* **Паспорт Образовательной программы**

**«** Безопасность компьютерных систем **»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | **09.10.2020** |

* **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 | Безопасность компьютерных систем |
| 2.2 | Ссылка на страницу программы | https://cloud.stu.lipetsk.ru/index.php/s/HQZApSwYxLtHXxx#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=666 |
| 2.4 | Уровень сложности | Базовый |
| 2.5 | Количество академических часов | 10**2** |
|  | 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) | 86 |
| 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 «Безопасность компьютерных систем» является изучение современных средств и методов защиты информационных систем от несанкционированного доступа, средств разграничения доступа, криптографических алгоритмов, межсетевых экранов, изучение прикладных пакетов для обеспечения безопасности информации.

2. Требования к результатам обучения

В результате освоения программы слушатель должен приобрести следующие знания:

- классификации и модели угроз безопасности информации в автоматизированных системах;

- принципы построения защищенных автоматизированных систем и типовые инструменты обеспечения безопасности информации, предусмотренные в современных операционных системах, СУБД, а также реализованные в специализированных средствах защиты информации;

- методы и средства защиты от удаленных атак на сетевые ресурсы, обеспечения безопасности межсетевого взаимодействия;

- основные направления применения криптографических технологий при защите автоматизированных систем;

- принципы организации систем обнаружения вторжений, мониторинга защищенности локальной и сетевой компьютерной среды.

В результате освоения программы слушатель должен приобрести следующие умения:

- инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения;

- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты;

- устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения;

В результате освоения программы слушатель должен приобрести следующие навыки:

- навыками конфигурирования встроенных инструментов безопасности при администрировании распространенных операционных систем и СУБД;

- навыками создания плана резервного копирования;

- навыками анализа защищенности автоматизированной системы с помощью специализированных программных средств;

- навыками работы с программной и технической документацией на программно-аппаратные средства защиты информации.

ФГБОУ ВО «Липецкий государственный технический университет»

УТВЕРЖДАЮ

Ректор ЛГТУ

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

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

Дополнительная профессиональная программа повышения квалификации

« Безопасность компьютерных систем »

102 часа.

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Целью реализации программы «Безопасность компьютерных систем» является изучение современных средств и методов защиты информационных систем от несанкционированного доступа, средств разграничения доступа, криптографических алгоритмов, межсетевых экранов, изучение прикладных пакетов для обеспечения безопасности информации.

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. Классификации и модели угроз безопасности информации в автоматизированных системах;

2.1.2. Принципы построения защищенных автоматизированных систем и типовые инструменты обеспечения безопасности информации, предусмотренные в современных операционных системах, СУБД, а также реализованные в специализированных средствах защиты информации;

2.1.3. Методы и средства защиты от удаленных атак на сетевые ресурсы, обеспечения безопасности межсетевого взаимодействия;

2.1.4. Основные направления применения криптографических технологий при защите автоматизированных систем;

2.1.5. Принципы организации систем обнаружения вторжений, мониторинга защищенности локальной и сетевой компьютерной среды.

2.2. Умение (способность к деятельности)

2.2.1 Инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения;

2.2.2. Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты;

2.2.3. Устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения.

2.3.Навыки (использование конкретных инструментов)

2.3.1. Конфигурирование встроенных инструментов безопасности при администрировании распространенных операционных систем и СУБД;

2.3.2. Создание плана резервного копирования;

2.3.3. Анализ защищенности автоматизированной системы с помощью специализированных программных средств;

2.3.4. Работа с программной и технической документацией на программно-аппаратные средства защиты информации.

**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.** | **Защита программ и данных** | **36** | **6** | **12** | **18** |
| **3.** | **Механизмы защиты операционных систем** | **12** | **2** | **4** | **6** |
| **4.** | **Информационная безопасность компьютерных сетей** | **24** | **4** | **8** | **12** |
| **5.** | **Защита информации в СУБД** | **12** | **2** | **4** | **6** |
| **6.** | **Нормативно-правовые основы применения, сертификации средств и систем защиты информации** | **12** | **2** | **4** | **6** |
| **Итоговая аттестация** | |  |  | | |
| **Итоговый контроль** | | **6** | 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** | 06.11.2020 |
| **2** | **Защита программ и данных** | **36** | 07.11.2020, 09.11.2020, 10.11.2020,  11.11.2020,  12.11.2020,  13.11.2020 |
| 3 | **Механизмы защиты операционных систем** | **12** | 14.11.2020,  16.11.2020 |
| 4 | **Информационная безопасность компьютерных сетей** | **24** | 17.11.2020,  18.11.2020,  19.11.2020,  20.11.2020 |
| 5 | **Защита информации в СУБД** | **12** | 21.11.2020,  23.11.2020 |
| 6 | **Нормативно-правовые основы применения, сертификации средств и систем защиты информации** | **12** | 24.11.2020,  25.11.2020 |
| **Всего:** | | 102 | 06-25.11.2020 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 | Защита программ и данных | 36 | 6 | 12 | 18 | - |
| 2.1 | Защищаемая информация и основные способы несанкционированного доступа в автоматизированной системе. Классификация средств защиты информации. Механизмы защиты информационных систем. | 12 | 2 | 4 | 6 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 2.2 | Защита от разрушающих программных воздействий. Резервирование и восстановление данных. | 12 | 2 | 4 | 6 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 2.3 | Защита программного обеспечения от изучения и копирования. | 12 | 2 | 4 | 6 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 3 | Механизмы защиты операционных систем | 12 | 2 | 4 | 6 |  |
| 3.1 | Угрозы безопасности и типичные атаки на операционную систему. Типовая структура подсистемы безопасности операционной системы и выполняемые ей функции. Средства обеспечения безопасности в операционных системах семейства Windows. | 12 | 2 | 4 | 6 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 4 | Информационная безопасность компьютерных сетей | 24 | 4 | 8 | 12 |  |
| 4.1 | Введение в сетевую безопасность. Межсетевые экраны: понятие периметра сети. Сканеры безопасности. Системы обнаружения вторжений. | 12 | 2 | 4 | 6 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 4.2 | Основы криптографических методов защиты информации. Технология VPN. | 12 | 2 | 4 | 6 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 5 | Защита информации в СУБД | 12 | 2 | 4 | 6 |  |
| 5.1 | Введение в безопасность СУБД. Средства обеспечения безопасности данных в базе. | 12 | 2 | 4 | 6 | Проверка заданий, выполненных в рамках самостоятельной работы |
| 6 | Нормативно-правовые основы применения, сертификации средств и систем защиты информации | 12 | 2 | 4 | 6 |  |
| 6.1 | Общие сведения о стандартизации в области защиты информации. Международные, зарубежные и отечественные стандарты в области защиты информации. Сертификация средств защиты информации. | 12 | 2 | 4 | 6 | Проверка заданий, выполненных в рамках самостоятельной работы |

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

Модуль 1. Защита программ и данных (18 ч.)

Тема 1.1. Защищаемая информация и основные способы несанкционированного доступа в автоматизированной системе. Классификация средств защиты информации. Механизмы защиты информационных систем. (6 ч.)

Тема 1.2. Защита от разрушающих программных воздействий. Резервирование и восстановление данных. (6 ч.)

Тема 1.3. Защита программного обеспечения от изучения и копирования. (6 ч.)

Модуль 2. Механизмы защиты операционных систем(6 ч.)

Тема 2.1. Угрозы безопасности и типичные атаки на операционную систему. Типовая структура подсистемы безопасности операционной системы и выполняемые ей функции. Средства обеспечения безопасности в операционных системах семейства Windows. (6 ч.)

Модуль 3. Информационная безопасность компьютерных сетей(12 ч.)

Тема 3.1. Введение в сетевую безопасность. Межсетевые экраны: понятие периметра сети. Сканеры безопасности. Системы обнаружения вторжений. (6 ч.)

Тема 3.2. Основы криптографических методов защиты информации. Технология VPN. (6 ч.)

Модуль 4. Защита информации в СУБД(6 ч.)

Тема 4.1. Введение в безопасность СУБД. Средства обеспечения безопасности данных в базе. (6 ч.)

Модуль 5. Нормативно-правовые основы применения, сертификации средств и систем защиты информации(6 ч.)

Тема 5.1. Общие сведения о стандартизации в области защиты информации. Международные, зарубежные и отечественные стандарты в области защиты информации. Сертификация средств защиты информации. (6 ч.)

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| 1 | 1.1 | Защищаемая информация и основные способы несанкционированного доступа в автоматизированной системе. Классификация средств защиты информации. Механизмы защиты информационных систем | Кейс-задание на противодействие несанкционированному доступу |
| **2** | 1.2 | Защита от разрушающих программных воздействий. Резервирование и восстановление данных | Кейс-задание на резервное копирование |
| 3 | 1.3 | Защита программного обеспечения от изучения и копирования | Кейс-задание на защиту от изучения и копирования |
| 4 | 2.1 | Угрозы безопасности и типичные атаки на операционную систему. Типовая структура подсистемы безопасности операционной системы и выполняемые ей функции. Средства обеспечения безопасности в операционных системах семейства Windows | Кейс-задание на использование средств обеспечения безопасности в операционных системах семейства Windows |
| 5 | 3.1 | Введение в сетевую безопасность. Межсетевые экраны: понятие периметра сети. Сканеры безопасности. Системы обнаружения вторжений | Кейс-задание на сканера безопасности |
| 6 | 3.2 | Основы криптографических методов защиты информации. Технология VPN | Кейс-задание на использование технология VPN |
| 7 | 4,1 | Введение в безопасность СУБД. Средства обеспечения безопасности данных в базе | Кейс-задание на методы обеспечения безопасности данных в баз данных |
| 8 | 5.1 | Общие сведения о стандартизации в области защиты информации. Международные, зарубежные и отечественные стандарты в области защиты информации. Сертификация средств защиты информации | Кейс-задание по стандартизации средств защиты информации |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| 1 | Виды НСД | Основные способы НСД в локальном компьютере. Методы и средства защиты информации от НСД в локальном компьютере. Задачи и функции программно-аппаратных средств защиты компьютера. Традиционные методы, технологии и средства защиты информации в автоматизированной системе. Методы и средства ограничения доступа к компонентам компьютера.  Дискреционный и мандатный принципы разграничения доступа. Методы аутентификации пользователей. Принцип действия, достоинства и недостатки аппаратных устройств на основе электронных (магнитных) идентификаторов. Принцип действия, достоинства и недостатки аппаратных устройств на основе биометрических характеристик субъекта. | Дискреционный и мандатный принципы разграничения доступа. Методы аутентификации пользователей. |
| 2 | Виды антивирусных программ | Защита от изменения и контроль целостности. Замкнутая программная среда. Регистрация событий (журналирование) в автоматизированной системе. Защита автоматизированной системы с помощью СЗИ от НСД Secret Net. Контроль доступа к устройствам и интерфейсам с помощью DeviceLock.  Классификация разрушающих программных воздействий. Принципы работы антивирусных средств.  Основные технологии и методы резервного копирования. Создание плана резервного копирования с помощью ПО Acronis Backup & Recovery.  Принципы и методы анализа и исследования программ. Методы защиты от изучения программ. Классификация и принципы действия технических методов защиты от несанкционированного копирования информации.  Защита операционных систем. Средства собственной защиты. Процедура идентификации и аутентификации. Контроль и управление доступом. Регистрация событий. Реализация механизмов безопасности на аппаратном уровне. Защита на уровне расширений BIOS.  Защита на уровне загрузчиков операционной среды. Создание защищенной операционной системы. Основные положения архитектуры микроядерных ОС. Микроядерная архитектура с точки зрения создания защищенных систем. Встроенные механизмы безопасности в ОС Windows. Домены безопасности. Критерии защищенности операционной системы. | Защита автоматизированной системы с помощью СЗИ от НСД Secret Net. Контроль доступа к устройствам и интерфейсам с помощью DeviceLock.  Классификация разрушающих программных воздействий. Принципы работы антивирусных средств.  Создание плана резервного копирования с помощью ПО Acronis Backup & Recovery. |
| 3 | Утечка информации через аппаратное обеспечение | Основные каналы утечки информации при подключении к сетям общего пользования. Методы и средства защиты информации при подключении к сетям общего пользования. Протоколы аутентификации при удаленном доступе.  Сканеры безопасности. Защита от анализаторов протоколов. Применение ПО Rapid7 Nexpose Community Edition для анализа защищенности автоматизированной системы. Межсетевые экраны – эффективная технология сетевой защиты информации. Современные требования к межсетевым экранам. Классификация и технология VPN. Системы обнаружения вторжений. Управление криптографическими ключами и хранение ключевой информации. Концепция иерархии ключей.  Развертывание защищенного рабочего места клиента VPN-сети на основе ПО ViPNet Client. Создание и модификация защищенной виртуальной сети ViPNet. | Методы защиты от изучения программ.  Защита операционных систем.  Сканеры безопасности. Межсетевые экраны.  Развертывание защищенного рабочего места клиента VPN-сети на основе ПО ViPNet Client. |
| 4 | Базы данных | Угрозы НСД, специфичные для СУБД. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы защиты данных встроенными средствами СУБД. Средства обеспечения защиты информации в СУБД: идентификация и проверка подлинности пользователей, управление доступом, поддержание целостности информации, организация аудита. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС. Типы контроля безопасности: потоковый, контроль вывода, контроль доступа.  Модели безопасности, применяемые при построении защиты в СУБД. Ссылочная целостность, триггерная и событийная реализации правил безопасности. Транзакция и восстановление. Кластерная организация серверов баз данных. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных. Особенности применения криптографических методов. Функции администратора безопасности баз данных. | Методы защиты данных встроенными средствами СУБД |
| 5 | Стандартизация и сертификация | Основные зарубежные и отечественные стандарты в области информационной безопасности и их применение. Классификация автоматизированных систем в соответствии с руководящими документами. Классификации и модели угроз безопасности информации в АС, представленные в основных отечественных и зарубежных стандартах и нормативных документах. Модель нарушителя при локальном и удалённом НСД.  Основы разработки и проектирования программно-аппаратных комплексов обеспечения информационной безопасности. Влияние стандартов безопасности на проектирование и разработку программно-аппаратных средств защиты информации. | Основы разработки и проектирования программно-аппаратных комплексов обеспечения информационной безопасности |

**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 6 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. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах.
2. Средства и методы ограничения доступа к файлам.
3. Классификация средств хранения ключей и идентифицирующей информации.
4. Методы противодействия динамическим способам снятия защиты программ от копирования.
5. Методы защиты программ от исследования.
6. Подходы к задаче защиты от копирования программ.
7. Общая характеристика и классификация компьютерных вирусов.
8. Общая характеристика средств нейтрализации компьютерных вирусов.
9. Защита на уровне загрузчиков операционной среды.
10. Архитектура подсистемы безопасности операционной системы Windows.
11. Разграничение прав пользователей в операционной системе Windows.
12. Аудит событий безопасности в операционной системе Windows.
13. Домены безопасности.
14. Микроядерная архитектура с точки зрения создания защищенных операционных систем.
15. Аутентификация пользователей при локальном и удаленном доступе к компьютерным сетям.
16. Средства обеспечения целостности и конфиденциальности при передаче информации по каналам связи.
17. Технология и классификация VPN.
18. Требования к межсетевым экранам.
19. Методы поиска уязвимостей.
20. Симметричные и асимметричные алгоритмы шифрования информации.
21. Функции удостоверяющего центра.
22. Структура удостоверяющего центра.
23. Концепция иерархии ключей.
24. Генерация и хранение ключей.
25. Распределение ключей.

**.**

**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

«Безопасность компьютерных систем»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | способность применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная |  | |
| профессиональная | + | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Умения: проводить мероприятия по обеспечению компьютерной безопасности  Навыки: использование программно-технических средств компьютерной безопасности | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
| ЗНАТЬ: классификации и модели угроз безопасности информации в автоматизированных системах;  принципы построения защищенных автоматизированных систем и типовые инструменты обеспечения безопасности информации, предусмотренные в современных операционных системах, СУБД, а также реализованные в специализированных средствах защиты информации;  методы и средства защиты от удаленных атак на сетевые ресурсы, обеспечения безопасности межсетевого взаимодействия;  основные направления применения криптографических технологий при защите автоматизированных 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: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения;  осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных средств защиты | | 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: навыками конфигурирования встроенных инструментов безопасности при администрировании распространенных операционных систем и СУБД;  навыками создания плана резервного копирования | | 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 | |
| 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: принципы организации систем обнаружения вторжений, мониторинга защищенности локальной и сетевой компьютерной среды. | | 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: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства защиты программного обеспечения;  устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения | | 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: навыками анализа защищенности автоматизированной системы с помощью специализированных программных средств;  навыками работы с программной и технической документацией на программно-аппаратные средства защиты информации | | 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 обеспечение безопасности компьютерных систем: Обслуживание программно-аппаратных средств защиты информации в операционных системах. Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях. Обслуживание средств защиты информации прикладного и системного программного обеспечения.

**VII.Дополнительная информация**



**VIII.Приложенные Скан-копии**

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

14.10.2020 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / П.В. Сараев /