Министерство образования и науки Российской Федерации

Московский государственный университет имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ Декан факультета ВМК\_\_\_\_\_\_\_\_\_\_\_\_\_Е.И. Моисеев ″\_\_\_\_″ \_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. |

**ПРОГРАММА**

повышения квалификации

**Основы сетевой безопасности**

 (наименование программы)

Москва – 2018 г.

**1. Цель реализации программы**

После прослушивания курса и успешной сдачи экзамена слушатели будут

**Знать**

Понятия и определения, относящиеся к информационной безопасности, основные алгоритмы симметричного и асимметричного шифрования, криптографические хэш-функции и способы аутентификации сообщений, основные понятия инфраструктуры открытого ключа; принципы создания безопасной ИТ-инфраструктуры, основные технологии туннелирования прикладного и сетевого уровней, классификацию межсетевых экранов, классификацию систем обнаружения и предотвращения проникновений.

**Уметь**

Использовать различные механизмы и сервисы обеспечения безопасности в протоколах туннелирования, создавать политики межсетевых экранов и систем обнаружения проникновений.

**Владеть**

Методологией создания политики безопасности, политик межсетевых экранов и систем обнаружения проникновения.

**2. Формализованные результаты обучения**

Курс предполагает изучение методологических и алгоритмических основ, стандартов, а также механизмов и сервисов безопасности информационных технологий. Значительное внимание уделяется изучению наиболее важных сервисов и механизмов защиты информации, криптографических алгоритмов и протоколов, проблем информационной безопасности в сети интернет. В частности рассмотрены основные алгоритмы симметричного шифрования: DES, 3DES, IDEA, ГОСТ 28147, Blowfish, Rijndael, а также режимы их использования; рассмотрены алгоритмы шифрования с открытым ключом RSA, Диффи-Хеллмана и DSS, рассмотрены принципы распределения открытых ключей, стандарт Х.509 третьей версии и принципы создания инфраструктуры открытого ключа, рассмотрены наиболее широко используемые протоколы сетевой безопасности прикладного уровня и протокол создания виртуальных частных сетей.

Рассматриваются технологии межсетевых экранов, систем обнаружения проникновений. Основное внимание уделяется получению практических навыков по созданию безопасной сетевой инфраструктуры, в частности развертыванию и настройки межсетевых экранов.

Рассматриваются наиболее широко используемые протоколы сетевой безопасности прикладного, сетевого и канального уровней. Основное внимание уделяется получению практических навыков, необходимым для развертывания и настройки виртуальных частных сетей.

**3. Содержание программы**

**Учебный план**

программы повышения квалификации

 «**Основы сетевой безопасности**»

**Категория слушателей:**  сетевые администраторы, желающие изучить теоретические основы сетевой безопасности, необходимые для развертывания и настройки виртуальных частных сетей.

**Срок обучения:** 72 часа дистанционной работы, 72 часа аудиторной (лабораторной) работы и 144 часа самостоятельной работы.

**Режим занятий:** 1 раз в неделю по 4 ак.часа или 4 дня по 8 ак. часов.

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименованиеразделов | Всего дистанционной и аудиторной работы(ак. часов) | В том числе |
| Дистанционная работа (лекции) | практич. и лаборат.занятия |
|  | Основные принципы создания надежной и безопасной ИТ-инфраструктуры | **6** | 2 | 4 |
|  | Сегментирование сетей на канальном уровне | **10** | 6 | 4 |
|  | Технологии межсетевых экранов | **28** | 12 | 16 |
|  | Криптографические механизмы безопасности | **20** | 20 | 0 |
|  | Технологии туннелирования | **44** | 16 | 28 |
|  | Аутентификация и хранение учетных записей | **12** | 4 | 8 |
|  | Системы обнаружения и предотвращения проникновений (IDPS) | **14** | 8 | 6 |
|  | Приоритезация трафика и создание альтернативных маршрутов | **10** | 4 | 6 |
|  |  | **144** | **72** | **72** |
| Итоговая аттестация | Сертификационный экзамен |

Учебно-тематический план

программы повышения квалификации

**«Основы сетевой безопасности»**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование разделов и тем | Всего дистанционной и аудиторной работы(ак. часов) | В том числе |
| Дистанционная работа (лекции) | практич.и лаборат. занятия |
| 1 | 2 | 3 | 4 | 5 |
| **1** | **Основные принципы создания надежной и безопасной ИТ-инфраструктуры**  | **6** | **2** | **4** |
| 1.1 | Введение. Классификация сетевых атак | 3 | 1 | 2 |
| 1.2 | Основные сервисы создания безопасной ИТ-инфраструктуры. Криптографические механизмы безопасности | 3 | 1 | 2 |
| **2** | **Сегментирование сетей на канальном уровне**  | **10** | **6** | **4** |
| 2.1 | Использование технологии VLAN для создания подсетей | 3 | 2 | 1 |
| 2.2 | Стандарт IEEE 802.1Q | 2 | 1 | 1 |
| 2.3 | Типовая топология сети с использованием VLAN | 2 | 1 | 1 |
| 2.4 | VLAN на основе портов | 3 | 2 | 1 |
| **3** | **Технологии межсетевых экранов** | **28** | **12** | **16** |
| 3.1 | Основные понятия сетевых технологий (стек протоколов, состояния ТСР-соединения) | 4 | 2 | 2 |
| 3.2 | Классификация межсетевых экранов | 4 | 2 | 2 |
| 3.3 | Политика межсетевого экрана | 6 | 2 | 4 |
| 3.4 | Межсетевые экраны с возможностями NAT | 6 | 2 | 4 |
| 3.5 | Топология сети при использовании межсетевых экранов | 4 | 2 | 2 |
| 3.6 | Планирование и внедрение межсетевого экрана | 4 | 2 | 2 |
| 4 | **Криптографические механизмы безопасности** | **20** | **20** | 0 |
| 4.1 | Алгоритмы симметричного шифрования | 6 | 6 | 0 |
| 4.2 | Хэш-функци | 2 | 2 | 0 |
| 4.3 | Алгоритмы асимметричного шифрования | 8 | 8 | 0 |
| 4.4 | Инфраструктура открытого ключа | 4 | 4 | 0 |
| 5 | **Технологии туннелирования** | **44** | **16** | **28** |
| 5.1 | Протокол GRE | 3 | 1 | 2 |
| 5.2 | Протоколы канального уровня | 11 | 5 | 6 |
| 5.3 | Семейство протоколов IPSec | 14 | 6 | 8 |
| 5.4 | Совместное использование протоколов L2TP и IPSec | 12 | 2 | 10 |
| 5.5 | Протокол SSL/TLS | 4 | 2 | 2 |
| 6 | **Аутентификация и хранение учетных записей** | **16** | **4** | **12** |
| 6.1 | Протокол RADIUS | 6 | 2 | 4 |
| 6.2 | Протокол LDAP | 10 | 2 | 8 |
| 7 | **Системы обнаружения и предотвращения проникновений (IDPS)** | **14** | **8** | **6** |
| 7.1 | Основное назначение IDPS | 2 | 1 | 1 |
| 7.2 | Способы классификации IDPS | 5 | 3 | 2 |
| 7.3 | Дополнительные инструментальные средства | 3 | 2 | 1 |
| 7.4 | Выбор и развертывание IDPS | 4 | 2 | 2 |
| 8 | **Приоритезация трафика и создание альтернативных маршрутов** | **10** | **4** | **6** |
| 8.1 | Создание альтернативных маршрутов доступа в интернет | 2 | 1 | 1 |
| 8.2 | Приоритезация трафика | 3 | 1 | 2 |
| 8.3 | Ограничение (шейпинг) трафика с использованием IDP | 2 | 1 | 1 |
| 8.4 | Гарантирование полосы пропускания | 3 | 1 | 2 |

Учебная программа

повышения квалификации

**«Основы сетевой безопасности»**

**Перечень лабораторных работ**

|  |  |
| --- | --- |
| Номер темы  | Наименование лабораторной работы  |
| 1 | Основные принципы создания надежной и безопасной ИТ-инфраструктуры. Основы администрирования межсетевого экрана.Разграничение доступа между двумя локальными сетями с помощью межсетевого экрана. |
| 2 | Сегментирование сетей на канальном уровне. Сегментирование подсетей с использованием управляемых коммутаторов. Сегментирование подсетей на основе port-based VLAN. |
| 3 | Технологии межсетевых экранов.Создание политики без проверки состояния. Создание политик для традиционного (или исходящего) NAT. Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing. |
| 5.1 | Протокол GRE. |
| 5.2 | Протоколы канального уровня. Соединение двух локальных сетей протоколом L2TP, аутентификация с использованием общего секрета |
| 5.3 | Семейство протоколов IPSec. Соединение двух локальных сетей IPSec в туннельном режиме, аутентификация с использованием общего секрета. Использование аутентификации по стандарту XAuth. Использование преобразования NAT в протоколе IPSec. Использование протокола DPD в протоколе IPSec. Способы аутентификации участников и распределение ключей. |
| 5.4 | Совместное использование протоколов L2TP и IPSec, GRE и IPSec.Соединение двух локальных сетей протоколом GRE/IPSec в транспортном режиме. Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме. Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме, для одной из локальных сетей используется NAT. |
| 6 | Аутентификация и хранение учетных записей. Протокол RADIUS. Использование сервера RADIUS для хранения учетных записей. Протокол LDAP.Использование сервера LDAP/MS AD для хранения учетных записей. Аутентификация доступа к ресурсам с использованием браузера |
| 7 | Системы обнаружения и предотвращения проникновений (IDPS).Антивирусное сканирование. Обнаружение и предотвращение вторжений. |
| 8 | Приоритезация трафика и создание альтернативных маршрутов. Создание альтернативных маршрутов с использованием статической маршрутизации. Ограничение полосы пропускания трафика. Ограничение полосы пропускания P2P-трафика с использованием IDP. |

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

Курс «Основы сетевой безопасности» разработаны совместно с компанией D-Link.

Практические занятия проводятся с использованием межсетевых экранов D-Link DFL 860E, имеющих сертификат ФСТЭК.

Для проведения лабораторных работ на 1 рабочее место требуется следующее оборудование:

* 3 компьютера, один из которых подключен к dmz-интерфейсу межсетевого экрана и на котором установлен веб-сервер, два оставшихся подключены к lan-интерфейсу межсетевого экрана;
* 1 межсетевой экран DFL-860E;
* кабели Ethernet.

Дополнительно:

* 1 компьютер выступает в роли сервера, на котором установлен контроллер домена (сервер AD) и RADIUS-сервер.

**5. Учебно-методическое обеспечение программы**

**Основная учебно-методическая литература**

1. Лапонина О.Р. Курс лекций. Учебное пособие «Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия» под редакцией проф. Сухомлина В.А. 2-е издание, исправленное, изд. ООО «ИНТУИТ.ру» Интернет-Университет Информационных Технологий, 2007г. ISBN 978-5-9556-0102-1 (ИНТУИТ.РУ), ISBN 978-5-94774-650-1 (БИНОМ.ЛЗ), 531с. (33,5 усл. печ. л.), тираж 2000 экз. Рекомендовано учебно-методическим объединением в области прикладной информатики для студентов высших учебных заведений, обучающихся по специальности 510200 «Прикладная математика и информатика».
2. Лапонина О.Р. «Основы сетевой безопасности. Ч.2 Технологии туннелирования» », под редакцией проф. В.А. Сухомлина, изд. Национальный Открытый Университет «ИНТУИТ», 2014г., ISBN 978-5-9556-0163-2, 474 с. (30 усл. печ. л.), тираж 1500 экз. Допущено УМО по классическому университетскому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению ВПО 010400 «Прикладная математика и информатика» и 010300 «Фундаментальная информатика и информационные технологии».

**Дополнительная учебно-методическая литература**

1. James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback « Report on the Development of the Advanced Encryption Standard (AES)». Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Technology Administration U.S. Department of Commerce. 2000г. 116c.
2. Государственный Стандарт Российской Федерации «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» 1994г.
3. Государственный Стандарт Российской Федерации «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Функция хэширования» 1994г.
4. RFC 2251 «Lightweight Directory Access Protocol (v3)», 1997г. 50с.
5. RFC 2252 «Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions», 1997г. 32с.
6. RFC 2253 «The String Representation of LDAP Search Filters», 1997г. 8с.
7. RFC 2256 «A Summary of the X.500(96) User Schema for use with LDAPv3», 1997г. 20с.
8. RFC 2587 «Internet X.509 Public Key Infrastructure LDAPv2 Schema», 1999г. 8с.
9. RFC 3383 «Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)», 2002г. 23с.
10. RFC 2246 «The TLS Protocol Version 1.0», 1999г. 80с.
11. RFC 3546 «Transport Layer Security (TLS) Extensions», 2003г. 29с.
12. RFC 3280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», 2002г. 129с.
13. RFC 3281 «An Internet Attribute Certificate Profile for Authorization», 2002г. 40с.
14. RFC 2401 «Security Architecture for the Internet Protocol», 1998г. 66с.
15. RFC 2408 «Internet Security Association and Key Management Protocol (ISAKMP)», 1998г. 86с.
16. RFC 2409 «The Internet Key Exchange (IKE)», 1998г. 41с.
17. RFC 2412 «The OAKLEY Key Determination Protocol», 1998г. 55с.
18. RFC 3383 «Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)», 2002г. 23с.
19. RFC 2993 «Architectural Implications of NAT», 2000г. 29с.
20. RFC 2663 «IP Network Address Translator (NAT) Terminology and Considerations», 1999г. 30с.
21. RFC 3022 «Traditional IP Network Address Translator (Traditional NAT)», 2001г. 16с.
22. RFC 3069 «VLAN Aggregation for Efficient IP Address Allocation», 2001г. 7с.
23. RFC 5389 «Session Traversal Utilities for NAT (STUN)», 2008г. 51с.
24. National Institute of Standards and Technology U.S. Department of Commerce «Intrusion Detection Systems», Special Publication 800-31, 2004 г. 51 с.
25. National Institute of Standards and Technology U.S. Department of Commerce «Guide to Intrusion Detection and Prevention Systems (IDPS)», Special Publication 800-94, 2007г. 127с.

**6. Требования к результатам обучения**

Итоговая аттестация проводится в виде тестов.

**7. Составители программы**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Ф.И.О. (полностью) | Занимаемая должность | Учёная степень, звание | Контакты: |
| телефоны | e-mail |
| 1. | Лапонина Ольга Робертовна | Научный сотрудник лаб. Открытых информационных технологий | - | (495) 939-26-38 | laponina@oit.cmc.msu.ru |