  влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | | | Знает основы кибербезопасности  Умеет осуществлять поиск новой методической документации по регламентации мероприятий и оказанию услуг в области защиты информации.  Владеет навыком изложения перечня информации для информирования персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных  средств защиты информации. |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость  владения другими | | Способность использовать возможности компьютера и цифровой среды | | | |
|  | компетенциями для  формирования данной компетенции | |  | | | |
| 6 | Средства и технологии оценки | | Практические задания и тесты | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Наименование компетенции | 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 объектов защиты. | |
| 2 | Указание типа компетенции | профессиональная | |
| 3 | Определение, содержание и основные сущностные характеристики компетенции | Компетенция предполагает способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации, а также знание типовых средств и методов защиты информации в локальных и глобальных вычислительных сетях и технические средства защиты информации.  Знает:   * Понятие угрозы информационной безопасности. * Классификацию угроз информационной безопасности. * Нормативные правовые акты в области защиты информации. * Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях. * Организационные меры по защите информации. * Особенности применения программных и программно- аппаратных средств защиты информации в автоматизированных системах. * Технические средства защиты информации. * Методы обработки текстовой и графической информации. * Основы цифровой грамотности. Умеет: * документацию по регламентации мероприятий и оказанию услуг в области защиты информации. * Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией   Владеет:   * навыком ведения протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем. * навыком ведения протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем. | |
| 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 понятие угрозы информационной безопасности.  умеет классифицировать угрозы информационной безопасности.  Владеет нормативными правовыми актами в области защиты информации. |
|  |  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знает типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях.  Умеет использовать  методы обработки текстовой и графической информации.  Владеет основами цифровой грамотности. |
|  |  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает особенности применения программных и программно-аппаратных средств защиты информации в  автоматизированных системах.  Умеет применять организационные меры по защите информации.  Владеет навыком использования типовых средств и методов защиты информации в локальных и глобальных  вычислительных сетях. |
|  |  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно  влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает программные, программно-аппаратные и технические средства защиты информации.  Умеет использовать особенности применения программных, программно- аппаратных и технических средств защиты информации в  автоматизированных системах.  Владеет навыком применения программных и программно-аппаратных |
|  |  |  | средств защиты информации в  автоматизированных системах. |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной  компетенции | Способность использовать возможности компьютера и цифровой среды | |
| 6 | Средства и технологии оценки | Практические задания и тесты | |

# Рекомендаций к программе от работодателей:

# 

# d:\Users\georgievskikh.n\Desktop\Рекомендательное письмо Консом СКС.jpg

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

|  |  |
| --- | --- |
| **Цели получения персонального цифрового сертификата** | |
| **текущий статус** | **цель** |
| **Развитие компетенций в текущей сфере занятости** | |
| работающий по найму в организации, на предприятии  работающий по найму в организации, на предприятии  работающий по найму в организации, на предприятии  временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.)  временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.) | развитие профессиональных качеств повышение заработной платы  смена работы без изменения сферы профессиональной деятельности  повышение уровня дохода  сохранение и развитие квалификации |

|  |  |
| --- | --- |
| Утверждаю  ректор ФГБОУ ВО «МГТУ им. Г.И. Носова» | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.В. Чукин |
|  | М.П. |