МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ   
ОБРАЗОВАТЕЛЬНОЕ УЧЕРЕЖДЕНИЕ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М. Д. Миллионщикова

****

1. **ПАСПОРТ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

**«Безопасность IT-структуры»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | 24.09.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | ФГБОУ ВО «Грозненский государственный нефтяной технический университет имени академика М.Д.Миллионщикова» |
| 1.2 | Логотип образовательной организации | C:\Users\Laura\Downloads\ГГНТУ logo.png |
| 1.3 | Провайдер ИНН | 20200000531 |
| 1.4 | Ответственный за программу ФИО | Хаджиева Лаура Куйраевна |
| 1.5 | Ответственный должность | Старший преподаватель кафедры "Сети связи и системы коммутации" |
| 1.6 | Ответственный Телефон | +7 (928) 023 05 05 |
| 1.7 | Ответственный Е-mail | **l**aura.hadjieva3009@mail.ru |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Безопасность IT-структуры |
| 2.2 | Ссылка на страницу программы | https://www.netacad.com/ru/courses/cybersecurity |
| 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 | Образовательная программа предусматривает ее реализацию с применением дистанционных образовательных технологий, с возможностью передачи данных в форме цифрового следа на платформе ФГБОУ ВО "Грозненский государственный нефтяной технический университет имени академика М.Д.Миллионщикова" - htt://open.gstou.ru и образовательного контента сетевой академии Cisco. |
| 2.5 | Уровень сложности | Базовый |
| 2.6 | Количество академических часов | 72 |
| 2.7 | Практико-ориентированный 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) | Всего 72 часа, из них:  - теоретические занятия -28 час.;  - практические занятия -28 час.,  - самостоятельная работа- 8 час.;  - текущая контроль – 4 час.;  - итоговый контроль – 4 час. |
| 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 | Стоимость обучения одного обучающегося по образовательной программе установлено организацией: 25 000 рублей.  Ссылки на аналогичные программы других организаций:  **1)** <https://edu.softline.com/vendors/softline/obespechenie-bezopasnosti-personalnyh-dannyh-pri-ih-obrabotke-v-informacionnyh-sistemah-personalnyh-dannyh/>;  2) <https://meoshop.ru/product/povyishenie-kvalifikatsii/programma-kiberbezopasnost-i-zashhita-dannyh-v-tsifrovoj-obrazovatelnoj-srede-72-chasa/>;  3) <http://atcenter.ru/services/obuchenie-po-informatsionnoj-i-transportnoj-bezopasnosti/>;  4) <https://school.codeby.net/lms/courses/63-paranoid-anonimnost-i-bezopasnost-v-seti/preview.html?utm_source=checkroi.ru&utm_medium=checkroi.ru&utm_campaign=checkroi.ru> |
| 2.9 | Минимальное количество человек на курсе | 100 |
| 2.10 | Максимальное количество человек на курсе | 150 |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 130 чел. |
| 2.12 | Формы аттестации | Текущая аттестации слушателей -аттестация по отдельным разделам, темам и вопросам программы - проводится на основе результатов выполнения соответствующих учебных заданий (тестирование, практических заданий). Итоговая аттестация, рефлексия по образовательной программе согласно положению о ПЦС, проводится "Университетом 2035" по контрольно-измерительным материалам. |
| 2.13 | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Области реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа «Сетевое администрирование в телекоммуникациях»:  - владение инструментами работы с большими данными и инструментами визуализации;  - понимание основ кибербезопасности. |

1. **Аннотация образовательной программы**

**дополнительной профессиональной программы повышения квалификации**

**«Безопасность IT-структуры»**

**Целевая аудитория**

Лица, имеющие высшее или среднее профессиональное образование, руководители и персонал образовательных организаций, научно-педагогические работники учреждений высшего и среднего профессионального образования, работники системы дополнительного образования в возрасте от 18 лет до пенсионного возраста, а также ИТ-специалисты, которые хотели бы расширить свои базовые навыки в области маршрутизации, коммутации и кибербезопасности.

Слушатели курса  должны уже обладать следующими навыками и знаниями:  
- знания и навыки в области сетевых технологий на уровне CCENT;  
- базовые навыки работы с ПК и Интернетом.

**Цель курса**

- подготовка специалистов к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники, получение основополагающих знаний о программно-аппаратных средствах защиты информации в операционных системах, вычислительных сетях и системах управления базами данных, средствах антивирусной защиты, в освоении основ обеспечения безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности (согласно Профессиональному стандарту 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденному Министерством труда и социальной защиты Российской Федерации №598н от 1 ноября 2016г.)

Области реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа «Сетевое администрирование в телекоммуникациях»:

* владение инструментами работы с большими данными и инструментами визуализации;
* понимание основ кибербезопасности.

**Тематическая область знаний**

Кибербезопасность и защита данных

**Формируемые компетенции**

ПК-1: Способен обслуживать средства защиты информации в компьютерных системах и сетях.

ПК-2: Способен обслуживать программно-аппаратные средства защиты информации в операционных системах.

**Планируемые результаты обучения**

В результате освоения программы слушатель должен:

*знать:*

* архитектуру и пользовательские интерфейсы операционных систем;
* порядок обеспечения безопасности информации при эксплуатации операционных систем;
* источники угроз информационной безопасности и меры по их предотвращению;
* сущность и содержание понятия информационной безопасности, характеристики ее составляющих;
* типовые средства защиты информации в операционных системах;
* программно-аппаратные средства и методы защиты информации;
* порядок эксплуатации средств антивирусной защиты в операционных системах;
* формы и методы инструктажа пользователей по порядку работы в операционных системах;
* общие принципы функционирования программно-аппаратных средств криптографической защиты информации;
* порядок оформления эксплуатационной документации;
* нормативно-правовые акты в области защиты информации;
* организационные меры по защите информации.

*уметь:*

* настраивать компоненты подсистем защиты информации операционных систем;
* управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
* применять программно-аппаратные средства защиты информации в операционных системах;
* применять антивирусные средства защиты информации в операционных системах;
* работать в операционных системах с соблюдением действующих требований по защите информации;
* выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;

*иметь навыки:*

* ввода в эксплуатацию программно-аппаратных средств защиты информации в операционных системах;
* в установке средств антивирусной защиты в соответствии с действующими требованиями;
* в восстановлении работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации.

**Перечень основных разделов программы**

***Модуль 1. Особенности функционирования программно-аппаратных средств защиты информации***

[Основные понятия и определения](http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/lektsiya-1-po-ib-osnovnye-ponyatiya/). Индентификация пользователей КС как субъектов доступа к данным. Хранение аутентифицирующей информации в открытых компьютерных системах. Особенности программно-аппаратных комплексов защиты данных в локальных сетях и на рабочих местах.

***Модуль 2. Технологии межсетевого экранирования***

Механизмы работы средств межсетевого экранирования. Списки контроля доступа. Обход межсетевых экранов. Требования и показатели защищенности межсетевых экранов.

***Модуль 3. Системы обнаружения атак и вторжений***

[Модели систем обнаружения вторжений](http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/lektsiya-11-po-ib-kompyuternye-prestupleniya/). Обнаружение сигнатур. Обнаружение аномалий. Методы обхода систем обнаружения вторжений. Системы предупреждения вторжений.

***Модуль 4. Виртуальные частные сети. Защита от вредоносного программного обеспечения и удаленных атак***

Протоколы VPN канального уровня. Протокол IPSec. Типы вредоносного ПО и защита от угроз. Классификация и обобщенные сценарии атак. Атаки на сетевые протоколы и защита от них.

**Реализующее подразделение:** кафедра «Сети связи и системы коммутации» института прикладных информационных технологий ФГБОУ ВО ГГНТУ.

**Авторы программы:**

**- Степаненко Андрей Викторович –** руководитель Центра поддержки академий Cisco в ЮФО и СКФО, автор образовательной программы "Кибербезопасность".

Привлекается к реализации образовательной программы ФГБОУ ВО ГГНТУ на основе гражданско-правового договора;

- **Хаджиев Магомед Рамзанович** – доцент кафедры «Сети связи и системы коммутации», кандидат технических наук, доцент.

**Преподаватели:**

* **Хасамбиев Ибрагим Вахаевич** – доцент кафедры «Сети связи и системы коммутации», кандидат технических наук, доцент;
* **Хаджиев Магомед Рамзанович** – доцент кафедры «Сети связи и системы коммутации», кандидат технических наук, доцент;
* **Хаджиева Лаура Куйраевна** – старший преподаватель кафедры «Сети связи и системы коммутации».

**Форма обучения:** онлайн.

**Дата начала:** 02.11.2020

**Дата окончания:** 16.11.2020**.**

**Срок обучения:** 2 недели**.**

**Трудоемкость программы:** 72 часа.

**Выдаваемый документ:** удостоверение о повышении квалификации

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ   
ОБРАЗОВАТЕЛЬНОЕ УЧЕРЕЖДЕНИЕ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М. Д. Миллионщикова



**Дополнительная профессиональная программа повышения квалификации**

**«Безопасность IT-структуры»**

**72 час.**

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

- подготовка специалистов к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники, получение основополагающих знаний о программно-аппаратных средствах защиты информации в операционных системах, вычислительных сетях и системах управления базами данных, средствах антивирусной защиты, в освоении основ обеспечения безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности (согласно Профессиональному стандарту 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденному Министерством труда и социальной защиты Российской Федерации №598н от 1 ноября 2016г.)

Области реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа «Сетевое администрирование в телекоммуникациях»:

* владение инструментами работы с большими данными и инструментами визуализации;
* понимание основ кибербезопасности.

**2. Планируемые результаты обучения:**

2.1. Знание (осведомленность в областях):

* + 1. архитектуру и пользовательские интерфейсы операционных систем;
    2. порядок обеспечения безопасности информации при эксплуатации операционных систем;
    3. источники угроз информационной безопасности и меры по их предотвращению;
    4. сущность и содержание понятия информационной безопасности, характеристики ее составляющих;
    5. типовые средства защиты информации в операционных системах;
    6. программно-аппаратные средства и методы защиты информации;
    7. порядок эксплуатации средств антивирусной защиты в операционных системах;
    8. формы и методы инструктажа пользователей по порядку работы в операционных системах;
    9. общие принципы функционирования программно-аппаратных средств криптографической защиты информации;
    10. порядок оформления эксплуатационной документации;
    11. нормативно-правовые акты в области защиты информации;
    12. организационные меры по защите информации.

2.2. Умение (способность к деятельности)

* + 1. настраивать компоненты подсистем защиты информации операционных систем;
    2. управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
    3. применять программно-аппаратные средства защиты информации в операционных системах;
    4. применять антивирусные средства защиты информации в операционных системах;
    5. работать в операционных системах с соблюдением действующих требований по защите информации;
    6. выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации.

2.3. Навыки (использование конкретных инструментов)

* + 1. ввода в эксплуатацию программно-аппаратных средств защиты информации в операционных системах;
    2. в установке средств антивирусной защиты в соответствии с действующими требованиями;
    3. в восстановлении работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации.

**3.Категория слушателей**

3.1. Образование: высшее/ среднее профессиональное образование.

3.2. Квалификация: специалист среднего профессионального образования/бакалавр/специалист/ магистр.

**4.Учебный план программы «Безопасность IT-структуры»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| **1** | Модуль 1. Особенности функционирования программно-аппаратных средств защиты информации | 16 | 7 | 7 | 2 |
| **2** | Модуль 2. Технологии межсетевого экранирования | 16 | 7 | 7 | 2 |
| **3** | Модуль 3. Системы обнаружения атак и вторжений | 16 | 7 | 7 | 2 |
| **4** | Модуль 4. Виртуальные частные сети. Защита от вредоносного программного обеспечения и удаленных атак | 16 | 7 | 7 | 2 |
| Текущая контроль | | 4 | 28 | 28 | 8 |
| **Итоговая аттестация** | | 4 | **экзамен** | | |
| **Итого:** | | 72 |  | | |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | Модуль 1. Особенности функционирования программно-аппаратных средств защиты информации | **16** | **02.11.2020 –**  **05.11.2020** |
| **2** | Модуль 2. Технологии межсетевого экранирования | **16** | **06.11.2020 –**  **09.11.2020** |
| **3** | Модуль 3. Системы обнаружения атак и вторжений | **16** | **10.11.2020 –**  **12.11.2020** |
| **4** | Модуль 4. Виртуальные частные сети. Защита от вредоносного программного обеспечения и удаленных атак | **16** | **13.11.2020 –**  **16.11.2020** |
| **5** | Самостоятельная работа | **8** | **02.11.2020-16.11.2020** |
| **6** | Текущий контроль | **4** | **В конце каждого модуля** |
| **7** | Итоговая аттестация | **4** | **17.11.2020 –**  **21.11.2020** |
| **Всего:** | | **72 часа** |  |

**6.Учебно-тематический план программы «Сетевое администрирование в телекоммуникациях»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | **Модуль 1. Особенности функционирования программно-аппаратных средств защиты информации** | **16** | **5** | **9** | **2** | **тест** |
| 1.1 | [Основные понятия и определения](http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/lektsiya-1-po-ib-osnovnye-ponyatiya/). Индентификация пользователей КС как субъектов доступа к данным | 2 | 1 | 1 |  |  |
| 1.2 | Хранение аутентифицирующей информации в открытых компьютерных системах. | 7 | 2 | 4 | 1 |  |
| 1.3 | Особенности программно-аппаратных комплексов защиты данных в локальных сетях и на рабочих местах. | 7 | 2 | 4 | 1 |  |
| **2** | **Модуль 2. Технологии межсетевого экранирования** | **16** | **5** | **9** | **2** | **тест** |
| 2.1 | Механизмы работы средств межсетевого экранирования. Списки контроля доступа. | 2 | 1 | 1 |  |  |
| 2.2 | Обход межсетевых экранов | 7 | 2 | 4 | 1 |  |
| 2.3 | Требования и показатели защищенности межсетевых экранов | 7 | 2 | 4 | 1 |  |
| **3** | **Модуль 3. Системы обнаружения атак и вторжений** | **16** | **6** | **8** | **2** | **тест** |
| 3.1 | [Модели систем обнаружения вторжений](http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/lektsiya-11-po-ib-kompyuternye-prestupleniya/) | 4 | 2 | 2 |  |  |
| 3.2 | Обнаружение сигнатур. Обнаружение аномалий | 6 | 2 | 3 | 1 |  |
| 3.3 | Методы обхода систем обнаружения вторжений. Системы предупреждения вторжений. | 6 | 2 | 3 | 1 |  |
| **4** | **Модуль 4. Виртуальные частные сети. Защита от вредоносного программного обеспечения и удаленных атак** | **16** | **7** | **7** | **2** | **тест** |
| 4.1 | Протоколы VPN канального уровня. Протокол IPSec. | 4 | 2 | 2 |  |  |
| 4.2 | Типы вредоносного ПО и защита от угроз | 6 | 2 | 3 | 1 |  |
| 4.3 | Классификация и обобщенные сценарии атак. Атаки на сетевые протоколы и защита от них. | 6 | 2 | 3 | 1 |  |

**7. Учебная (рабочая) программа повышения квалификации «Сетевое администрирование в телекоммуникациях»**

**Модуль 1.Особенности функционирования программно-аппаратных средств защиты информации(16 час.)**

**Тема 1.1** [**Основные понятия и определения**](http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/lektsiya-1-po-ib-osnovnye-ponyatiya/)**. Индентификация пользователей КС как субъектов доступа к данным (2 час)**

**Содержание темы:**

В рамках данной темы рассматриваются объекты защиты информации, основные угрозы безопасности информации, основные понятия и концепции, идентификация и аутентификация.

**Тема 1.2 Хранение аутентифицирующей информации в открытых компьютерных системах (7 час)**

**Содержание темы:**

В данной теме рассматривается хранение аутентифицирующей информации в открытых компьютерных системах, протоколы стойкой удаленной аутентификации пользователей, Протокол CHAP, S/KEY.

**Тема 1.3 Особенности программно-аппаратных комплексов защиты данных в локальных сетях и на рабочих местах (7 час).**

**Содержание темы:**

В данной теме рассматриваются комплексы защиты данных на рабочих местах, особенности комплексов обеспечения защищенных сетевых соединений.

**Модуль 2. Технологии межсетевого экранирования****(16 час.)**

**Тема 2.1 Механизмы работы средств межсетевого экранирования. Списки контроля доступа. ( 2 час)**

**Содержание темы:**

В данной теме рассматривается фильтрация пакетов, типы межсетевых экранов, персональные и распределенные межсетевые экраны, назначение ACL, простые и расширенные списки.

**Тема 2.2** **Обход межсетевых экранов ( 7 час)**

**Содержание темы:**

В данной теме рассматриваются подходы обхода межсетевых экранов, таких как: постепенный подход и туннелирование.

**Тема 2.3**  **Требования и показатели защищенности межсетевых экранов ( 7 час)**

**Содержание темы:**

В данной теме рассматривается тестирование межсетевых экранов и показатели защищенности межсетевых экранов.

**Модуль 3. Системы обнаружения атак и вторжений (16 час.)**

**Тема 3.1** [**Модели систем обнаружения вторжений**](http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/lektsiya-11-po-ib-kompyuternye-prestupleniya/) **(4 час)**

**Содержание темы:**

В данной теме рассматриваются: модель Д.Деннинг и модель CIDF.

**Тема 3.2 Обнаружение сигнатур. Обнаружение аномалий. ( 6 час)**

**Содержание темы:**

В данной теме рассматривается система обнаружения вторжений Snort, правила Snort, методы Data Mining, методы технологии мобильных агентов методы построения иммунных систем.

**Тема 3.3** **Методы обхода систем обнаружения вторжений. Системы предупреждения вторжений ( 6 час)**

**Содержание темы:**

В данной теме рассматриваются методы обхода сетевых, методы обхода хостовых систем, принципы обнаружения вторжений и типы систем предупреждения вторжений.

**Модуль 4. Виртуальные частные сети. Защита от вредоносного программного обеспечения и удаленных атак(16 час.)**

**Тема 4.1** Протоколы VPN канального уровня. Протокол IPSec. **( 4 час)**

**Содержание темы:**

В данной теме рассматривается туннелирование, протоколы VPN канального уровня, туннельный и транспортный режим протокола, протокол обмена интернет-ключами.

**Тема 4.2** **Типы вредоносного ПО и защита от угроз ( 6 час)**

**Содержание темы:**

В данной теме рассматриваются типы вредоносного программного обеспечения, такие как: вирусы, черви, руткиты, типы атак и обобщенный сценарий атаки.

**Тема 4.3** **Классификация и обобщенные сценарии атак. Атаки на сетевые протоколы и защита от них**  **( 6 час)**

**Содержание темы:**

В данной теме рассматриваются атаки на протоколы транспортного уровня и атаки на протоколы сетевого уровня.

**8. Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1.1** | **1** | Практическое занятие 1. Изучение сетевых атак, а также инструментов для аудита безопасности и проведения атак | · Изучите произошедшие сетевые атаки.  ·-Выберите сетевую атаку и составьте по ней отчет для представления его аудитории.  · Изучите инструменты аудита безопасности.  · Выберите один из инструментов и составьте его презентацию для класса. |
| **1.6** | **2** | Практическое занятие 1. Развитие технологий межсетевого экранирования | Настройка и подготовка к работе Cisco ASA 550/5/  Инициализация ЦУС и ПУ ЦУС АПКШ «Континент»/. Правила фильтрации и трансляции. |
| **1.7** | **2** | Практическое занятие 2. Списки контроля доступа | Разработка расширенных ACL. Исследование работы простых списков контроля доступа. |
| **1.8** | **2** | Практическое занятие 3. Списки контроля доступа | Настройка и проверка ACL-списков для IPv6. Исследование работы простых списков контроля доступа |
| **1.11** | **3** | Практическое занятие 4. Модели систем обнаружения вторжений | Изучение программного обеспечения для мониторинга сети |
| **1.12** | **3** | Практическое занятие 5. Обнаружение сигнатур | Настройка Syslog и NTP |
| **1.14** | **4** | Практическое занятие 6. Протоколы VPN канального уровня | Отладка базового PPP с аутентификацией. Настройка базового PPP с аутентификацией. |
| **1.15** | **4** | Практическое занятие 7. Атаки на сетевые протоколы и защита от них | Сбор и анализ данных NetFlow. Настройка туннеля VPN GRE по схеме «точка-точка». Настройка Site-to-Site VPN IPSec с технологией NAT.  Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL. |
| **1.16** | **4** | Практическое занятие 8. Атаки на сетевые протоколы и защита от них | Поиск и устранение неполадок конфигураций NAT. Установка и предварительная настройка антивирусных программ. Настройка параметров безопасности коммутатора |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1** | 1.При качественном подходе риск измеряется в терминах?  2.При полномочной политике безопасности совокупность меток с одинаковыми значениями образует?  2.Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это?  3.Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это?  3.Программный модуль, кото­рый имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа?  4.Соответствие средств безопасности решаемым задачам характеризует?  5.С помощью закрытого ключа информация?  6.Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется?  7.Организационные требования к системе защиты?  8.Основу политики безопасности составляет?  9.Недостаток систем шифрования с открытым ключом?  10.Наукой, изучающей математические методы защиты информации путем ее преобразования, является?  11.Обеспечение целостности информации в условиях случайного воздействия изучается?  12. Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа?  13.Конечное множество используемых для кодирования информации знаков называется? | 1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.  2. Основные понятия информационной безопасности.  3. Структура понятия информационная безопасность.  4. Система защиты информации и ее структура.  5. Экономическая информация как товар и объект безопасности.  6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.  7. Персональные данные и их защита. 8. Информационные угрозы, их виды и причины возникновения.  9. Информационные угрозы для государства.  10. Информационные угрозы для компании. | 1. Модели угроз и нарушителей информационной безопасности  2. Программные закладки. Классификация, воздействие на компьютерную систему.  3. Методы защиты от программных закладок.  4. Методы защиты компьютерной системы от взлома.  5. Предотвращение взлома компьютерной системы на уровне СУБД  6. Предотвращение взлома компьютерной системы на уровне операционной системы.  7. Политика ИБ и политика СУИБ: сходства и различия.  8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.  9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  10. Анализ рисков ИБ: основные подходы, основные этапы процесса.  11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).  13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.  16. Система инженерно-технической защиты информации  17. Организационная основа системы обеспечения информационной безопасности РФ  18. Источники угроз информационной безопасности.  19. Защита информации. Основные термины и определения. |
| **2** | 1. Модели угроз и нарушителей информационной безопасности  2. Программные закладки. Классификация, воздействие на компьютерную систему.  3. Методы защиты от программных закладок.  4. Методы защиты компьютерной системы от взлома.  5. Предотвращение взлома компьютерной системы на уровне СУБД  6. Предотвращение взлома компьютерной системы на уровне операционной системы.  7. Политика ИБ и политика СУИБ: сходства и различия.  8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.  9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  10. Анализ рисков ИБ: основные подходы, основные этапы процесса.  11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).  13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.  16. Система инженерно-технической защиты информации  17. Организационная основа системы обеспечения информационной безопасности РФ  18. Источники угроз информационной безопасности.  19. Защита информации. Основные термины и определения. | 1 Информационные угрозы для личности (физического лица). 2. Действия и события, нарушающие информационную безопасность.  3. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.  4. Способы воздействия информационных угроз на объекты.  5. Внешние и внутренние субъекты информационных угроз.  6. Компьютерные преступления и их классификация.  7. Исторические аспекты компьютерных преступлений и современность.  8. Субъекты и причины совершения компьютерных преступлений.  9. Вредоносные программы, их виды. 10. История компьютерных вирусов и современность.  11. Государственное регулирование информационной безопасности. | 1. Фильтрация пакетов. 2. Типы межсетевых экранов. 3. Персональные и распределенные межсетевые экраны. 4. Назначение ACL. 5. Простые и расширенные списки. 6. Подходы обхода межсетевых экранов. 7. Постепенный подход. 8. Туннелирование. 9. Тестирование межсетевых экранов. 10. Показатели защищенности межсетевых экранов |
| 3 | 1. Фильтрация пакетов. 2. Типы межсетевых экранов. 3. Персональные и распределенные межсетевые экраны. 4. Назначение ACL. 5. Простые и расширенные списки. 6. Подходы обхода межсетевых экранов. 7. Постепенный подход. 8. Туннелирование. 9. Тестирование межсетевых экранов. 10. Показатели защищенности межсетевых экранов | 1. Деятельность международных организаций в сфере информационной безопасности.  2. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.  3. Доктрина информационной безопасности России. 4. Уголовно-правовой контроль над компьютерной преступностью в России. 2  5. Федеральные законы по ИБ в РФ. 27. Политика безопасности и ее принципы.  6. Фрагментарный и системный подход к защите информации. 7. Методы и средства защиты информации.  8. Организационное обеспечение ИБ.  9. Организация конфиденциального делопроизводства.  10. Комплекс организационно-технических мероприятий по обеспечению защиты информации. | 1. Модель контроля целостности Кларка-Вилсона.  2. Модель безопасности на основе матрицы доступов HRU.  3. Модель распространения прав доступа TAKE-GRANT.  4. Модель системы безопасности Белла-Лападула.  5. Модель безопасности информационных потоков.  5. Модели нарушителя информационных систем.  6. Модели нарушения целостности программ и данных в электронно-вычислительных машинах.  7. Теория безопасных систем. ТСВ.  8. Политики безопасности. Домены безопасности. Основные типы.  9. Парольная защита Требования и атаки.  10. Криптографические методы защиты. Основные требования, модели, способы и реализации. |
| 4 | 1. Модель контроля целостности Кларка-Вилсона.  2. Модель безопасности на основе матрицы доступов HRU.  3. Модель распространения прав доступа TAKE-GRANT.  4. Модель системы безопасности Белла-Лападула.  5. Модель безопасности информационных потоков.  5. Модели нарушителя информационных систем.  6. Модели нарушения целостности программ и данных в электронно-вычислительных машинах.  7. Теория безопасных систем. ТСВ.  8. Политики безопасности. Домены безопасности. Основные типы.  9. Парольная защита Требования и атаки.  10. Криптографические методы защиты. Основные требования, модели, способы и реализации. | 1. Инженерно-техническое обеспечение компьютерной безопасности.  12. Организационно-правовой статус службы безопасности.  13. Защита информации в Интернете.  14. Электронная почта и ее защита.  15. Защита от компьютерных вирусов.  16. «Больные» мобильники и их «лечение».  17. Популярные антивирусные программы и их классификация.  18. Организация системы защиты информации экономических объектов.  19.Криптографические методы защиты информации.  20. Этапы построения системы защиты информации.  21. Оценка эффективности инвестиций в информационную безопасность.  22. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.  23. Управление информационной безопасности на государственном уровне.  24. Аудит ИБ автоматизированных банковских систем. 25. Электронная коммерция и ее защита.  26. Менеджмент и аудит информационной безопасности на уровне предприятия. 27. Информационная безопасность предпринимательской деятельности.  28. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов. | 1. Асимметричное шифрование. Модели и алгоритмы.  2. Симметричное шифрование. Модели и алгоритмы.  3. Электронно-цифровая подпись. Модели, требования, атаки, способы обмана, реализация ЭЦП.  4. Криптографические атаки на схемы шифрования.  5. Критерии оценки безопасности компьютерных систем министерства обороны США («Оранжевая книга»).  6. Европейские критерии безопасности информационных технологий.  7. Федеральные критерии безопасности информационных технологий.  8. Руководящие документы Государственной Технической Комиссии при Президенте РФ.  9. Защита распределенных баз данных: транзакция, репликация, резервирование и другие особенности по надежности.  10. Общие положения криптографии. Имитостойкость, имитозащита.  11. Криптографические алгоритмы. Перемешивания и рассеивания. Подстановки.  12. Реализация шифров. Методы получения случайных и псевдослучайных чисел.  13. Блочные и поточные шифры на основе реализации требований ГОСТ 28147-99  14. Блочные и поточные шифры на основе симметричных криптографических алгоритмов.  15. Методы анализа симметричных криптосистем.  16. Методы криптоанализа несимметричных криптосистем  17. Протокол SSH.  18. Применение криптографических алгоритмов для обеспечения безопасности информации в информационных системах. Технология VPN.  19. Технологии WPA и WPA2.  20. Применение криптографических алгоритмов для обеспечения безопасности информации в информационных системах.  21. Основы технологии инфраструктуры открытых ключей.  22. Основные компоненты и сервисы ИОК.  23. Введение в компьютерные атаки. Модель атаки. Результат атаки.  24. Атаки с использованием промежуточных узлов и территорий.  25. Технологии обнаружения компьютерных атак и их возможности.  26. Модели нарушителей информационной безопасности  27. Модели угроз информационной безопасности  28. Программные закладки. Классификация, воздействие на компьютерную систему.  29. Методы защиты от программных закладок.  30. Методы защиты компьютерной системы от взлома.  31. Назначение межсетевых экранов.  32. Уровни сетевой модели, на которых применяется фильтрация пакетов.  33. Статическая и динамическая трансляция адресов.  34. Значение функции трансляции адресов с точки зрения обеспечения информационной безопасности.  35. Предотвращение взлома компьютерной системы на уровне СУБД  36. Предотвращение взлома компьютерной системы на уровне операционной системы.  37. Политика ИБ и политика СУИБ: сходства и различия.  38. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.  39. Анализ рисков ИБ: основные понятия  40. Цели и задачи процесса анализа рисков, роль процесса в рамках СУИБ.  41. Анализ рисков ИБ: основные подходы, основные этапы процесса.  42. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  43. Расследование инцидентов ИБ  44. Виды расследования инцидентов  45. Критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).  46. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  47. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.  48. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.  49. Система инженерно-технической защиты информации  50. Организационная основа системы обеспечения информационной безопасности РФ  51. Источники угроз информационной безопасности.  52. Защита информации. Основные термины и определения |

**8.2.**  **Описание показателей и критериев оценивания, шкалы оценивания.**

*Практические задания* – задания, выполняемые с использованием изучаемого программного обеспечения с целью углубления и закрепления теоретических знаний и развития навыков самостоятельного проведения эксперимента.

*Тестирование* - это форма измерения знаний обучаемых, основанная на применении педагогических тестов. Тестирование содержит список вопросов и различные варианты ответов, с выбором одного правильного ответа. Каждый вопрос оценивается в определенное количество бал лов. В тесте 10 вопросов, вес каждого вопроса - 10 баллов, итого обучаемый может набрать -100 баллов.

Определение результатов оценивания: по результатам выполненных контрольных работ выставляются оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценивание производится в соответствии с критериями:

«отлично» – задание выполнено полностью и правильно;

«хорошо» – задание выполнено полностью, но решение содержит несущественные ошибки;

«удовлетворительно» – задание выполнено не полностью или содержит существенные ошибки;

«неудовлетворительно» – задание не выполнено или выполнено в корне неверно.

86 баллов и более - "отлично".

71-85 баллов - "хорошо".

56-70 баллов - "удовлетворительно".

55 баллов и менее - "неудовлетворительно"

**8.3.**  **Примеры контрольных заданий по модулям или всей образовательной программе.**

**Практико-ориентированные задания**

**Задание 1.1** Изучение сетевых атак, а также инструментов для аудита безопасности и проведения атак:

-Изучите произошедшие сетевые атаки.

-Выберите сетевую атаку и составьте по ней отчет для представления его аудитории.

- Изучите инструменты аудита безопасности.

-Выберите один из инструментов и составьте его презентацию для класса.

**Задание 1.2** Развитие технологий межсетевого экранирования

- Настройка и подготовка к работе Cisco ASA 550/5/

- Инициализация ЦУС и ПУ ЦУС АПКШ «Континент»/.

- Правила фильтрации и трансляции.

**Задание 1.3** Списки контроля доступа

-Разработка расширенных ACL.

-Исследование работы простых списков контроля доступа.

**Задание 1.4** Списки контроля доступа

- Настройка и проверка ACL-списков для IPv6.

- Исследование работы простых списков контроля доступа.

**Задача 1.5** Модели систем обнаружения вторжений

-Изучение программного обеспечения для мониторинга сети

**Задача 1.6** Обнаружение сигнатур

- Настройка Syslog и NTP.

**Задача 1.7** Протоколы VPN канального уровня

-Отладка базового PPP с аутентификацией.

- Настройка базового PPP с аутентификацией.

**Задача 1.8** Атаки на сетевые протоколы и защита от них

-Сбор и анализ данных NetFlow.

-Настройка туннеля VPN GRE по схеме «точка-точка».

-Настройка Site-to-Site VPN IPSec с технологией NAT.

-Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL.

**Задача 1.9** Атаки на сетевые протоколы и защита от них

-Поиск и устранение неполадок конфигураций NAT.

-Установка и предварительная настройка антивирусных программ.

-Настройка параметров безопасности коммутатора.

**8.4.**  **Тесты и обучающие задачи (кейсы), иные практико-ориентированные формы заданий.**

При качественном подходе риск измеряется в терминах?

A.денежных потерь

B.заданных с помощью шкалы или ранжирования

C.оценок экспертов

D.объема информации

ANSWER: B

При полномочной политике безопасности совокупность меток с одинаковыми значениями образует?

A.область равной критичности

B.область равного доступа

C.уровень безопасности

D.уровень доступности

ANSWER: C

Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это?

A.уязвимость информации

B.надежность информации

C.защищенность информации

D.базопасность информации

ANSWER: D

Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это?

A.аудит

B.аутентификация

C.авторизация

D.идентификация

ANSWER: B

Программный модуль, кото­рый имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа?

A.фильтр

B.заместитель

C.перехватчик

D.имитатор

ANSWER: D

Соответствие средств безопасности решаемым задачам характеризует?

A.эффективность

B.корректность

C.адекватность

D.унификация

ANSWER: A

С помощью закрытого ключа информация?

A.копируется

B.транслируется

C.расшифровывается

D.зашифровывается

ANSWER: C

Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется?

A.избирательным

B.мандатным

C.привилегированным

D.идентифицируемым

ANSWER: B

Организационные требования к системе защиты?

A.управленческие и идентификационные

B.административные и аппаратурные

C.административные и процедурные

D.аппаратурные и физические

ANSWER: C

Основу политики безопасности составляет?

A.программное обеспечение

B.управление риском

C.способ управления доступом

D.выбор каналов связи

ANSWER: C

Недостаток систем шифрования с открытым ключом?

A.при использовании простой замены легко произвести подмену одного шифрованного текста другим

B.относительно низкая производительность

C.знеобходимость распространения секретных ключей

D.на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

ANSWER: B

Наукой, изучающей математические методы защиты информации путем ее преобразования, является?

A.криптоанализ

B.криптология

C.стеганография

D.криптография

ANSWER: B

Обеспечение целостности информации в условиях случайного воздействия изучается?

A.стеганографией

B.теорией помехоустойчивого кодирования

C.криптологией

D.криптоанализом

ANSWER: B

Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа?

A.перехват

B.уборка мусора

C.наблюдение

D компроме­тация

ANSWER: D

Конечное множество используемых для кодирования информации знаков называется?

A.шифром

B.кодом

C.алфавитом

D.ключом

ANSWER: C

**8.5.**  **Описание процедуры оценивания результатов обучения.**

Оценка уровня сформированности (освоения) компетенций осуществляется на основе таких составляющих как: знание, умение, владение навыками и/или опытом деятельности в соответствии с планируемыми результатами обучения по ДПП. В качестве критериев оценки уровня сформированности (освоения) у слушателей компетенций при проведении итогового зачета/экзамена с применением средств электронного обучения, применяется 4–балльная шкала (таблица 1).

**Таблица 1–Критерии оценки уровня сформированности компетенций**

|  |  |
| --- | --- |
| **Оценка компетенции**  **(4-балльная шкала)** | **Характеристика сформированных компетенций** |
| **«отлично»**  **зачтено** | – слушатель глубоко и всесторонне усвоил учебный материал ДПП;  – уверенно, логично, последовательно и грамотно его излагает;  – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения к практической деятельности;  – умело обосновывает и аргументирует выдвигаемые им идеи;  – делает выводы и обобщения;  – свободно владеет системой специализированных понятий;  - выполнил ВАР на высоком профессиональном уровне |
| **«хорошо»**  **зачтено** | – слушатель твердо усвоил учебный материал ДПП, грамотно и по существу излагает его, опираясь на знания основной литературы;  – не допускает существенных неточностей;  – увязывает усвоенные знания с практической деятельностью;  – аргументирует научные положения;  – делает выводы и обобщения;  – владеет системой специализированных понятий;  - выполнил ВАР на хорошем уровне. |
| **«удовлетворительно»**  **зачтено** | – слушатель усвоил только основной учебный материал ДПП, по существу излагает его, опираясь на знания только основной литературы;  – допускает несущественные ошибки и неточности;  – испытывает затруднения в практическом применении знаний;  – слабо аргументирует научные положения;  – затрудняется в формулировании выводов и обобщений;  – частично владеет системой специализированных понятий;  - выполнил ВАР на среднем уровне. |
| **«неудовлетворительно»**  **не зачтено** | – слушатель не усвоил значительной части учебного материала ДПП;  – допускает существенные ошибки и неточности при рассмотрении проблем;  – испытывает трудности в практическом применении знаний;  – не может аргументировать научные положения;  – не формулирует выводов и обобщений;  - не выполнил ВАР или содержание работы не соответствует тематике. |

**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** |
|  | **Степаненко Андрей Викторович** | Руководитель Центра поддержки академий Cisco в ЮФО и СКФО, автор образовательной программы "Кибербезопасность". | [http://ipit.gstou.ru/%d0%ba%d0%b0%d1%84%d0%b5%d0%b4%d1%80%d0%b 0-%d1%81%d0%ba](http://ipit.gstou.ru/%d0%ba%d0%b0%d1%84%d0%b5%d0%b4%d1%80%d0%25b%200-%d1%81%d0%ba) | **C:\Users\Acer\Downloads\IMG_20201022_100814.jpg** | **C:\Users\Acer\Downloads\подпись1.jpg** |
| **1** | **Хасамбиев Ибрагим Вахаевич** | ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. Акад. М.Д. Миллионщикова», к.т.н., доцент кафедры «Сети связи и системы коммутации» | <http://ipit.gstou.ru/%d0%ba%d0%b0%d1%84%d0%b5%d0%b4%d1%80%d0%b0-%d1%81%d0%ba> | **C:\Users\Laura\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Хасамбиев И.В..jpg** | C:\Users\Laura\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Хас.png |
| **2** | **Хаджиев Магомед Рамзанович** | ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. Акад. М.Д. Миллионщикова», к.т.н., доцент кафедры «Сети связи и системы коммутации» |  | **C:\Users\Laura\Desktop\Хаджиев М.Р..JPG** |  |
|  | **Хаджиева Лаура Куйраевна** | ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. Акад. М.Д. Миллионщикова», старший преподаватель кафедры «Сети связи и системы коммутации» | <http://ipit.gstou.ru/%d0%ba%d0%b0%d1%84%d0%b5%d0%b4%d1%80%d0%b0-%d1%81%d0%ba> |  | **C:\Users\Laura\Desktop\Хад.png** |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Адаптивное тестирование, самостоятельная работа, рефлексия | 1.Бизяев, А. А. Сети связи и системы коммутации. Практикум: учебное пособие / А. А. Бизяев, К. А. Куратов. – Новосибирск: Новосибирский государственный технический университет, 2016. – 84 c. – ISBN 978-5-7782-2935-8.  2.Практикум по дисциплине Сетевая безопасность и ее планирование / составители В. А. Докучаев [и др.], под редакцией В. А. Докучаев. – Москва: Московский технический университет связи и информатики, 2016. – 28 c. – ISBN 2227-8397. 3.Семенов, А. А. Сетевые технологии и Интернет: учебное пособие / А. А. Семенов. – Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. – 148 c. – ISBN 978-5-9227-0662-9.  3. Платонов, Владимир Владимирович. Программно-аппаратные средства защиты информации : учебник для вузов / В.В. Платонов. - Москва : Академия, 2013. - 330, [1] с. : ил. ; 22. - (Высшее профессиональное образование. Информационная безопасность. Бакалавриат). - Библиогр.: с. 326-327. - 1000 экз. -ISBN 978-5-7695-9327-7.  4. Программно-аппаратные средства защиты информации : учеб. пособие : специальность 090103 - Организация и технология защиты информации / М-во образования и науки Рос. Федерации, ГОУ ВПО "Ставроп. гос. ун-т" / авт.- сост. В. А. Грицык. - Ставрополь : Изд-во СГУ, 2010. - 95 с.  Дополнительная литература:  1. А.В. Спесивцев, В.А. Вегнер. Л.К). Крутиков, В.В. Серегин, В.А. Сидоров - Защити информации в персональных ЭВМ. - М.: Радио и связь, - 200.  2. С. П. Расторгуев Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен. 2003.  3. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Концепция зашиты СВТ и АС от НСД к информации. - М.: Воениздат, 2004. В. 7.Гайкович. А. Першин Безопасность электронных банковских систем. - М.: Единая Европа.2004.  4. Зегжда Д.П. Ивашко A.M. Основы безопасности информационных систем. - М: «Горячая линия Телеком», 2000.  Методическая литература:  -Учебное пособие «Программно-аппаратные средства защиты информации : учеб. пособие : специальность 090103 - Организация и технология защиты информации / М-во образования и науки Рос. Федерации, ГОУ ВПО "Ставроп. гос. ун-т" / авт.- сост. В. А. Грицык. - Ставрополь : Изд-во СГУ, 2010. - 95 с.» |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| <http://open.gstou.ru> | <https://www.netacad.com/courses/all-courses> |
| http://www.infosec.ru/ | <https://www.netacad.com/virtual/app/introduction-packet-tracer> |
|  | <http://blog.netskills.ru/> |

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

|  |  |
| --- | --- |
| **Вид занятий** | **Наименование оборудования,**  **программного обеспечения** |
| Лекции | Лекционный зал (ГУК 2-23)  **Техническое обеспечение:** Проектор BenQ MS502 – 1шт; Настенный экран Lumen – 1шт; Подключение к Интернету (Вайнах-телеком). Веб-камера, наушники, микрофон для текстовой, голосовой и видеосвязи обучающихся и преподавателей, персональный компьютер для преподавателя. **Программное обеспечение:**  ОС Windows-10, Microsoft Office-10, Adobe Acrobat Reader; Visual Studio, HTML-Kit (редактор веб-страниц), Smart Web Builder, WebSite X5 Free, Artweaver (Бесплатный растровый графический редактор), среда программирования WingWare. |
| Практическое занятие | Лабораторная аудитория для проведения занятий лабораторного и практического тип (ГУК-2-04. Лаборатория Cisco)  **Техническое обеспечение:**  Компьютеры (15 шт): CPU: Intel Core i3 2120; Mainboard: Asus P8H61-M LX3; RAM: Samsung DDR3 4Gb PC3-10700; HDD: 500Gb Seagate ST500DM002; PC Case: Quri + 450W; Проектор BenQ MS502 – 1шт; Настенный экран Lumen – 1шт; Подключение к Интернету (Вайнах-телеком). Веб-камера, наушники, микрофон для текстовой, голосовой и видеосвязи обучающихся и преподавателе  (процессор IntelPentiumCore 2, оперативная память 4 Гб, жесткий диск 500 Гб, DVD±R/RW, монитор TFT 19", 1280x1024). — 12 шт.;  IP АТС;  сервер HP ProLiant DL1000 G6;  коммутаторы Huawei S2326TP-EI-AC;  коммутаторы Cisco Catalyst WS-C2960-24TT-L;  коммутаторы JuniperEX2200-24P;  коммутаторы SNR-S2950-24G;  маршрутизаторы Mikrotik Cloud Core Router 1016-12G;  маршрутизаторы Cisco 3925;  шлюз VoIP SNR, 4 FXO, 4 FXS, 2 RJ45;  устройство анализа и классификации трафика СКАТ-6 Complete, NAGBundle;  IP-телефоны CiscoCP-7970G;  шкаф Стойка 42U;  JuniperSRX240H; межсетевой экран CiscoASA5520;  нuaweiAR2200;  беспроводной маршрутизатор MikrtoikRB 2011  **Программное обеспечение:**  ОС Windows-10, Microsoft Office-10, Adobe Acrobat Reader; Visual Studio, HTML-Kit (редактор веб-страниц), Smart Web Builder, WebSite X5 Free, Artweaver (Бесплатный растровый графический редактор), среда программирования WingWare, ПО Secret Net 5.0, ПО Dallas Lock 7.0, ПО Secret Disk. |

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ   
ОБРАЗОВАТЕЛЬНОЕ УЧЕРЕЖДЕНИЕ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М. Д. Миллионщикова



**ПАСПОРТ КОМПЕТЕНЦИИ**

Сетевое администрирование в телекоммуникациях

(наименование дополнительной профессиональной образовательной программы повышения квалификации)

ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. Акад. М.Д. Миллионщикова»

(наименование организации, реализующей дополнительную профессиональную образовательную программу повышения квалификации)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1.** | **Наименование компетенций** | | способность осуществлять техническую поддержку процессов создания (модификации) и сопровождения информационных ресурсов | |
| **2.** | **Указание типа компетенции** | Общекультурная/универсальная | профессиональная | |
| общепрофессиональная |
| профессиональная |
| профессиональная -специализированная |
| **3.** | **Определение, содержание и основные сущностные характеристики компетенции** | | ПК-1: Способен обслуживать средства защиты информации в компьютерных системах и сетях.  ПК-2: Способен обслуживать программно-аппаратные средства защиты информации в операционных системах. | |
| **4.** | **Дескриптор знаний, умений и навыков**  **по уровням** | | **Уровни сформированности компетенции обучающегося** | **Индикаторы** |
|  | | **Начальный уровень**  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) |  |
|  | ПК-1 Способен администрировать процессы контроля производительных устройств и программного обеспечения. | | **Базовый уровень** (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности | В результате освоения программы слушатель должен:  *знать:*   * архитектуру и пользовательские интерфейсы операционных систем; * порядок обеспечения безопасности информации при эксплуатации операционных систем; * источники угроз информационной безопасности и меры по их предотвращению; * сущность и содержание понятия информационной безопасности, характеристики ее составляющих; * типовые средства защиты информации в операционных системах; * программно-аппаратные средства и методы защиты информации; * порядок эксплуатации средств антивирусной защиты в операционных системах; * формы и методы инструктажа пользователей по порядку работы в операционных системах; * общие принципы функционирования программно-аппаратных средств криптографической защиты информации; * порядок оформления эксплуатационной документации; * нормативно-правовые акты в области защиты информации; * организационные меры по защите информации.   *уметь:*   * настраивать компоненты подсистем защиты информации операционных систем; * управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей; * применять программно-аппаратные средства защиты информации в операционных системах; * применять антивирусные средства защиты информации в операционных системах; * работать в операционных системах с соблюдением действующих требований по защите информации; * выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;   *иметь навыки:*   * ввода в эксплуатацию программно-аппаратных средств защиты информации в операционных системах; * в установке средств антивирусной защиты в соответствии с действующими требованиями; * в восстановлении работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации. |
|  | | **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной |  |
|  |  | | **Профессиональный** (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) |  |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Для формирования компетенции базового уровня слушатели   должны уже обладать следующими навыками и знаниями: ● знания и навыки в области сетевых технологий на уровне CCENT ● базовые навыки работы с ПК и Интернетом. | |
|  | Средства и технологии оценки | | автоматизированные системы контроля на платформе в виде цифрового следа:  -<http://open.gstou.ru>;  -платформа академии Cisco: <https://www.netacad.com/portal/web/self-enroll/m/course-77645> | |

**V. Рекомендаций к программе от работодателей**:

По данной программе представлены рекомендации от работодателей:

* 1. АО «Вайнах Телеком»;
  2. АО «Альфа-СТК».

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

**Сценарии профессиональной траектории граждан:**

|  |  |  |
| --- | --- | --- |
| **Цели получения персонального цифрового сертификата** | | |
| **Текущий статус** | **Цель**  подготовка специалистов к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники, получение основополагающих знаний о программно-аппаратных средствах защиты информации в операционных системах, вычислительных сетях и системах управления базами данных, средствах антивирусной защиты, в освоении основ обеспечения безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности (согласно Профессиональному стандарту 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденному Министерством труда и социальной защиты Российской Федерации №598н от 1 ноября 2016г.) | |
| **Развитие компетенций в текущей сфере занятости** | | |
| работающий по найму в организации, на предприятии | | развитие профессиональных качеств |
| **Переход в новую сферу занятости** | | |
| освоение смежных профессиональных областей | | повышение уровня дохода, расширение профессиональной деятельности |

**VII.Дополнительная информация**

**Реализующее подразделение:** ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова», Институт прикладных информационных технологий, кафедра «Информационные технологии» (<http://ipit.gstou.ru>).

**Ссылка на образовательную программу:** <https://open.gstou.ru/course/view.php?id=40>

**Авторы программы**:

**- Степаненко Андрей Викторович –** руководитель Центра поддержки академий Cisco в ЮФО и СКФО, автор образовательной программы "Кибербезопасность".

Привлекается к реализации образовательной программы ФГБОУ ВО ГГНТУ на основе гражданско-правового договора;

- доцент кафедры «Сети связи и системы коммутации», института прикладных информационных технологий Хаджиев Магомед Рамзанович.

**Список преподавателей, реализующих программу:**

1. к.т.н., доцент кафедры «Сети связи и системы коммутации», института прикладных информационных технологий Хаджиев Магомед Рамзанович;
2. к.т.н., доцент кафедры института прикладных информационных технологий «Сети связи и системы коммутации» Хасамбиев Ибрагим Вахаевич.
3. Старший преподаватель института прикладных информационных технологий кафедры «Сети связи и системы коммутации» Хаджиева Лаура Куйраевна

**Форма обучения:** онлайн-обучение.

**Дата начала:** 02.11.2020-16.11.2020**.**

**Срок обучения:** 2 недели**.**

**Трудоемкость программы:** 72 часа.

**Выдаваемый документ:** удостоверение о повышении квалификации

**VIII.Приложенные Скан-копии**

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