# I. Паспорт Образовательной программы

**«Защита информации»**

|  |  |
| --- | --- |
| **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 | Защита информации |
| 2.2 | Ссылка на страницу программы | [http://idpo.magtu.ru/index.php/component/jsho](http://idpo.magtu.ru/index.php/component/jshopping/product/view/79/749?Itemid=0)  [pping/product/view/79/749?Itemid=0](http://idpo.magtu.ru/index.php/component/jshopping/product/view/79/749?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 | 36 |

|  |  |  |
| --- | --- | --- |
|  | 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) |  |
| 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://edu.softline.com/vendors/softline/tehnicheskaya-zashhita-informacii-organizaciya-zashhity-informacii-ogranichennogo-dostupa-ne-soderzhashhej-svedeniya-sostavlyayushhie-gosudarstvennuyu-tajnu/>  <https://www.cntiprogress.ru/seminarsforcolumn/12659.aspx>  <https://itsecurity.ru/catalog/pk123/> |
| 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 | Тестирование |
| 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**

В ходе обучения по программе повышения квалификации «Защита информации» у слушателей будут сформированы следующие компетенции:

* + Администрирование систем защиты информации автоматизированных

систем

* Обеспечение работоспособности систем защиты информации при

возникновении нештатных ситуаций

Для обучения по программе слушатель должен:

* + знать предметную область; базовые принципы работы с информацией, основы информационного поиска, базовые нормативные акты РФ;
  + уметь: устанавливать и изучать требуемое ПО, осуществлять информационный поиск;
  + владеть навыками уверенной работы на компьютере.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому так необходимо знать основы обеспечения информационной безопасности компьютерных систем и сетей. В ходе обучения слушатели узнают не только основы обеспечения защиты информации, но и выполнят практические работы для закрепления полученных знаний. Практические задания охватываю разносторонние сферы деятельности, что позволит слушателям после окончания курса применять полученные знания, умения, навыки в повсеместной жизни.



# ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1. **Цель программы**

Повышение профессионального уровня слушателей в сфере обеспечения защиты информации в рамках имеющейся квалификации

# Планируемые результаты обучения:

Программа разработана с учетом требований профессионального стандарта № 843

«Специалист по защите информации в автоматизированных системах», Приказ Министерства труда и социальной защиты РФ от 15.09.2016 № 522н.

По окончании обучения планируется достижение слушателями следующих результатов по реализации обобщенных трудовых функции В Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (уровня квалификации 6);

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

|  |  |  |
| --- | --- | --- |
| ***Администрирование систем защиты информации автоматизированных систем*** | | |
| *Трудовые действия* | *Необходимые умения* | *Необходимые знания* |
| * Обеспечение | * Устанавливать и | * Программно- |
| безопасности | настраивать программные | аппаратные средства защиты |
| информации с учетом | средства с учетом | информации |
| требования эффективного | требований по обеспечению | автоматизированных систем |
| функционирования автоматизированной | защиты информации   * Использовать | * Основные меры по защите информации в |
| системы | криптографические методы и | автоматизированных системах |
|  | средства защиты |  |
|  | информации в |  |
|  | автоматизированных |  |
|  | системах |  |
|  | * Анализировать |  |
|  | события, связанные с |  |
|  | защитой информации в |  |
|  | автоматизированных |  |
|  | системах |  |
| ***Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций*** | | |
| *Трудовые действия* | *Необходимые умения* | *Необходимые знания* |
| * Восстановление | * Классифицировать и | * Программно- |
| после сбоев и отказов | оценивать угрозы | аппаратные средства |
| программного | информационной | обеспечения защиты |
| обеспечения | безопасности | информации |
| автоматизированных | * Применять | автоматизированных систем |
| систем | программные средства | * Организационные |
|  | обеспечения безопасности | меры по защите информации |
|  | данных |  |

# 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 «Защита информации»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Защита информации | 70 | 12 | 36 | 22 |
| Итоговая аттестация | | 2 | тестирование | | |
|  | | 72 |  |  |  |

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

**«Защита информации»**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Наименование учебных модулей/темы** | **Трудоёмкость**  **(час)** | **Сроки**  **обучения** |
| 1 | Защита информации | 70 | С 01.11.2020 по  14.11.2020 |
| 1.1 | Сущность и понятие защиты информации | 10 | С 01.11.2020 по  02.11.2020 |
| 1.2 | Угрозы безопасности информации | 10 | С 03.11.2020 по  04.11.2020 |
| 1.3 | Административный уровень защиты  информации | 10 | С 05.11.2020 по  06.11.2020 |
| 1.4 | Процедурный уровень защиты информации | 12 | С 07.11.2020 по  09.11.2020 |
| 1.5 | Программные средства защиты  информации | 18 | С 10.11.2020 по  13.11.2020 |
| 1.6 | Криптографические методы защиты  информации | 10 | С 13.11.2020 по  14.11.2020 |
|  | Итоговая аттестация | 2 | 15.11.2020 |
| **Всего:** | | 72 |  |

1. **Учебно-тематический план программы «Защита информации»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/ п** | **Модуль / Тема** | **Всего**  **, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекци**  **и** | **практически**  **е занятия** | **самостоятельна**  **я работа** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Защита  информации | 70 | 12 | 36 | 22 |  |
| 1.1 | Сущность и  понятие защиты информации | 10 | 2 | 4 | 4 | Практическа я работа |
| 1.2 | Угрозы  безопасности информации | 10 | 2 | 4 | 4 | Практическа я работа |
| 1.3 | Административны  й уровень защиты информации | 10 | 2 | 4 | 4 | Практическа я работа |
| 1.4 | Процедурный уровень защиты  информации | 12 | 2 | 6 | 4 | Практическа я работа |
| 1.5 | Программные средства защиты  информации | 18 | 2 | 12 | 4 | Практическа я работа |
| 1.6 | Криптографическ ие методы защиты  информации | 10 | 2 | 6 | 2 | Практическа я работа |
|  | Итоговая  аттестация | 2 |  |  |  | Тестировани  е |
|  | Итого | 72 | 12 | 36 | 22 |  |

1. **Учебная (рабочая) программа повышения квалификации «Защита информации»**

***Модуль 1. Защита информации (70 часов)***

Тема 1.1 Сущность и понятие защиты информации (10 часов)

*Основные понятия. Значение информационной безопасности для субъектов информационных отношений. Понятие и сущность защиты информации. Цели и*

*концептуальные основы защиты информации. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой информации*

Тема 1.2 Угрозы безопасности информации (10 часов)

*Угрозы информационной безопасности и защиты информации.*

*Дестабилизирующее воздействие на защищаемую информацию. Классификация видов угроз информационной безопасности по различным признакам. Несанкционированный доступ к информации*

Тема 1.3 Административный уровень защиты информации (10 часов)

*Политика безопасности. Программа безопасности. Оценка рисков и базовый уровень защиты.*

Тема 1.4 Процедурный уровень защиты информации (12 часов)

*Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ*

Тема 1.5 Программные средства защиты информации (18 часов)

*Защита программного обеспечения от несанкционированного доступа. Краткий обзор существующих на рынке средств защиты информации от несанкционированного доступа. Задача защиты от вмешательства посторонних лиц и аппаратные средства аутентификации. Удаление информации с заданными требованиями.*

Тема 1.6 Криптографические методы защиты информации (10 часов)

*Методы криптографии. Средства криптографической защиты информации.*

*Криптографические преобразования. Шифрование и дешифрование информации. Цифровая подпись. Стеганография*

# Описание практико-ориентированных заданий и кейсов

|  |  |  |  |
| --- | --- | --- | --- |
| **№ темы**  **/модул я** | **Название темы/модуля** | **Наименование практического занятия** | **Описание** |
| 1.1 | Сущность и понятие защиты информации | Практическая работа №1. Надежность и достоверность информации. Сервисы определения надежности ресурса в Интернет. | **Задание 1. Найти ресурс Федерального Госоргана**  Найдите официальный ресурс Федерального Госоргана, укажите его и поясните, почему, на ваш взгляд, он является достоверным.  **Задание 2. Найти ресурс областного Госоргана**  Найдите официальный ресурс областного Госоргана, укажите его и поясните, почему, на ваш взгляд, он является достоверным.  **Задание 3. Найти новостной ресурс** Найдите официальный новостной ресурс, укажите его и поясните, почему, на ваш взгляд, он является достоверным  **Задание 4. Угрозы доступности, целостности и конфиденциальности личной информации.**  Кейсы  **Задание 5. Письма счастья**  Кейсы  **Задание 6. Мобильные приложения.**  Кейсы  **Задание 7. Манипуляции действиями пользователя**  Кейсы |
| 1.2 | Администрати  вный уровень защиты | Практическая работа №2.  Определение угроз и модели нарушителя | Проанализировать представленную  предметную область, определить угрозы, разработать модель нарушителя, оценить |

|  |  |  |  |
| --- | --- | --- | --- |
|  | информации | предметной области. Оценка рисков нарушения безопасности. Выработка рекомендаций  по снижению риска. | риски нарушения безопасности по заданным параметрам |
| 1.3 | Процедурный уровень защиты информации | Практическая работа №3. Аудит защищенности сетей | **Задание 1. Конфигурация компьютера** [SysInfo Detector](http://sysinfo-detector.ru/download/) – программа для сбора информации о конфигурации компьютера. Позволяет определить установленные устройства, их тип, модель и прочую информацию, даже при отсутствии в системе драйверов. Это возможно, благодаря сбору информации не из реестра Windows, а опрашивая непосредственно сами устройства на аппаратном уровне.   1. Изучите конфигурацию вашего компьютера с помощью программы SysInfo Detector. 2. Предоставьте отчет преподавателю в виде скриншотов работы программы с комментариями. 3. Какие программы на вашем ПК не являются лицензионными?   **Задание 2. Нелицензионное ПО**  Lpro – программа для проверки лицензий установленных программ с автоматическим и ручным поиском.  Программа получает список установленного программного обеспечения от операционной системы, и далее поочередно сравнивает с базой данных.  Найденные совпадения отображает в таблице. Полученные результаты можно экспортировать в Excel и т.д.   1. С помощью программы Lpro проверьте, какие программы на вашем ПК не являются лицензионными. 2. Предоставьте отчет преподавателю в виде скриншотов работы программы с комментариями.   Задание 3. Мониторинг и защита Wi-Fi сетей  Сканер беспроводных локальных сетей [Acrylic WiFi Home](https://www.acrylicwifi.com/ru/%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82%D1%8B-%D0%B4%D0%BB%D1%8F-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%B8-%D0%B8%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8/%D1%81%D0%BA%D0%B0%D0%BD%D0%B5%D1%80-%D1%81%D0%B5%D1%82%D0%B5%D0%B9-wi-fi-acrylic-wifi-free/) является урезанной версией коммерческого решения компании Tarlogic Security.  [NetSpot](https://www.netspotapp.com/ru/) – мощная программа для поиска, анализа и диагностики беспроводных Wi- Fi-сетей. Если вы профессионально занимаетесь проектированием (созданием) беспроводных сетей или хотите настроить наилучшим образом точку доступа в своей квартире (офисе), то это приложение станет хорошим помощником, позволив построить карту покрытия своего помещения и  избежать появления так называемых |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | «мертвых» зон.   1. Изучите доступную вам Wi-Fi сеть с помощью программы Acrylic WiFi Home или программы NetSpot. 2. Предоставьте отчет преподавателю в виде скриншотов работы программы с комментариями. 3. Какие уязвимости обнаружила программа? |
| **Задание 4. Сетевые атаки и брандмауэры** [GlassWire](https://www.comss.ru/page.php?id=2176) – монитор сетевой безопасности и фаервол для контроля вашей сети.  Инструмент защищает компьютер, наглядно представляя сетевую активность на удобном графике и помогая выявлять необычное поведение вредоносных программ в Интернете.   1. Изучите возможности программы GlassWire. 2. Предоставьте отчет преподавателю в виде скриншотов работы программы с комментариями. 3. Какие уязвимости обнаружила программа? |
| Практическая работа №4. Парольная защита | **Задание 1. Генератор случайных паролей *Онлайн сервисы генерации паролей:*** [GenPas](http://genpas.peter23.com/) – генератор паролей с энтропией и выбором параметров генерации, плюс проверка на устойчивость паролей.  [Генератор паролей](https://calculator888.ru/generator-parolej/) – генерация 9 вариантов правильных и сложных для взлома паролей, с подробной инструкцией работы генератора.  [PassGenerator](https://passgenerator.ru/) – онлайн-программа, которая создает для вас уникальный пароль в соответствии с заданными параметрами.  [RandStuff](https://randstuff.ru/password/) – сервис генерации паролей, мудрых мыслей, предсказаний, чисел, счастливых билетов.  [Генератор паролей](https://xgenerate.com/) – онлайн-программа, которая создает для вас уникальный пароль в соответствии с заданными параметрами. ***Программы:***  [Random Password Generator](https://sonikelf.ru/attach/img/3glS9ET.zip) [Генератор паролей 1.5](https://www.softportal.com/get-42720-generator-parolej.html)   1. Все этапы представить в отчете в виде скриншотов экрана с комментариями. 2. Сгенерируйте по 2 пароля с помощью каждого ресурса и программы. 3. Определите, с каким ресурсом вам было комфортнее работать и почему. 4. Какой ресурс вы будете использовать в дальнейшем? |
|  | **Задание 2. Устойчивость пароля ко взлому** |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Стойкость пароля** – мера оценки времени, которое необходимо затратить на угадывание пароля или его подбор каким- либо методом, например, методом полного перебора. Оценка того, как много попыток (времени) в среднем потребуется взломщику для угадывания пароля. Другое определение термина – функция от длины пароля, его запутанности и непредсказуемости.  ***Онлайн сервисы проверки пароля на устойчивость ко взлому:***  [Kaspersky Lab](https://password.kaspersky.com/ru/) – проверка устойчивости пароля, примерное время взлома вашего пароля и сравнительный факт, что может произойти за это же время.  [Exploit](https://exploit.in/passcheck/) – сервис проверки устойчивости пароля.  [Надежность пароля](http://earninguide.biz/passwordmeter.php) – проверка устойчивости пароля в баллах, отчётность по баллам.  [HOW SECURE IS MY PASSWORD](https://howsecureismypassword.net/)? –  проверка устойчивости пароля, примерное время взлома вашего пароля, выявление причин уязвимости, советы в улучшении вашего пароля.  [Pwned Passwords](https://haveibeenpwned.com/Passwords) – проверка вашего пароля с базой данных всех взломанных паролей, если хоть раз этот пароль был взломан, то сервис вам об этом сообщит. Это не обязательно означает, что это хороший пароль, просто он не проиндексирован на этом сайте.   1. Все этапы представить в отчете в виде скриншотов экрана с комментариями. 2. Проверьте на устойчивость ко взлому сгенерируемые ранее пароли. 3. Сделайте сравнение результатов устойчивости с разных сервисов. 4. Проверьте свой часто используемый пароль в базе взломанных паролей. 5. Сделайте выводы. |
| Практическая работа №5.  Менеджер паролей | [Менеджер паролей онлайн](https://passgenerator.ru/menedzher-paroley)  **Пошаговая инструкция по**  **использованию менеджера паролей Шаг 1: Получаем пароль**  Вы можете скопировать ваш пароль откуда угодно, придумать самостоятельно или воспользоваться генератором паролей.  **Шаг 2: Сохраняем пароль с уникальным кодом для доступа**  Переходим на страницу сохранения пароля и вводим пароль. Дальше придумываем или генерируем код доступа, по которому в будущем мы сможем  получить наш сохраненный пароль. Код |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | доступа – это что-то вроде пин-кода от банковской карты или SIM-карты, его нужно запомнить или при необходимости сохранить в другом месте. Ваш код может быть коротким и совсем не сложным для вас, к примеру olga27 или 12345, допускается использование цифр, букв, символов и их комбинаций.  Пожалуйста, обратите внимание, что для всех комбинации с 1 по 9999 и всех единичные буквы латинского алфавита, уже сгенерированные по 20 постоянных паролей (одни основной и 19 дополнительных), которые можно использовать.  Далее вы можете выбрать количество (по умолчанию ноль) дополнительных похожих паролей, которые будут автоматически сгенерированы и сохранены вместе с вашим основным паролем. Эти пароли будут иметь нумерацию начиная с двух, так как единица - это ваш основной пароль, вы можете использовать любой из них, запомнив его порядковый номер.  Следующая дополнительная опция – это доступ по IP-адресу. Если вы хотите, чтобы сохраненный вами пароль имел ограниченный доступ для других пользователей вы можете указать IP- адреса, с которых можно будет его получить, для всех остальных пользователей сети доступ будет закрыт.  Еще одна дополнительная функция – это возможность выбрать период действия кода доступа и пароля, по истечении которого запись удаляется из системы. **Шаг 3: Находим наш пароль по коду** Для того чтобы найти сохраненный ранее пароль переходим на страницу получения пароля и вводим наш код. Ваш основной пароль отобразится под номером один на  оранжевом фоне, а дополнительные пароли (если они были созданы) будут иметь нумерацию начиная с двух.   1. Все этапы представить в отчете в виде скриншотов экрана с комментариями. 2. Заполните в онлайн-менеджере паролей свою базу паролей (используйте сгенерированные ранее или новые). Сделайте скрин своей базы паролей. 3. Проанализируйте возможности сохранения паролей, доступ к ним. 4. Когда удобно иметь такую базу? Какие уязвимости есть у подобного менеджера паролей? |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Программа **KeePass Password Safe –** свободная программа для хранения паролей, распространяемая по лицензии GPL. Программа разработана Домиником Райхлом для операционной системы Windows. Keepass является переносной программой и устанавливать её не обязательно.  Русскоязычный сайт поддержки программы [http://keepass.ru](http://keepass.ru/)   1. Все этапы представить в отчете в виде скриншотов экрана с комментариями. 2. Русифицируйте программу. 3. Создайте базу для хранения паролей. База должна называться вашей фамилией. 4. Установите пароль на базу. 5. Настройте:  * блокирование базы через 30 секунд; * блокирование базы при переключении пользователей.  1. Проанализируйте возможности сохранения паролей, доступ к ним. 2. Когда удобно иметь такую базу? Какие уязвимости есть у подобного менеджера паролей? |
| Практическая работа №6. Массовая рассылка писем | В процессе профессиональной или личной жизни зачастую возникает потребность в массовой рассылке почтовых сообщений, однако с соблюдением норм и правил профессионального этикета: адресат не должен видеть, что он один из множества, желательно личное обращение к адресату. Выполнить это стандартными средствами почтового сервера невозможно, поэтому нам понадобится установить программу Thunderbird и дополнение для нее.  **Thunderbird** – свободно распространяемая почтовая программа, которая работает в любой операционной системе.  Доступна на сайте [https://mozilla-](https://mozilla-russia.org/products/thunderbird/) [russia.org/products/thunderbird/](https://mozilla-russia.org/products/thunderbird/)  **Mail Merge** – это дополнение  для Thunderbird, которое позволяет разослать письма большому количеству адресатов. |
| 1.4 | Программные средства защиты информации | Практическая работа №7. Защита от несанкционированного доступа к информации | **Задание 1. Создание токен-приманки**   1. Переходим на официальный сайт [CanaryToken](http://whiteclouddrive.com/generate) 2. Заполняем поле ввода «Enter your Email Address». Вводим адрес электронной почты, куда будут приходить письма о том, что злоумышленник попался на нашу приманку.   Для примера можно воспользоваться |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | одноразовой почтой.   1. Во второе поле вводится путь до места, где будет лежать наша приманка на компьютере. 2. Далее выбираем создание токен- приманки в виде файла MS Word и нажимаем на ссылку для скачивания уже сформированного файла: 3. Дадим приманке имя, которое привлечет злоумышленника. Например, «мои пароли.docx». 4. Перемещаем «ловушку» в место, указанное при регистрации файла. 5. Для того, чтобы посмотреть механизм работы «приманки», достаточно просто его открыть и на вашу почту моментально придет письмо с предупреждением о том, что файл открыт и злоумышленник   «копается» в вашем компьютере (при открытии файла, можно увидеть, что сам файл пуст).   1. Самостоятельно создайте токен- приманку по описанному алгоритму. 2. Сделайте выводы об эффективности использования Honeypot и Honeytoken в вашей деятельности. 3. Предоставьте преподавателю отчет, содержащий скриншоты работы с сайтом и процессом создания токен-приманок, отчет о сработавших приманках.   **Задание 2. Закрытие доступа к папке в ОС Windows**  **Вариант 1. Архивация**   1. С помощью любого архиватора создайте архив с паролем из папки ФИО\_студента, папка по окончании создания пароля должна быть автоматически удалена. Сделайте скриншот параметров архивации. 2. Создайте архив, используя параметр   «Шифровать имена файлов» и архив без использования данного параметра. Сравните результаты. Сделайте выводы.   1. Сделайте выводы об эффективности использования архивации с паролем для обеспечения защиты от несанкционированного доступа. 2. Предоставьте преподавателю отчет, содержащий скриншоты процесса и выводы. Скриншоты должны позволять идентифицировать студента, выполнившего работу.   **Вариант 2. Сокрытие файлов**   1. Создайте папку ФИО. 2. С помощью пункта Свойства сделайте папку скрытой. Убедитесь, что она скрыта |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | от просмотра. Если папку видно, измените общие настройки папок соответствующим образом. Сделайте скриншоты каждого действия.   1. Создайте папку ФИО или сделайте видимой предыдущую папку. С помощью пункта Свойства измените значок папки на невидимый. Используя комбинацию клавиш «ALT» и цифровой панели «255» переименуйте папку. Изучите полученный результат. Где лучше всего разместить такую папку/файл? 2. Сделайте выводы об эффективности использования данных методов. 3. Предоставьте преподавателю отчет, содержащий скриншоты процесса. Скриншоты должны позволять идентифицировать студента, выполнившего работу.   **Задание 3. Анализ уязвимости интернет- логинов**  Have I Been Pwned? (Я Был Взломан?) – это интернет-сайт, разработанный в конце 2013 года, одним из сотрудников Microsoft, специалистом в области безопасности – Трой Хантом (Troy Hunt).  Сервис позволяет проанализировать сотни интернет-ресурсов подвергнутых взломам, хищению информации, утечкам и другим нарушениям данных. Он дает возможность любому желающему пользователю, проверить наличие персональной информации в базе скомпрометированных данных.   1. На ресурсе [**Have I Been Pwned**](https://haveibeenpwned.com/Passwords)проверьте адреса электронной почты, которые чаще всего используете для логинов на ресурсах.   Если почта будет замечена хотя бы в одном из «нарушений» открытом для общественности, то Вы увидите об этом сообщения: «Oh no – pwned!», в красном оформлении. Так же будет показана информация о сайтах, которые допустили утечку Ваших личных данных, когда именно и по какой причине   1. Проанализируйте полученные результаты. 2. Предоставьте преподавателю отчет, содержащий скриншоты процесса. Скриншоты должны позволять идентифицировать студента,   выполнившего работу. |
| Практическая работа №8.  Защита информации в | **Задание 1. Закрытие документа паролем**  1. Самостоятельно ознакомиться с |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | документах | возможностями настройки защиты информации в текстовом редакторе.   1. Настроить следующие способы защиты документа:    * Документ Фамилия\_Doc1 при открытии требует пароль на доступ к файлу, модификация файла запрещена (изменение текста невозможно).    * Документ Фамилия\_Doc2 открывается только для чтения.    * Документ Фамилия\_Doc3 при открытии требует пароль на доступ к файлу и редактирование (2 разных пароля).   **Задание 2. Создание документа с ограничением изменения текста**   1. Создайте документ, содержащий форму, ограниченную для изменения, но содержащую поля для заполнения.   Поля должны демонстрировать следующие параметры:   * + текст по умолчанию – этот текст будет автоматически подставляться в данное поле при создании документа на основе данной формы. Такой текст может быть изменен при условии, что в параметрах будет установлен флаг   «Разрешить изменения»;   * + максимальная длинна вводимого текста;   + формат текста, т.е. какими буквами будет написан вводимый в поле текст: прописными, строчными, первая буква первого вводимого слова начинается с прописной, остальные строчные, первые буквы каждого вводимого слова начинаются с прописной;   + поле «дата»   + подсказка для вводимых данных.  1. Создайте раздел, в котором можно вносить изменения в информацию. 2. Защитите документ таким образом, чтобы оставалась возможность редактирования полей и раздела. 3. Сохраните документ в виде шаблона ФИО.dot   **Документы MS Office Excel**  **Задание 3. Закрытие документа паролем**   1. Самостоятельно ознакомиться с возможностями настройки защиты информации в табличном редакторе. 2. Настроить следующие способы защиты документа:    * Документ Фамилия\_Ex1 при |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | открытии требует пароль на доступ к файлу.   * Документ Фамилия\_ Ex2 модификация файла запрещена (изменение текста невозможно). * Документ Фамилия\_ Ex3 есть защищенные скрытые листы, данные из которых обрабатываются на видимом листе. |
| Практическая работа №  9. Восстановление данных с помощью ПО | [Recuva](https://recuva.ru.uptodown.com/windows) – небольшая бесплатная утилита, которая предназначена для восстановления файлов, удаленных с ПК случайно или потерянных в результате программного сбоя или ошибки в работе приложений. Проста в использовании, не требует специальных знаний для успешного использования. Распространяется бесплатно. |
|  | **Задание 1.**  Создайте на своем рабочем диске папку  «Восстановление», в ней разместите файлы следующего вида: Фамилия.doc, \*.xls, \*.ppt,  \*.jpeg, \*.avi, \*.mp3, и папку Фамилия, в которой должны быть сохранена любая веб-страница с картинками (то есть содержит в себе папку, в которой находятся картинки со страницы и файл  \*.html). Содержимое файлов значения не имеет, размер файлов может быть любым, не равным 0. |
|  | **Задание 2.**  Удалите целиком папку «Восстановление» со своего компьютера (без помещения в Корзину). |
|  | **Задание 3.**  С помощью программы Recuva осуществите восстановление всех файлов,  находившихся в папке «Восстановление». |
| Практическая работа №  10. Безвозвратное удаление информации | [**Alternate File Shredder**](http://www.alternate-tools.com/pages/c_fileshredder.php?lang=ENG)  Программа предназначена для безвозвратного удаления отдельных файлов и папок.  **Задание 1. Создание файла.**   1. Создайте на рабочем столе файл   «ПаролиФИО.docx».   1. Внесите в него некоторые данные. |
|  | **Задание 2. Работа с программой Alternate File Shredder.**   1. Установите программу 2. Выберите файл «ПаролиФИО.docx». 3. Задайте количество итераций (если у вас ssd-диск, количество итераций задавайте не |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | более 2!).   1. Запустите уничтожение файлов. 2. Попробуйте восстановить удаленный файл с помощью программы Recuva или любой другой. 3. Сделайте выводы об эффективности данного способа.   **HDD Low Level Format Tool**  Утилита от сайта [HDDGURU](https://hddguru.com/software/HDD-LLF-Low-Level-Format-Tool/) предназначенная для низкоуровневого форматирования накопителей. Из возможностей можно выделить следующие: работает с интерфейсами S- ATA (SATA), IDE (E-IDE), SCSI, USB,  Firewire; поддерживает накопители следующих фирм-производителей: Maxtor, Hitachi, Seagate, Samsung, Toshiba, Fujitsu, IBM, Quantum, Western Digital; возможно форматирование Flash карт при использовании кардридера.  Утилита полностью уничтожит данные, проведет низкоуровневое форматирование и позволит изменить размер накопителя в пределах до 281 474 976 710 655 байт или 262143 гигабайт. Возможна работа с внешними устройствами через интерфейсы USB и Firewire. По возможности использует Ultra-DMA режим. Такой вид форматирования очищает таблицу разделов, MBR и каждый байт пользовательских данных.  **Внимание! Перед выполнением лабораторной работы убедитесь, что на флеш-карте отсутствует важная для вас информация!**  Весь рабочий процесс предоставить преподавателю в отчете в виде скриншотов экрана с комментариями.  **Задание 1. Удалите безвозвратно данные на флеш-носителе.**   1. Флеш-носитель должен называться вашей фамилией. 2. Разместите на носителе файл любого типа, названный вашей фамилией. 3. Убедитесь, что на флеш-носителе нет важной информации (восстановить ее будет невозможно!). 4. Запустите утилиту и проведите низкоуровневое форматирование вашего носителя. 5. Убедитесь, что форматирование окончено. 6. Попытайтесь открыть флеш-носитель |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | старндартными средствами операционной системы, зафиксируйте событие.   1. Попытайтесь восстановить файлы с флеш-носителя с помощью специализированных программ. 2. Сделайте выводы об эффективности данного способа. |
| 1.5 | Криптографич еские методы защиты информации | Практическая работа  №11. | **Задание 1. Шифровка методом замен**   1. Используя любой шифр, основанный на заменах, зашифровать свою фамилию и фразу из трех слов. 2. Зафиксируйте полученные криптограммы и ключи криптограммы. 3. Обменяйтесь криптограммами с товарищем, проделайте процедуру дешифрования. Убедитесь, что криптограммы расшифрованы правильно. 4. Сделайте выводы об эффективности данного способа. 5. Предоставьте преподавателю отчет, содержащий скриншоты процесса и выводы. Скриншоты должны позволять идентифицировать студента, выполнившего задание.   **Задание 2. Шифровка по методу Кардано**   1. Используя программу [«Шифратор](https://vbeg.ru/magazin/shifrator-reshyotka-kardano-v3/)   [«Решетка Кардано»»](https://vbeg.ru/magazin/shifrator-reshyotka-kardano-v3/) зашифруйте текстовое сообщение, длиной не менее 5 слов.   1. Зафиксируйте полученную криптограмму и ключ криптограммы. 2. Обменяйтесь криптограммой и ключом с товарищем, проделайте процедуру дешифрования. Убедитесь, что исходный текст совпал. 3. Сделайте выводы об эффективности данного способа. 4. Предоставьте преподавателю отчет, содержащий скриншоты процесса и выводы. Скриншоты должны позволять идентифицировать студента, выполнившего задание.   **Задание 3. Шифровка методом перестановок**   1. Самостоятельно изучите шифры простой и множественной подстановки. Выберите один, наиболее понятный для вас и с его помощью зашифруйте свою фамилию и фразу из трех слов. 2. Зафиксируйте полученные криптограммы и ключи криптограммы. 3. Обменяйтесь криптограммами с товарищем, проделайте процедуру дешифрования. Убедитесь, что криптограммы расшифрованы правильно. 4. Сделайте выводы об эффективности |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | данного способа.  5. Предоставьте преподавателю отчет, содержащий скриншоты процесса и выводы. Скриншоты должны позволять идентифицировать студента, выполнившего задание.  **Задание 4. Создание хеш-функции**   1. С помощью любого онлайн-генератора хеш-функции зашифруйте свою фамилию и любую фразу из двух слов. 2. Зафиксируйте полученные хеш- функции. 3. Обменяйтесь с товарищем кодовой фразой и ее хеш-функцией, определите вид алгоритма, сравните полученные цифровые слепки. 4. Предоставьте преподавателю отчет, содержащий скриншоты процесса и выводы. Скриншоты должны позволять идентифицировать студента, выполнившего задание.   **Задание 5. Криптосмайл**   1. Зашифруйте 5 названий фильмов, 5 названий книг и 5 строчек из песен с помощью смайлов 2. Обменяйтесь полученными криптограммами с товарищами. 3. Разгадайте криптограммы товарищей Пример:   Фильм    Ответ: Любовь и голуби Книга  Ответ: А.С. Грибоедов Горе от ума Песня  Ответ: Зеленоглазое такси |
| Практическая работа  №12. Защита информации с помощью стеганографии | **Задание 1. Определение метода шифрования**  Определите, какой метод сокрытия  информации: криптографический или стеганографический был использован в |



|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | данном случае. Обоснуйте ответ.  iVAMefl4B74  **Задание 2. Сокрытие данных в графических и музыкальных файлах.** [S-Tools](https://dfiles.ru/files/dx96er0z6) – программа для скрытия данных от посторонних глаз. Работает без инсталляции. Использует метод  стеганографии – данные прячутся в файлах графики (BMP или GIF) или музыкальном WAV-файле, которые внешне не отличаются от аналогичных файлов, не несущих спрятанной информации (картинку можно посмотреть, музыку можно послушать). Дело в том, что оцифрованные файлы (те же \*.bmp или  \*.wav) могут быть в определенной степени изменены, и это не повлияет на качество звука или изображения (вернее, эти изменения будут практически не заметны). Кроме этого, программа позволяет не только спрятать информацию во внешне ничем не примечательном файле, но и зашифровать ее.   1. В папке ФИО разместите 3 графических и 3 музыкальных файла под названиями ФИО1… ФИО3.bmp и ФИО1… ФИО3. Wav. 2. С помощью программы S-Tools (или любой другой аналогичной) спрячьте первую кодовую фразу в случайном графическом файле, вторую в любом wav- файле. 3. Обменяйтесь с товарищем папками с файлами. 4. Попытайтесь обнаружить, в каком из файлов находятся кодовые фразы. Найдите и расшифруйте их. 5. Предоставьте преподавателю отчет, содержащий скриншоты процесса и выводы. Скриншоты должны позволять идентифицировать студента, выполнившего задание.   **Задание 3. Определение метода шифрования и расшифровка QR-кода** |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | 1. Определите, какой метод сокрытия информации: криптографический или стеганографический был использован в данном случае. Обоснуйте ответ.   Безымянный   1. Расшифруйте загаданное слово. Опишите ваши затруднения при расшифровке. 2. Загадайте слово или кодовую фразу, зашифруйте ее аналогично примеру. 3. Обменяйтесь QR-кодами с товарищами,   попробуйте расшифровать (по 3 кода каждый). |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1** | 1. Что вы обычно делаете с ненужными напечатанными документами?   а) Выбрасываю в мусорку.  **б) Пускаю в шредер (измельчитель).**  в) Перечеркиваю ручкой  «напечатанную» страницу и использую потом как черновик.  г) Ничего не делаю. даже не знаю, куда они деваются.   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 | 1. Из каких характеристик состоит информационная безопасность?   1. доступность, целостность, актуальность; 2. доступность, системность, конфиденциальность; 3. **доступность, целостность, конфиденциальность;** 4. актуальность, целостность, конфиденциальность; 5. Распространение заведомо ложной информации, часто предоставляемой государством или его агентами иностранным властям или СМИ с целью оказать влияние их на мнение или политику –   **дезинформация**   1. В Российской Федерации действует следующее деление информации   Выберите один или несколько ответов:  **а) открытая информация;**  **б) конфиденциальная информация;** | 1. Актуальность и непротиворечивость информации, ее   защищенность от  разрушения и  несанкционированного изменения  а) защищенность; б) доступность; **в) целостность;**  г) конфиденциальность;   1. Защищаемая физическим лицом информация   личного характера, распространение которой может нанести моральный или материальный ущерб отдельному физическому лицу  **а) личная тайна;**  б) служебная тайна;  в) персональная тайна; г) персональные данные;   1. Возможность получить доступ к нужной   информации за неограниченное количество |

|  |  |  |  |
| --- | --- | --- | --- |
|  | архивирую с паролем.   1. Вы отправили на печать список клиентов, принтер стоит в коридоре, но вас отвлек коллега со срочной задачей, как поступите?   а) Выслушаю коллегу, потом заберу документы – 10 минут ничего не решат.  б) Если задача  действительно срочная, попрошу кого-нибудь пойти забрать бумаги.  в) Редко хожу сам за распечаткой, обычно прошу коллег. И сам других выручаю.  **г) Попрошу коллегу подождать и сразу схожу за распечаткой.**   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. Вы получили письмо с неизвестного адресата с пометкой «ВАЖНО» и пройсбой срочно посмотреть информацию по ссылке. Ваши действия?   **а) Я знаю всех, кто мне пишет. Письмо от незнакомца удалю, по ссылке не пойду.**  б) Раз письмо мне, открою его и перейду по ссылке.  в) Перешлю письмо более опытному коллеге, чтобы разобраться вместе.  г) Напишу ответ, чтобы уточнить информацию.   1. Вам нужно поработать из дома, но для этого нужно   «взять» с собой некоторые конфиденциальные документы как поступите?  а) Возьму с собой. Всегда так делаю.  б) Посоветуюсь с | в) строго конфиденциальная информация;  **г) для внутреннего использования;**   1. Формы уязвимости информации (уберите лишнее): **а) стабилизация информации;** б) хищение носителя информации;   в) несанкционированное уничтожение носителя информации;  г) подделка информации;   1. Можно ли отследить историю посещенных страниц? **а) да**   б) да, специальными программами  в) нет   1. При использовании программ-фильтров, нежелательный контент определяет   **пользователь**   1. Список запрещенных веб- адресов называется - …   а) белый список **б) черный список** в) игнор-лист   1. Найдите лишнее, среди путей несанкционированного получения информации:   а) хищение носителей информации и  производственных отходов;  б) дистанционное фотографирование;  **в) использование материалов СМИ.**   1. Аппаратные методы защиты   – это…  а) программные комплексы, предназначенные для защиты информации в ИС;  **б) устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу;**  в) различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие  защиту персонала (личные | времени – …  а) защищенность; **б) доступность;** в) целостность;  г) конфиденциальность;   1. Совокупность целенаправленных действий по обеспечению безопасности данных это   **защита информации**   1. Конфиденциальность – это:   а) защищенность информации от  правонарушителей и несанкционированных изменений;  б) возможность за разумное время получить требуемую информацию;  **в) защита от несанкционированного**  **доступа к информации;**  г) актуальность и непротиворечивость информации;   1. Установите   соответствие:   1. Носители, используемые в древности 2. Современные носители информации   а) глиняные дощечки; б) камень;  в) бумага; г) дерево; д) металл;  е) пергамент;  ж) магнитная лента; з) лазерный диск; и) фотобумага;  **Ответ:1 – a, б, д, е; 2 – в, ж, з, и**  7. Какие пароли вы используете для защиты аккаунтов?  а) Что-то, что не забуду (дата рождения, фамилия+дата рождения и т.п.).  б) Использую сложный набор букв и цифр в разном регистре. Держу их рядом с  компьютером, чтобы не забыть. |

|  |  |  |  |
| --- | --- | --- | --- |
|  | коллегами, если можно – возьму.  в) Вообще-то это запрещено, но работу закончить надо, потому возьму.  **г) Задержусь и поработаю с этими документами из офиса.**   1. Вам позвонили из федеральной налоговой службы и попросили сообщить некоторую 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. За незаконное использование конфиденциальных данных законодательством не предусмотрено:   а) Дисциплинарное взыскание  б) Административный штраф  в) Лишение свободы  **г) Смертная казнь**   1. Вы нашли флешку с логотипом компании, как поступите?   а) Открою на рабочем компьютере и постараюсь выяснить, чья она.  **б) Отдам сисадминам или безопасникам.**  в) Заберу домой и на личном компе посмотрю.  г) На своем компьютере проверять ее не стану, попрошу коллег сделать это.   1. Вам нужно установить программу на рабочий компьютер. Как поступите?   а) Скачаю из интернета бесплатную версию.  б) Попрошу помочь знакомого, который разбирается в вопросе.  **в) Напишу письмо-** | средства безопасности), материальных средств и финансов, информации от противоправных действий;  10. Какой признак **не** входит в отличительные признаки защищаемой информации?  а) засекречивать информацию может только ее собственник или уполномоченные им на то лица;  защищаемая информация  должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства;  **б) рассекречивать засекреченную информацию может должностное лицо, имеющее на это судебное решение;**  в) чем важнее для собственника информация, тем тщательнее он ее защищает. | **в) Для разных аккаунтов – разные сложные пароли. Чтобы не забыть, использую**  **«менеджер паролей».**  г) Использую пароль, который по умолчанию предложила система. Он самый надежный.   1. Физическое или юридическое лицо, случайно совершающее действия, следствием   которых является нарушение безопасности информации при ее обработке техническими средствами  **нарушитель**   1. Попытка реализации угрозы – …   а) взлом **б) атака** в) хакинг  г) нападение   1. Как в общем случае называют человека, который предпринимает попытки реализации угрозы?   а) хакер;  б) взломщик; в) крекер;  **г) злоумышленник;**   1. Неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования – …   а) уязвимость информации; б) разглашение информации;  **в) утечка информации;**  г) утрата информации;   1. Событие, возникающее как результат стечения обстоятельств, когда в силу каких-то причин используемые средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторов и нежелательного их воздействия на защищаемую информацию   – … |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **заявку. Если начальство одобрит, тогда программу установят.**  г) Если уже что-то подобное устанавливал, то сделаю все сам. Если нужно что-то новенькое, обращусь к сисадминам. |  | **а) уязвимость информации;**  б) разглашение информации;  в) утечка информации; г) утрата информации;   1. Несанкционированное доведение защищаемой информации до неконтролируемого количества получателей информации – …   а) уязвимость информации; **б) разглашение информации;**  в) утечка информации; г) утрата информации;   1. Нарушение статуса информации означает: Выберите один или несколько ответов:   **а) удаление информации; б) модификация информации;**  в) унификация информации;  **г) нарушение доступности информации;**   1. Этот вид контента регламентируется законодательными актами различного уровня   **а) запрещенный для любого возраста**  б) нежелательный для детей и подростков   1. Основной нормативный документ, регламентирующий вопросы нежелательного контента на   государственном уровне а) Уголовный Кодекс РФ **б) Конституция РФ**  в) Закон РФ «О цензуре в СМИ»  г) Административный кодекс РФ   1. Являются ли угрозы персоналу угрозами ИБ?   а) нет, так как персонал не владеет важной информацией;  **б) да;**  в) да, так как угроза персоналу всегда влечет потерю конфиденциальной  информации. |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | 1. Что включают в себя технические средства?   а) ограничение доступа лиц в компьютерные помещения и т.д.;  б) парольный доступ – задание полномочий пользователя;  **в) фильтры, экраны на аппаратуру.**   1. Что не входит в программные средства?   а) блокировка экрана и клавиатуры;  **б) устройства**  **аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати и т.д.;**  в) использование средств парольной защиты BIOS – на сам BIOS и на ПК в целом.   1. Что представляют собой нормативно- правовые средства защиты? а) правила и нормы поведения, направленные на обеспечение безопасности информации, не закрепленные законодательно или   административно, но  поддерживаемые в коллективах через традиции и механизм общественного мнения;  **б) включают в себя законы и другие правовые акты, а также механизмы их реализации,**  **регламентирующие информационные отношения в обществе;**  в) правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации, вводимые в действие административным путем.   1. Информационная безопасность – это…   а) защищенность информационной системы |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | от случайного  вмешательства, наносящего ущерб владельцу информации;  **б) защищенность информации и поддерживающей**  **инфраструктуры от**  **случайных или преднамеренных**  **воздействий**  **естественного или искусственного**  **характера, которые могут нанести неприемлемый ущерб субъектам информационных**  **отношений, в том числе владельцам и**  **пользователям информации и поддерживающей**  **инфраструктуры;**  в) защищенность информации от случайных воздействий искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и  пользователям информации и поддерживающей инфраструктуры.   1. Что такое безопасность данных?   **а) это состояние хранимых,**  **обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное**  **получение, изменение или уничтожение;**  б) это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное искажение;  в) это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их преднамеренное получение, изменение или уничтожение.   1. Что представляют |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | собой технические средства защиты?  **а) это комплексы специального**  **технического и программного**  **обеспечения,**  **предназначенные для предотвращения утечки обрабатываемой или хранящейся информации путем исключения несанкционированного**  **доступа к ней с помощью технических средств съема;**  б) это комплексы специального технического обеспечения, предназначенные для предотвращения утечки обрабатываемой информации путем исключения несанкционированного доступа к ней с помощью технических средств;  в) это комплексы специального технического и программного обеспечения, предназначенные для предотвращения доступа к информации путем исключения несанкционированного доступа к ней с помощью технических средств.  24. В чем суть организационных мероприятий по защите информации?  а) приобретение, установка и использование защищенных от различных воздействий технических средств обработки информации;  б) обеспечивают блокирование возможных каналов утечки  информации через технические средства с помощью специальных устройств, устанавливаемых на элементы конструкций  зданий, помещений, технических средств обработки информации;  **в) мероприятия ограничительного** |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **характера, сводящиеся к регламентации доступа и использования**  **технических средств обработки информации.**   1. Соотнесите примеры и виды ущерба    1. Неприемлемый ущерб    2. Допустимый ущерб   а. Студенты получили доступ к флеш-носителю преподавателя  б. Преподаватель заразил флеш-носитель вредоносной программой  в. Сотрудник  следственного комитета забыл ноутбук в кафе  г. Папка сотрудника следственного комитета с важными документами сгорела в пожаре  a) 1 – в, г; 2 – а, б;  б) 1 – а, б; 2 – в, г;  в) 1 – г; 2 – а, б, в;  **г) 1 – б, в; 2 – а, г;**   1. Деятельность клавиатурных шпионов -   а) находясь в оперативной памяти следят за вводимой информацией. Как только пользователь вводит некое кодовое слово,  клавиатурный шпион начинает выполнять вредоносные действия, заданные автором  **б) обманным путем завладевает**  **пользовательскими паролями, а затем переписывает эти пароли туда, откуда их может без особого труда извлечь злоумышленник**  в) находясь в оперативной памяти следят за вводимой пользователем информацией и по команде злоумышлиника производят нужную ему замену одних символов (или групп символов) другими  г) передают  злоумышлинику марку и тип используемой |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | пользователем клавиатуры   1. Угроза чему была реализована?   Ошибка 504 (Gateway Time Out) – http-код, который означает, что сайт или приложение, к которому вы обращаетесь, не успел обработать данные в отведённое ему время **угроза доступности**   1. Способы обеспечения конфиденциальности информации и носителей   **а) Ролевое управление доступом**  **б) Криптографический шифр**  **в) Стеганография**  г) Резервное копирование   1. Информация на жестком диске может разрушиться только   вследствие действия компьютерного вируса или злого умысла вашего недоброжелателя  **ложь**   1. Нарушение статуса информации означает: Выберите один или несколько ответов:   **а) удаление информации; б) модификация информации;**  в) унификация информации;  **г) нарушение доступности информации;** |

* 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.

1. Каким образом можно выстроить удобную и защищенную работу на АРМ: защита от НСД при оставленном без присмотра компьютере.
2. Обеспечение сохранности информации в пакетах прикладных программ (напр., MS Office) при сбое работы.
3. Защита от НСД к файлам, хранимых на жестком диске при:
   * разграничении доступа разных пользователей;
   * невозможности разграничения доступа разных пользователей.
4. Пользователь постоянно пользуется носителями информации из различных мест, при этом:
   * компьютер пользователя не подключен к Интернет;
   * компьютер пользователя подключен к Интернет.
5. Используя 3 различных метода сокрытия информации зашифровать сообщение

«Информация – царица мира»

1. Флеш-носитель заражён вредоносной программой, оставляющий доступными только ярлыки на папки. После работы антивирусной программы ярлыки были удалены. Опишите процедуру восстановления любым способом
2. Вы ошибочно удалили необходимые вам файлы, корзина так же была очищена. Каким образом вы можете восстановить файлы?

Опишите процедуру восстановления любым способом

1. Опишите процедуру низкоуровневого форматирования. Для чего она нужна?
2. Опишите разные способы удаления файла с компьютера, без применения специализированного ПО, в чем особенность каждого?
3. Опишите механизм удаления файла с компьютера на машинном уровне.
4. Опишите стеганографические способы сокрытия информации в компьютерном изображении: exif, geo-тег, архив, водяные знаки

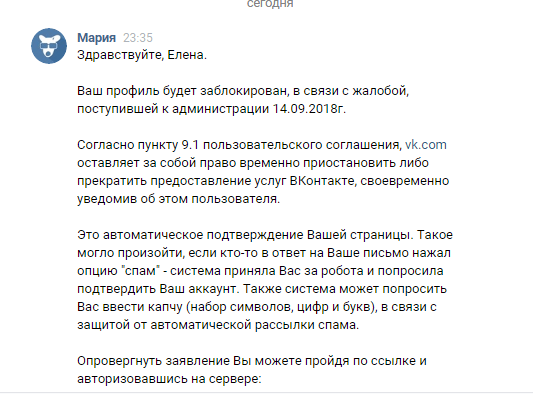
# тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий.

1. Известно, что у менеджера компании Алины есть личный электронный ящик, также что она пользуется социальными сетями (Вконтакте, Одноклассники, Facebook и пр). При этом она закрывает браузер не нажимая кнопку «выход», использует Internet Explorer, имеет 1-2 несложных пароля на все ресурсы, выходит в сеть в основном с рабочего места иногда из дома, все социальные сети привязаны к одному электронному ящику.
2. Определите риски по аспектам информационной безопасности: целостность, доступность, конфиденциальность.
3. Сформулируйте для Алины рекомендации по защите от угроз информационной безопасности.
4. Екатерине на электронную почту пришло письмо следующего содержания: «Здравствуйте, Владимир! Вами был сделан запрос для восстановления данных электронного кошелька

«WebMoneySet» . Ваш логин: vladimir1986. Ваш пароль:236834vm. Для управления счетом установите плагин для совершения денежных операций во вложении.» К письму прикреплен файл

\*exe.

1. Какие действия должна предпринять Екатерина в данной ситуации?
2. Используется ли какой-либо метод(-ы) психологического воздействия в данной ситуации? Если да, то какой(-ие)? Аргументируйте свою точку зрения.
3. Георгий имеет опыт работы в ИТ-индустрии более 3 лет, сейчас он ищет работу и разместил свое резюме на нескольких интернет-сервисах. Через некоторое время с ним связался Светлов А.А., представившийся HR-менеджером компании «Инфософт». Чтобы решить приглашать Георгия на собеседование или нет работодатель хочет проверить его навыки работы с мобильными программами. Светлов А.А. предлагает скачать специальную программу по ссылке и продемонстрировать свои умения. Георгий скачивает приложение, выполняет задание работодателя, однако на собеседование его не приглашают. Через некоторое время выясняется, что вредоносная программа позволила злоумышленникам завладеть денежными средствами Георгия с счета, привязанного к мобильному банку.
4. Какие ошибки можно выделить в информационном поведении Георгия?
5. Как действовать в данной ситуации?
6. Как избежать подобных ситуаций позднее?
7. Вы получили следующее сообщение:



Каковы должны быть ваши действия? Проанализируйте алгоритм манипуляции, подумайте, какой информацией вы должны владеть, чтобы ваш аккаунт не взломали и не заблокировали?

1. Проанализировать представленную предметную область, определить угрозы, разработать модель нарушителя, оценить риски нарушения безопасности по заданным параметрам

# описание процедуры оценивания результатов обучения.

Оценка результатов обучения проходит в форме итогового тестирования, тест включает в себя 15 теоретических вопросов и вопрос со свободной формой ответа (п.8.3).

Теоретический вопрос имеет вес в 1 балл.

Практический вопрос имеет вес в 5 баллов и оценивается преподавателем. Шкала оценки:

|  |  |
| --- | --- |
| Количество набранных баллов | Результат |
| 0-10 | незачёт |
| 11-20 | зачёт |

# 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 | Чернова Елена Владимиро вна | ФГБОУ ВПО  «МГТУ им. Г.И.  Носова», к.п.н., доцент кафедры Бизнес- информатики и информационных технологий | [https://www.magtu.](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/chernova-elena-vladimirovna.html) [ru/staff/personalny](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/chernova-elena-vladimirovna.html) [e-stranitsy-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/chernova-elena-vladimirovna.html) [prepodavatelej/item](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/chernova-elena-vladimirovna.html)  [/chernova-elena-](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/chernova-elena-vladimirovna.html) [vladimirovna.html](https://www.magtu.ru/staff/personalnye-stranitsy-prepodavatelej/item/chernova-elena-vladimirovna.html) | d:\Users\georgievskikh.n\Desktop\Преподаватели на сайт НТИ\chernova.jpg | **+** |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки, материалы курса,  учебная литература |
| дистанционные образовательные  технологии | <http://m.idpo.magtu.ru/course/view.php?id=200> |
| методы организации и осуществления учебной | Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.:  ил. |
|  | Практикум по информационной безопасности для бакалавров Прикладной информатики / Е.В. Чернова. – Электрон. текстовые дан. (1,29 Мб). – Магнитогорск : ФГБОУ ВО «МГТУ им. Г.И. Носова», 2019.  – 1 электрон. опт. диск (CD-R). – Систем. требования : IBMPC, любой, более lGHz ;  512 Мб RAM ; 10 Мб HDD ; М S WindowsXP и выше ; AdobeReader 8.0 и выше ; CD/ DVD-ROM дисковод ; мышь. – Загл. с титул. Экрана |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
|  | Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5- 534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: [https://biblio-](https://biblio-online.ru/viewer/informacionnaya-bezopasnost-cheloveka-449350%23page/1) [online.ru/viewer/informacionnaya-bezopasnost-](https://biblio-online.ru/viewer/informacionnaya-bezopasnost-cheloveka-449350%23page/1) [cheloveka-449350#page/1](https://biblio-online.ru/viewer/informacionnaya-bezopasnost-cheloveka-449350%23page/1) |
|  | Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-  00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: [https://biblio-](https://biblio-online.ru/viewer/informacionnaya-bezopasnost-434171%23page/1) |

|  |  |
| --- | --- |
|  | [online.ru/viewer/informacionnaya-bezopasnost-](https://biblio-online.ru/viewer/informacionnaya-bezopasnost-434171%23page/1)  [434171#page/1](https://biblio-online.ru/viewer/informacionnaya-bezopasnost-434171%23page/1) |
|  | Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. – 4-е изд., перераб. и доп. – Москва  : РИОР : ИНФРА-М, 2019. – 322 с. — (Высшее  образование). – ww.dx.doi.org/10.12737/11380. – Текст : электронный. – URL: [https://new.znanium.com/catalog/document?id=336](https://new.znanium.com/catalog/document?id=336219) [219](https://new.znanium.com/catalog/document?id=336219) |
|  | PHDays — международный форум по  практической безопасности - <https://www.phdays.com/ru/> |
|  | Статьи от компании Positive Technologies -  <https://habr.com/ru/company/pt/profile/> |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекции | Компьютер с доступом в Интернет |
| Практические занятия | Компьютер с доступом в Интернет, MS Excel, MS Word, Kaspersky Endpoint Security для бизнеса-Стандартный, 7Zip, Lpro, GlassWire, Генератор паролей 1.5, KeePass Password Safe, Thunderbird, Recuva, Alternate File Sredder, HDD Low Level Format  Tool, Шифратор «Решетка Кардано», S-Tools, Mozilla Firefox для Windows |
| Самостоятельная работа | Компьютер с доступом в Интернет, MS Excel, MS Word, Kaspersky Endpoint Security для бизнеса-Стандартный, 7Zip, Lpro, GlassWire, Генератор паролей 1.5, KeePass Password Safe, Thunderbird, Recuva, Alternate File Sredder, HDD Low Level Format  Tool, Шифратор «Решетка Кардано», S-Tools, Mozilla Firefox для Windows |

ПАСПОРТ КОМПЕТЕНЦИИ

«Защита информации»

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

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | Администрирование систем защиты информации автоматизированных систем | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Под компетенцией понимается способность обеспечивать защиту информации в автоматизированной системе с учетом поставленных требований  Слушатель должен:  Знать:   * Программно-аппаратные средства защиты информации автоматизированных систем; * Основные меры по защите информации в автоматизированных системах;   Уметь:   * Устанавливать и настраивать программные средства с учетом требований по обеспечению защиты информации * Использовать криптографические методы и средства защиты информации в автоматизированных системах; * Анализировать события, связанные с защитой информации в автоматизированных системах;   Владеть:   * Навыками использования программных средств для решения поставленных задач по защите информации | |
| 4. | Дескриптор знаний, умений и | Уровни | Индикаторы |
|  | навыков по уровням | сформированности |  |
|  |  | компетенции |  |
|  |  | обучающегося |  |
|  |  | Начальный уровень | Знает:  основы компьютерной грамотности  Умеет:  устанавливать и настраивать ПО по заданным параметрам  Владеет:  навыками уверенного  пользования ПК для решения поставленных задач |
|  | (Компетенция |
|  | недостаточно развита. |
|  | Частично проявляет |
|  | навыки, входящие в |
|  | состав компетенции. |
|  | Пытается, стремится |
|  | проявлять нужные |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | навыки, понимает их |  |
| необходимость, но у |
| него не всегда |
| получается.) |
|  | Базовый уровень | Знает:  о проблемах обеспечения защиты информации  Умеет:  применять программные средства обеспечения защиты информации для решения поставленных задач (уничтожение, сокрытие информации и др.)  Владеет:  Навыком отбора готовых решений к требуемой  ситуации защиты информации |
| (Уверенно владеет |
| навыками, способен, |
| проявлять |
| соответствующие |
| навыки в ситуациях с |
| элементами |
| неопределённости, |
| сложности.) |
|  | Продвинутый | Знает:  программно-аппаратные средства защиты информации  Умеет:  формулировать требования к обеспечению защиты информации: ставить цель и задачи  Владеет:  навыком работы с программами и алгоритмами криптографической защиты  информации |
| (Владеет сложными |
| навыками, способен |
| активно влиять на |
| происходящее, |
| проявлять |
| соответствующие |
| навыки в ситуациях |
| повышенной |
| сложности.) |
|  | Профессиональный | Знает:  методы и средства защиты информации  Умеет:  подбирать, устанавливать, настраивать и применять специальные программные средства обеспечения защиты информации для решения поставленных задач (уничтожение, сокрытие информации и др.)  Владеет:  навыком формулировки требований к обеспечению защиты информации и определять пути их  достижения: ставить цель, |
| (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 |

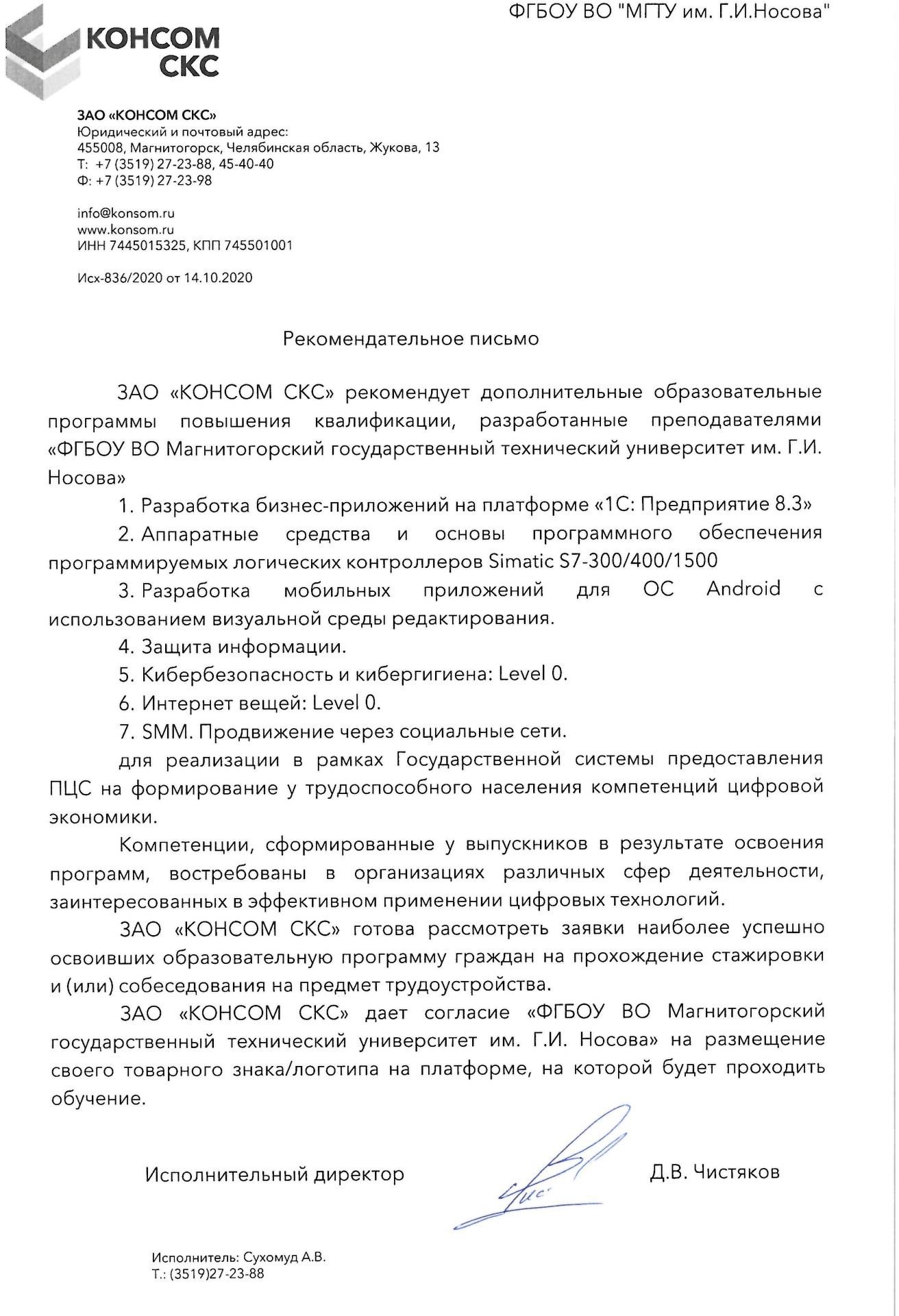
|  |  |  |  |
| --- | --- | --- | --- |
|  |  | сложности.) | задачи, подбирать методы и средства защиты информации  проблемной области |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Способность использовать возможности компьютера | |
| 6. | Средства и технологии оценки | Практические задания | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Под компетенцией понимается способность восстанавливать после сбоев и отказов программного обеспечения автоматизированные системы | |
|  |  | Слушатель должен:  Знать:   * Организационные меры по защите информации; | |
|  |  | Уметь:   * Классифицировать и оценивать угрозы информационной безопасности; * Применять программные средства обеспечения безопасности данных; | |
|  |  | Владеть:   * Навыками использования программных средств   для восстановления после сбоя систем обработки информации | |
| 4. | Дескриптор знаний, умений и | Уровни | Индикаторы |
|  | навыков по уровням | сформированности |  |
|  |  | компетенции |  |
|  |  | обучающегося |  |
|  |  | Начальный уровень | Знает:  основные угрозы защиты информации и способы их предупреждения  Умеет:  определять требования к организации процесса защиты документированной |
|  | (Компетенция |
|  | недостаточно развита. |
|  | Частично проявляет |
|  | навыки, входящие в |
|  | состав компетенции. |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | информации  Владеет:  представлением о способах несанкционированного доступа к носителям данных |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знает:  основные угрозы безопасности информации и модели нарушителя  Умеет:  создавать надежный и устойчивый ко взлому пароль  Владеет:  представлением о способах защиты информации от нарушения статуса |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает:  современное программное обеспечение для сохранения требуемого статуса информации  Умеет:  подбирать, настраивать и использовать современное программное обеспечение для сохранения требуемого статуса информации  Владеет:  навыком применять специализированное ПО для восстановления 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 | Знает:  различные ресурсы для проверки уровня защиты статуса информации: доступность, конфиденциальность  Умеет:  подбирать, настраивать и использовать специализированное ПО для восстановления информации  Владеет:  навыком подбора ресурсов для решения поставленных задач по восстановлению автоматизированных систем после сбоя, либо для |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | сложности.) | недопущения сбоя |
| 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 | |

# Рекомендаций к программе от работодателей:



1. **Указание на возможные сценарии профессиональной траектории граждан** по итогам освоения образовательной программы

|  |  |  |
| --- | --- | --- |
| **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  работающий по найму в организации, на предприятии  временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.) | сохранение текущего рабочего места развитие профессиональных качеств повышение заработной платы  смена работы без изменения сферы профессиональной деятельности  сохранение и развитие квалификации | |

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