* **Паспорт Образовательной программы**

**«** Защита информации **»**

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

* **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | ФГБОУ ВО "Липецкий государственный технический университет" |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 4826012416 |
| 1.4 | Ответственный за программу ФИО | Корнеева Анастасия Олеговна |
| 1.5 | Ответственный должность | Специалист по учебно-методической работе деканата факультета дополнительного образования |
| 1.6 | Ответственный Телефон | +7(904)285-23-83 |
| 1.7 | Ответственный Е-mail | korneeva\_ao@stu.lipetsk.ru |

* **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Защита информации |
| 2.2 | Ссылка на страницу программы | https://cloud.stu.lipetsk.ru/index.php/s/nFNR8imo6E2THZ7#pdfviewer |
| 2.3 | Формат обучения | Онлайн |
|  | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | Личный кабинет на сайте ЛГТУ  http://eserv.stu.lipetsk.ru/course/view.php?id=667 |
| 2.4 | Уровень сложности | Базовый |
| 2.5 | Количество академических часов | 96 |
|  | 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) | 48 |
| 2.6 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | 15 000 руб.  МФТИ (Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа)  https://mipt.ru/cdpo/programs/software/supervised\_learning.php?ELEMENT\_ID=1899815&clear\_cache=Y 108 ч.47500 руб. МФТИ (Технологии и средства защиты компьютерных систем)  обучения)  <https://mipt.ru/cdpo/programs/software/supervised_learning.php?ELEMENT_ID=1851491&clear_cache=Y>  102 ч. 49500 руб. МФТИ (Защита персональных данных) https://mipt.ru/cdpo/programs/software/supervised\_learning.php?ELEMENT\_ID=1910217&clear\_cache=Y  72 ч. 29000 руб. |
| 2.7 | Минимальное количество человек на курсе | 10 |
| 2.8 | Максимальное количество человек на курсе | 15 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | - |
| 2.10 | Формы аттестации | Итоговое задание |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Связь, информационные и коммуникационные технологии |

* **Аннотация программы**

1. Цель реализации программы

Целью реализации программы «Защита информации» является формирование у слушателей готовности планировать и реализовывать в различных видах профессиональной деятельности мероприятия по обеспечению информационной безопасности с использованием технических и программных средств.

2. Требования к результатам обучения

В результате освоения программы слушатель должен приобрести следующие знания:

- подходы к организации системы защиты информации,

- методологию оценки уязвимостей, эффективности мероприятий по защите,

- способы и виды средств защиты компьютерных систем;

В результате освоения программы слушатель должен приобрести следующие умения:

- проводить анализ реализации политики безопасности,

- устанавливать и настраивать программно-технические средства защиты;

В результате освоения программы слушатель должен приобрести следующие навыки:

- различными средствами защиты информации и оценки защищенности.

ФГБОУ ВО «Липецкий государственный технический университет»

УТВЕРЖДАЮ

Ректор ЛГТУ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Сараев П.В.

« \_\_\_ » \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г.

Дополнительная профессиональная программа повышения квалификации

« Защита информации »

96 часа.

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Целью реализации программы «Защита информации» является формирование у слушателей готовности планировать и реализовывать в различных видах профессиональной деятельности мероприятия по обеспечению информационной безопасности с использованием технических и программных средств.

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. Подходы к организации системы защиты информации;

2.1.2. Методологию оценки уязвимостей, эффективности мероприятий по защите;

2.1.3. Способы и виды средств защиты компьютерных систем;

2.2. Умение (способность к деятельности)

2.2.1 Проводить анализ реализации политики безопасности;

2.2.2. Устанавливать и настраивать программно-технические средства защиты;

2.3.Навыки (использование конкретных инструментов)

2.3.1. Различными средствами защиты информации и оценки защищенности.

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

* Среднее специальное / высшее техническое
* Не имеет значения
* Не имеет значения
* Не имеет значения

**4.Учебный план программы «Безопасность компьютерных систем»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Модуль** | **Всего часов** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| **1** | **Входной контроль** | **2** |  |  | **2** |
| **2.** | **Нарушения безопасности в компьютерных системах. Модели информационной безопасности** | **20** | **6** | **4** | **10** |
| **3.** | **Стандарты информационной безопасности. Правовое регулирование в области безопасности информации** | **8** | **4** | **0** | **4** |
| **4.** | **Несанкционированный доступ к информации. Политика безопасности** | **36** | **6** | **12** | **18** |
| **5.** | **Защита информации в компьютерных сетях** | **20** | **6** | **4** | **10** |
| **6.** | **Системы защиты программного обеспечения. Защита от вредоносного программного обеспечения** | **8** | **2** | **2** | **4** |
| **Итоговая аттестация** | |  |  | | |
| **Итоговый контроль** | | **4** | Выполнение индивидуального задания | | |

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | **Входной контроль** | **2** | 07.11.2020 |
| **2** | **Нарушения безопасности в компьютерных системах. Модели информационной безопасности** | **20** | 07.11.2020, 08.11.2020, 09.11.2020 |
| 3 | **Стандарты информационной безопасности. Правовое регулирование в области безопасности информации** | **8** | 10.11.2020 |
| 4 | **Несанкционированный доступ к информации. Политика безопасности** | **36** | 11.11.2020,  12.11.2020,  14.11.2020,  15.11.2020,  16.11.2020 |
| 5 | **Защита информации в компьютерных сетях** | **20** | 16.11.2020,  17,.11.2020,  18.11.2020,  19.11.2020 |
| 6 | **Системы защиты программного обеспечения. Защита от вредоносного программного обеспечения** | **8** | 21.11.2020,  22.11.2020,  23.11.2020 |
| **Всего:** | | 96 | 07-23.11.2020 г. |

**6.Учебно-тематический план программы « Б**езопасность компьютерных систем **»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Входной контроль | 2 | 0 | 0 | 2 | Оценка результатов тестирования |
| 2 | Нарушения безопасности в компьютерных системах. Модели информационной безопасности | 20 | 6 | 4 | 10 | - |
| 2.1 | Исследование причин нарушений безопасности. Уязвимости. | 4 | 2 | 0 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 2.2 | Угрозы информационной безопасности. Классификация угроз. | 8 | 2 | 2 | 4 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 2.3 | Анализ моделей информационной безопасности. Основные определения и математическая формализация. | 8 | 2 | 2 | 4 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 3 | Стандарты информационной безопасности. Правовое регулирование в области безопасности информации | 8 | 4 | 0 | 4 |  |
| 3.1 | Обзор и сравнительный анализ существующих стандартов информационной безопасности | 4 | 2 | 0 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 3.2 | Государственная политика РФ в области безопасности информационных технологий | 4 | 2 | 0 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 4 | Несанкционированный доступ к информации. Политика безопасности | 36 | 6 | 12 | 18 |  |
| 4.1 | Противодействие несанкционированному доступу. Криптография. Классификация шифров | 4 | 2 | 0 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 4.2 | Алгоритмы поточного и блочного шифрования. Симметричные и ассиметричные алгоритмы. Цифровая электронная подпись. | 28 | 2 | 12 | 14 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 4.3 | Реализация и гарантирование политики безопасности. Организационные методы защиты информации | 4 | 2 | 0 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 5 | Защита информации в компьютерных сетях | 20 | 6 | 4 | 10 |  |
| 5.1 | Способы безопасного доступа к локальным и глобальным сетям. | 4 | 2 | 2 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 5.2 | Основы и цель политики безопасности в компьютерных сетях. Управление доступом | 4 | 2 | 2 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 5.3 | Построение защищенных виртуальных сетей | 4 | 2 | 0 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 6 | Системы защиты программного обеспечения. Защита от вредоносного программного обеспечения | 8 | 2 | 2 | 4 |  |
| 6.1 | Классификация компьютерных вирусов. Классификация систем защиты программного обеспечения | 5 | 1 | 2 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 6.2 | Методы, способы и средства защиты информации в информационных системах | 3 | 1 | 0 | 2 | Проверка заданий, выполненных в рамках самостоятельной работы |

**7. Учебная (рабочая) программа повышения квалификации « Безопасность компьютерных систем»**

Модуль 1. Нарушения безопасности в компьютерных системах. Модели информационной безопасности (19 ч.)

Тема 1.1. Исследование причин нарушений безопасности. Уязвимости. (2 ч.)

Тема 1.2. Угрозы информационной безопасности. Классификация угроз. (4 ч.)

Тема 1.3. Анализ моделей информационной безопасности. Основные определения и математическая формализация. (4 ч.)

Модуль 2. Стандарты информационной безопасности. Правовое регулирование в области безопасности информации (4 ч.)

Тема 2.1. Обзор и сравнительный анализ существующих стандартов информационной безопасности (2 ч.)

Тема 2.2. Государственная политика РФ в области безопасности информационных технологий (2 ч.)

Модуль 3. Несанкционированный доступ к информации. Политика безопасности (18 ч.)

Тема 3.1. Противодействие несанкционированному доступу. Криптография. Классификация шифров (2 ч.)

Тема 3.2. Алгоритмы поточного и блочного шифрования. Симметричные и ассиметричные алгоритмы. Цифровая электронная подпись. (14 ч.)

Тема 3.3. Реализация и гарантирование политики безопасности. Организационные методы защиты информации (2ч.)

Модуль 4. Защита информации в компьютерных сетях ( 10ч.)

Тема 4.1. Способы безопасного доступа к локальным и глобальным сетям. (4 ч.)

Тема 4.2. Основы и цель политики безопасности в компьютерных сетях. Управление доступом (4 ч.)

Тема 4.3. Построение защищенных виртуальных сетей (2 ч.)

Модуль 5. Системы защиты программного обеспечения. Защита от вредоносного программного обеспечения (4 ч.)

Тема 5.1. Классификация компьютерных вирусов. Классификация систем защиты программного обеспечения (3 ч.)

Тема 5.2. Методы, способы и средства защиты информации в информационных системах (1 ч.)

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| 1 | 1.2 | Изучение и защита реализации шифра Вижинера | Написание программной реализации шифра Вижинера |
| **2** | 1.3 | Исследование свойств парольных систем. Изучение программных средств создания защищенных хранилищ | Кейс-задание по защищенным хранилищам |
| 3 | 2 | Изучение программ-анализаторов уязвимостей компьютерных систем | Кейс-задание по сканирующему анализатору |
| 4 | 3.1 | Изучение реализации шифра DES | Написание программной реализации шифра Написание программной реализации шифра DES |
| 5 | 3.2 | Изучение реализации алгоритма CRC | Написание программной реализации шифра CRC |
| 6 | 3.3 | Изучение реализации шифра RSA | Написание программной реализации шифра RSA |
| 7 | 4,1 | Изучение сетевых фильтров | Кейс-задание на методы обеспечения безопасности ctntdsvb abkmnhfvb |
| 8 | 4.2 | Установка и настройка системы SecretNet | Кейс-задание по системы SecretNet |
| 9 | 5 | Изучение и защита реализации алгоритма электронной цифровой подписи | Написание программной реализации АЦП |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| 1 | Виды нарушений информационной ьезопасности | Угрозы информационной безопасности. | Исследование причин нарушений безопасности. Уязвимости. Классификация угроз. |
| 2 | Виды правового регулирования | Государственная политика РФ в области безопасности информационных технологий | Обзор и сравнительный анализ существующих стандартов информационной безопасности. Российские стандарты. Национальные и международные стандарты |
| 3 | Что такое политика безопасности | Криптография. Классификация шифров. Алгоритмы поточного и блочного шифрования. Симметричные и ассиметричные алгоритмы. | Анализ моделей информационной безопасности. Основные определения. Математическая формализация. Реализация и гарантирование политики безопасности. Организационные методы защиты информации. Противодействие несанкционированному доступу. |
| 4 | Что такое сетевой фильтр | Классификация систем защиты программного обеспечения. Достоинства и недостатки основных систем защиты. Показатели эффективности. Основы и цель политики безопасности в компьютерных сетях. Управление доступом. Многоуровневая защита корпоративных сетей | Способы безопасного доступа к локальной сети. Современные средства и технологии. Способы безопасного доступа к глобальным сетям. Современные средства и технологии. Защищенные технологии удаленного доступа. Построение защищенных виртуальных сетей. Шифрование в сетях передачи данных. |
| 5 | Что такое компьютерные вирусы | Цифровая электронная подпись. | Классификация компьютерных вирусов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов. |

**8.2.**  Входной контроль охватывает всех обучаемых и проводится в форме собеседования. Целью его является определение уровня знаний обучаемых. Итоговая аттестация проводится в форме выполнения индивидуальных заданий. Итоговая работа рассчитана на 4 ч., выполняется как кейс-задание в рамках самостоятельной работы, позволяет оценить знания, умения и уровень приобретенных компетенций.

**8.3.**  Итоговое задание

Изучение методов, способов и средств защиты информации в информационных системах.

Задание.

Выберите одну из предложенных преподавателем предметных областей и изучите способы и средства организации защиты информации. Темы не являются обязательными. Студент может предложить свою, близкую ему, тему, которую до выполнения работы необходимо согласовать с преподавателем.

**Примерная тематика**

1. Модели ценности информации.

2. Классификация угроз информационной безопасности.

3. Методы обеспечения компьютерной безопасности.

4. Причины, виды и каналы утечки информации.

5. Жизненный цикл программного обеспечения компьютерных систем. Технологическая и эксплуатационная безопасность.

6. Модель угроз и принципы обеспечения безопасности компьютерных систем.

7. Средства деструктивного воздействия на компьютерные системы.

8. Контрольно-испытательные методы анализа безопасности программного обеспечения.

9. Логико-аналитические методы контроля безопасности программ.

10. Классификация требований к системам защиты.

11. Многоуровневая защита корпоративных сетей.

12. Администрирование межсетевого экрана.

13. Криптоанализ.

14. Основные классы симметричных криптосистем. Блочные шифры.

15. Потоковые шифры.

16. Асимметричные криптосистемы.

17. Алгоритмы электронной цифровой подписи.

18. Тенденции развития и применения методов и средств защиты информации в компьютерных системах.

19. Разработка модели защищенной локальной вычислительной системы.

20. Разработка модели защищенной распределенной вычислительной системы.

21. Защита линий связи.

22. Защита вычислительного объекта.

23. Защита баз данных (БД).

24. Защита подсистем управления.

25. Моделирование активных компонентов архитектуры сетевой защиты, активные компоненты, БД в системе защиты.

26. Моделирование оптимальных структур БД в системе защиты.

27. Исследование свойств DES алгоритма, эффект обвала, свойство дополнения.

28. Исследование недостатков DES алгоритма, малой длина ключа, малого число циклов шифрования, нахождение вырожденных и полувырожденных ключей шифрования.

29. Шифрование симметрическими алгоритмами шифрования, и подбор методов получения исходной информации без знания исходного ключа.

30. Шифрование асимметрическими алгоритмами шифрования, и подбор методов получения исходной информации без знания исходного ключа.

31. Формирование методов выработки ключей шифрования.

32. Разработка оптимальных протоколов взаимной проверки подлинности.

**8.4.**  Итоговое кейс-задание оценивается в:

1-2 балла - «неудовлетворительно», не зачтено.

3 балла - «удовлетворительно», зачтено.

4 балла - «хорошо», зачтено.

5 баллов - «отлично», зачтено. **.**

**9.Организационно-педагогические условия реализации программы**

**9.1. Кадровое обеспечение программы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Фамилия, имя, отчество (при наличии)** | **Место основной работы и должность, ученая степень и ученое звание (при наличии)** | **Ссылки на веб-страницы с портфолио (при наличии)** | **Фото в формате jpeg** | **Отметка о полученном согласии на обработку персональных данных** |
| **1** | Батищев Роман вячеславович | ЛГТУ, доцент, к.т.н., доцент | http://www.stu.lipetsk.ru/struct/kaf/inf/about/staff.html | Батищев.jpg |  |
| **2** | Ведищев Виталий Викторович | ЛГТУ, профкссор, к.т.н., доцент | http://www.stu.lipetsk.ru/struct/kaf/asu/about/staff.html | Ведищев.jpg |  |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
|  | Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— Саратов: Профобразование, 2019.— 702 c.— Режим доступа: http://www.iprbookshop.ru/87995.html.— ЭБС «IPRbooks»  Краковский Ю.М. Защита информации [Электронный ресурс]: учебное пособие/ Краковский Ю.М.— Электрон. текстовые данные.— Ростов-на-Дону: Феникс, 2016.— 349 c.— Режим доступа: http://www.iprbookshop.ru/59350.html.— ЭБС «IPRbooks»  Никифоров С.Н. Защита информации. Защищенные сети [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 80 c.— Режим доступа: http://www.iprbookshop.ru/74382.html.— ЭБС «IPRbooks»  Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие/ Фороузан Бехроуз А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 782 c.— Режим доступа: http://www.iprbookshop.ru/72337.html.— ЭБС «IPRbooks»  Никифоров С.Н. Защита информации. Защита от внешних вторжений [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 84 c.— Режим доступа: http://www.iprbookshop.ru/74381.html.— ЭБС «IPRbooks»  Никифоров С.Н. Защита информации [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2015.— 384 c.— Режим доступа: http://www.iprbookshop.ru/74365.html.— ЭБС «IPRbooks» |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Университетская библиотека online | <http://biblioclub.ru> |
| Университетская библиотечная система «Znanium». | <http://www.intuit.ru> |
| Rapid7 Nexpose Community Edition — бесплатный сканер уязвимостей | <https://itsecforu.ru/2017/10/05/rapid7-nexpose-community-edition-%D0%B1%D0%B5%D1%81%D0%BF%D0%BB%D0%B0%D1%82%D0%BD%D1%8B%D0%B9-%D1%81%D0%BA%D0%B0%D0%BD%D0%B5%D1%80-%D1%83%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D0%B5%D0%B9/> |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Практические | ЭВМ с доступом к сети Internet Наличие установленного пакета Microsoft Visual Studio и специализированных программ (по типам) согласно перечню практических работ, лицензионных или свободно распространяемых, например: Dallas Lock, Max Patrol, Secret Net, DeviceLock, Acronis Backup & Recovery, ViPNet Client. |
| Самостоятельная работа | ЭВМ с доступом к сети Internet Наличие установленного пакета Microsoft Visual Studio и специализированных программ (по типам) согласно перечню практических работ, лицензионных или свободно распространяемых, например: Dallas Lock, Max Patrol, Secret Net, DeviceLock, Acronis Backup & Recovery, ViPNet Client. |

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

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

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

ПАСПОРТ КОМПЕТЕНЦИИ

дополнительной профессиональной образовательной

программы повышения квалификации

«Защита информации»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | способность оценивать уязвимости, эффективность мероприятий по защите, способы и виды средств защиты компьютерных систем, устанавливать и настраивать программно-технические средства защиты | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная |  | |
| профессиональная | + | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Умения: проводить мероприятия по обеспечению защиты информации  Навыки: использование программно-технических защиты информации | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
| ЗНАТЬ: подходы к организации системы защиты информации, методологию оценки уязвимостей, эффективности мероприятий по защите, способы и виды средств защиты компьютерных систем | | Начальный уровень | Общие, но не структурированные знания методов абстрактного мышления, анализа и синтеза при решении исследовательских и практических задач |
| Базовый уровень | Сформированные, но содержащие отдельные пробелы знания основных методов к абстрактного мышления, анализа и синтеза при решении исследовательских и практических задач |
| Профессиональный | Сформированные систематические знания методов абстрактного мышления, анализа и синтеза при решении исследовательских и практических задач |
| УМЕТЬ: проводить анализ реализации политики безопасности, устанавливать и настраивать программно-технические средства защиты ы | | Начальный уровень | В целом успешно, но не систематически осуществляемые анализ альтернативных вариантов решения исследовательских задач и оценка экономической эффективности реализации этих вариантов |
| Базовый уровень | В целом успешные, но содержащие отдельные пробелы анализ альтернативных вариантов решения исследовательских задач и оценка экономической эффективности реализации этих вариантов |
| Профессиональный | Сформированное умение анализировать альтернативные варианты решения исследовательских задач и оценивать экономическую эффективность реализации этих вариантов |
| ВЛАДЕТЬ: различными средствами защиты информации и оценки защищенности | | Начальный уровень | В целом успешное, но не систематическое применение навыков методологического использования абстрактного мышления при решении проблем, возникающих при выполнении исследовательских работ, самостоятельного мышления, отстаивания своей точки зрения |
| Базовый уровень | В целом успешное, но содержащее отдельные пробелы применение навыков методологического использования абстрактного мышления при решении проблем, возникающих при выполнении исследовательских работ, самостоятельного мышления, отстаивания своей точки зрения |
| Профессиональный | Успешное и систематическое применение навыков методологического использования абстрактного мышления при решении проблем, возникающих при выполнении исследовательских работ, самостоятельного мышления, отстаивания своей точки зрения |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Необходимые базовые компетенции:  - навыки системного и логического мышления, умение анализировать информацию, выделять в ней главное;  - владение персональным компьютером, операционной системой Windows;  - владение навыками программирования на языке высокого уровня стандартных алгоритмов обработки информации | |
| 6. | Средства и технологии оценки | | Набор практических заданий для выявления уровня сформированности компетенции | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | способность применять различные средств защиты информации и оценки защищенности. | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная |  | |
| профессиональная | + | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Умения: оценивать и выбирать необходимые средства защиты компьютерных систем | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
| ЗНАТЬ: методологию оценки уязвимостей, эффективности мероприятий по защите, способы и виды средств защиты компьютерных систем | | Начальный уровень | Имеет не полные представления об основных методах и принципах поиска и классификации информации в интернете и электронных библиотеках |
| Базовый уровень | Сформированные, но содержащие отдельные пробелы представления об основных методах и принципах поиска и классификации информации в интернете и электронных библиотеках |
| Профессиональный | Отлично знает основные методы и принципы поиска и классификации информации в интернете и электронных библиотеках |
| УМЕТЬ: проводить анализ реализации политики безопасности, устанавливать и настраивать программно-технические средства защиты ы | | Начальный уровень | Не умеет находить, классифицировать и оценивать найденную информацию, а так же использовать ее для расширения своего научного мировоззрения |
| Базовый уровень | Слабо умеет находить, классифицировать и оценивать найденную информацию, а так же использовать ее для расширения своего научного мировоззрения |
| Профессиональный | Хорошо умеет находить, классифицировать и оценивать найденную информацию, а так же использовать ее для расширения своего научного мировоззрения |
| ВЛАДЕТЬ: различными средствами защиты информации и оценки защищенности | | Начальный уровень | Частично владеет навыками самообразования, в том числе - использования интернета и нейросетей в поиске и классификации найденной информации; владеть навыками применения найденной информации для расширения и углубления своего научного мировоззрения |
| Базовый уровень | Достаточно хорошо владеет навыками самообразования, в том числе - использования интернета и нейросетей в поиске и классификации найденной информации; владеть навыками применения найденной информации для расширения и углубления своего научного мировоззрения |
| Профессиональный | Свободно владеет навыками самообразования, в том числе - использования интернета и нейросетей в поиске и классификации найденной информации; владеть навыками применения найденной информации для расширения и углубления своего научного мировоззрения |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Необходимые базовые компетенции:  - навыки системного и логического мышления, умение анализировать информацию, выделять в ней главное;  - владение персональным компьютером, операционной системой Windows | |
| 6. | Средства и технологии оценки | | Набор практических заданий для выявления уровня сформированности компетенции | |

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

-

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

1.ОБУ «Информационно-технический центр»,

2. ГУЗ «Липецкий областной онкологический диспансер»,

3. ПАО «Ростелеком»

4. АО «НЛМК-инжиниринг»

5. Филиал ОАО «РЖД»,

6. МедСофт.

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

Развитие профессиональных качеств, сохранение и развитие квалификации.

Слушатель после окончания курса может выполнять следующие трудовые функции, связанные с обеспечением защиты информации: Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем; Установка и настройка средств защиты информации в автоматизированных системах.

**VII.Дополнительная информация**



**VIII.Приложенные Скан-копии**

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