Федеральное государственное бюджетное образовательное учреждение высшего образования
Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики

УТВЕРЖДАЮ
Декан факультета ВМК МГУ
_____ **/И.А.Соколов/**
«__» _____ **2023 г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля):

Технологии и принципы сетевой безопасности. Межсетевые экраны

Уровень высшего образования:

бакалавриат

Направление подготовки (специальность):

02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) ОПОП:

дисциплина относится к вариативной части программы

Форма обучения:

очная

Москва 2023

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ бакалавриата, магистратуры, реализуемых последовательно по схеме интегрированной подготовки по направлениям 02.03.02, 02.04.02 «Фундаментальная информатика и информационные технологии» в редакции приказа МГУ от 30 декабря 2016 г.

1. **Аннотация**

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, Salsa20, ChaCa20, а также режимы их использования; рассмотрены алгоритмы шифрования с открытым ключом RSA, Диффи-Хеллмана и DSS, рассмотрены принципы распределения открытых ключей, стандарт X.509 третьей версии и принципы создания инфраструктуры открытого ключа, рассмотрены наиболее широко используемые протоколы сетевой безопасности прикладного уровня и протокол создания виртуальных частных сетей.

2. **УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ**

Подготовка научно-педагогических кадров в бакалавриате.

3. **НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ**

Направление 02.03.02 «Фундаментальная информатика и информационные технологии».

4. **МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Дисциплина входит в обязательную часть образовательной программы бакалавриата.

5. **ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ**

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	**Планируемые результаты обучения**
Способность разрабатывать и применять основные стандарты, механизмы и сервисы обеспечения безопасности информационных технологий (СПК-3).	З1 (СПК-3) 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. У1 (СПК-3) Уметь Настраивать разграничение доступа на канальном уровне с использованием технологии VLAN и на сетевом уровне с использованием межсетевых экранов; использовать различные механизмы и сервисы обеспечения безопасности в протоколах туннелирования GRE, IPSec. В1 (СПК-3) Владеть Методологией создания политики безопасности.

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетные единицы, всего 108 часов, из них 54 часа составляет контактная работа с преподавателем – 36 часов занятий лекционного типа, 18 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.) и 54 часа составляет самостоятельная работа учащегося.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по алгоритмам, языкам программирования, архитектуре ЭВМ, операционным системам, системам программирования, сетевым технологиям в объеме, соответствующем основным образовательным программам бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Вид занятия	Форма проведения занятий	Цель
1	Лекции в электронном виде на сайте факультета	Изучение теоретического материала	Получение теоретических знаний по дисциплине.
2	Промежуточное тестирование	Использование системы электронного обучения со случайным выбором тестов, контролем времени прохождения теста, ограничением количества попыток и автоматической проверкой тестов	Повышение степени понимания теоретического материала.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и краткое содержание разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Всего (часы)**	В том числе			
		Контактная работа (работа во взаимодействии с преподавателем) Виды контактной работы, часы			**Самостоятельная работа обучающегося, часы**
		Лекции	**Семинары**	**Всего**	
Тема 1. Введение. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация сетевых атак; цели и задачи обеспечения безопасности: доступность, целост-	**6**	2	1	3	**3**

ность, конфиденциальность, ответственность, гарантирование; модели сетевой безопасности и безопасности информационной системы.					
Тема 2. Межсетевые экраны. Классификация межсетевых экранов. Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT. Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана. **Лабораторные работы.** **1. Сегментирование сетей на канальном уровне.** Создание подсетей с использованием технологии VLAN. **2. 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.	**6**	2	1	3	**3**
Тема 3. Алгоритмы симметричного шифрования. Основные понятия алгоритмов симметричного шифрования, ключ шифрования, plaintext, ciphertext; стойкость алгоритма, типы операций, сеть Фейштеля; алгоритмы DES и тройной DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147. Стандарт алгоритмов симметричного шифрования – AES; критерии выбора алгоритма и сравнительная характеристика пяти финалистов. Характеристики алгоритмов, особенности программной реализации, возможность их реализации в окружениях с ограничениями пространства, возможность вычисления на лету подключей. Алгоритм Rijndael; математические понятия, лежащие в основе алгоритма Rijndael; структура раунда алгоритма Rijndael. Алгоритмы поточного шифрования Salsa20 и ChaCha20. Режимы выполнения блочных алгоритмов; способы создания псевдослучайных чисел.	**16**	8	4	12	**4**
Тема 4. Криптография с открытым ключом. Основные понятия криптографии с открытым ключом, способы ее использования: шифрование, создание и проверка цифровой подписи, обмен ключа. Алгоритмы RSA и Диффи-Хеллмана.	**10**	4	2	6	**4**
Тема 5. Хэш-функции и аутентификация сообщений. Основные понятия обеспечения целостности сообщений с помощью MAC и хэш-функций; простые хэш-функции. Сильные хэш-функции MD5, SHA-1, SHA-2, SHA-3 и ГОСТ 3411; обеспечение целостности сообщений и вычисление MAC с помощью алгоритмов симметричного шифрования, хэш-функций и стандарты HMAC и AEAD.	**10**	4	2	6	**4**
Тема 6. Цифровая подпись. Требования к цифровым подписям, стандарты цифровой подписи ГОСТ 3410 и DSS.	**6**	2	1	3	**3**
Тема 7. Криптография с использованием эллиптических кривых. Математические понятия, связанные с криптографией на эллиптических кривых.	**6**	2	1	3	**3**

Тема 8. Алгоритмы обмена ключей и протоколы аутентификации. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Аутентификационный сервис Kerberos; требования, которым должен удовлетворять Kerberos, протокол Kerberos, функции AS и TGS, структура билета (ticket) и аутентификатора; понятие области (realm) Kerberos; протокол 5 версии.	**6**	2	1	3	**3**
Тема 9. Инфраструктура Открытого Ключа. Понятия инфраструктуры открытого ключа: сертификат открытого ключа, сертификационный центр, конечный участник, регистрационный центр, CRL, политика сертификата, регламент сертификационной практики, проверяющая сторона, репозиторий; архитектура PKI. Профиль сертификата X.509 v3 и профиль CRL v2; сертификационный путь; основные поля сертификата и расширения сертификата; критичные и некритичные расширения; стандартные расширения. Профиль CRL v2 и расширения CRL, области CRL, полный CRL, дельта CRL; Алгоритм проверки действительности сертификационного пути. Протоколы PKI управления сертификатом. On-line протокол определения статуса сертификата; политика сертификата и регламент сертификационной практики. Сервис директории LDAP, сравнение LDAP с реляционными базами данных; информационная модель LDAP, модель именования LDAP, понятие дерева директории, DN, схемы, записи, атрибута записи, класса объекта. Основные свойства протокола LDAP. Abstract Syntax Notation One (ASN.1); простые и структурные типы; идентификатора объекта.	**10**	4	2	6	**4**
Тема 10. Протокол TLS/SSL. Протокол Записи и протокол Рукопожатия, понятие "состояние соединения". Полное и сокращенное Рукопожатие. Выработка общего секрета и создание из него ключевого материала с помощью псевдослучайной функции (PRF). Расширения, используемые для добавления функциональностей в протокол TLS.	**6**	2	1	3	**3**
Тема 11. Семейство протоколов IPSec. Возможные способы реализации IPSec. Степень детализации управления трафиком. Протоколы ESP и AH. Политика безопасности. Способы аутентификации участников и распределение ключей. **Лабораторные работы.** **1. Протоколы сетевого уровня.** Протокол GRE. **2. 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.	**10**	4	2	6	**4**

Соединение двух локальных сетей протоколом GRE/IPSec в транспортном режиме.					
Промежуточная аттестация – *тестирование с использованием средств электронной проверки результатов*	**16**				**16**
Итого	**108**	**36**	**18**	**54**	**54**

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к практическим заданиям текущего контроля и промежуточной аттестации.

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

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 Administration U.S. Department of Commerce. 2000г. 116с.
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.

Ресурсы информационно-телекоммуникационной сети «Интернет»

1. https://ietf.org

Информационные технологии, используемые в процессе обучения

№ п/п	Вид занятия	Форма проведения занятий	Цель
1	Лекции в электронном виде на сайте факультета	Изучение теоретического материала	Получение теоретических знаний по дисциплине.
2	Лабораторные работы	Развертывание и настройка протоколов туннелирования на маршрутизаторах D-Link DFL 860E (имеют сертификат ФСТЭК)	Повышение степени понимания теоретического материала

Материально-техническая база: Необходимое оборудование: D-Link DFL 860E (имеют сертификат ФСТЭК).

12. ЯЗЫК ПРЕПОДАВАНИЯ: Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ: Научный сотрудник Лапонина Ольга Робертовна (laponina@oit.cmc.msu.ru)

Приложение

Оценочные средства для промежуточной аттестации по дисциплине
«Технологии и принципы сетевой безопасности. Межсетевые экраны»

Промежуточная аттестация состоит из двух этапов – выполнения тестовых заданий, проверяющих приобретенные учащимся умения и навыки, и индивидуального собеседования, проверяющего приобретенные знания.

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ	**КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ из соответствующих карт компетенций**					**ОЦЕНОЧНЫЕ СРЕДСТВА**
	1	2	3	4	5	
	Неудовлетворительно	**Неудовлетворительно**	**Удовлетворительно**	**Хорошо**	**Отлично**	
З1 (СПК-3) 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.	Отсутствие знаний	Фрагментарные представления о понятиях и определениях, относящихся к информационной безопасности, основных алгоритмах симметричного и асимметричного шифрования, криптографических хэш-функциях и способах аутентификации сообщений, основных понятиях Инфраструктуры Открытого Ключа.	В целом сформированные, но неполные знания о понятиях и определениях, относящихся к информационной безопасности, основных алгоритмах симметричного и асимметричного шифрования, криптографических хэш-функциях и способах аутентификации сообщений, основных понятиях Инфраструктуры Открытого Ключа.	Сформированные, но содержащие отдельные пробелы знания о понятиях и определениях, относящихся к информационной безопасности, основных алгоритмах симметричного и асимметричного шифрования, криптографических хэш-функциях и способах аутентификации сообщений, основных понятиях Инфраструктуры Открытого Ключа.	Сформированные систематические знания о понятиях и определениях, относящихся к информационной безопасности, основных алгоритмах симметричного и асимметричного шифрования, криптографических хэш-функциях и способах аутентификации сообщений, основных понятиях Инфраструктуры Открытого Ключа.	Индивидуальное собеседование
У1 (СПК-3)	Отсутствие	Фрагментарные	В целом сформиро-	Сформированное, но	Сформированное	***Практиче-***

Уметь ***использовать различные механизмы и сервисы обеспечения безопасности в протоколах туннелирования.***	умений	умения ***в области использования различные механизмы и сервисы обеспечения безопасности в протоколах туннелирования.***	ванное, но не систематическое умение ***в области использования различные механизмы и сервисы обеспечения безопасности в протоколах туннелирования.***	содержащее отдельные пробелы умение ***в области использования различные механизмы и сервисы обеспечения безопасности в протоколах туннелирования.***	систематическое умение ***в области использования различные механизмы и сервисы обеспечения безопасности в протоколах туннелирования.***	***ское контрольное задание***
В1 (СПК-3) владеть методологией создания политики безопасности.	Отсутствие навыков	Фрагментарное владение методологией создания политики безопасности.	В целом сформированное, но не систематическое владение методологией создания политики безопасности.	Сформированное, но содержащее отдельные пробелы владение методологией создания политики безопасности.	Сформированное систематическое владение методологией создания политики безопасности.	Практическое контрольное задание

Фонды оценочных средств

Список вопросов для индивидуального собеседования на промежуточной аттестации.

1. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, классификация сетевых атак.
2. Классификация межсетевых экранов. Пакетные фильтры с поддержкой и без поддержки состояния. Межсетевые экраны прикладного уровня.
3. Политики межсетевого экрана. Межсетевые экраны с возможностями NAT.
4. Понятие DMZ. Различные топологии DMZ сетей с использованием межсетевых экранов разного типа.
5. Основные сервисы и криптографические механизмы безопасности.
6. Алгоритмы симметричного шифрования. Понятие стойкости алгоритма, области применения, типы операций, используемых в алгоритмах симметричного шифрования.
7. Сеть Фейстеля, SP-сеть.
8. Алгоритмы DES и тройной DES.
9. Алгоритмы симметричного шифрования Blowfish, ГОСТ 28147.
10. Алгоритм Rijndael. Математические понятия, лежащие в основе алгоритма Rijndael. Структура алгоритма Rijndael.
11. Алгоритм ГОСТ 34.12-2015 «Кузнечик».

12. Поточные алгоритмы шифрования. Алгоритмы Salsa20 и ChaCha20.
13. Режимы выполнения алгоритмов симметричного шифрования.
14. Способы создания псевдослучайных чисел.
15. Требования к криптографическим хеш-функциям.
16. Структура Меркла — Дамгора. Хеш-функции MD5, SHA-1, SHA-2 и ГОСТ 3411.
17. Хеш-функция SHA-3.
18. Коды аутентификации сообщений.
19. Основные понятия, относящиеся к криптографии с открытым ключом, способы использования алгоритмов с открытым ключом: шифрование, создание и проверка цифровой подписи, обмен ключа.
20. Алгоритм RSA.
21. Алгоритм Диффи-Хеллмана.
22. Основные требования к цифровым подписям, стандарты цифровой подписи ГОСТ 3410 и DSS.
23. Криптография с использованием эллиптических кривых.
24. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны.
25. Аутентификация и обмен ключей в протоколе Kerberos.
26. Инфраструктура открытого ключа. Сертификаты X.509 v3.
27. Инфраструктура открытого ключа. Репозиторий сертификатов. Способы отмены сертификатов.
28. Аутентификация и обмен ключей в протоколе TLS.
29. Семейство протоколов IPSec. Основные топологии. Протоколы AH и ESP. Базы данных SPD и SAD. Аутентификация сторон и обмен ключа в протоколе IKE.

Методические материалы для проведения процедур оценивания результатов обучения

Практическое контрольное задание для промежуточной аттестации является довольно объемным, поэтому частично выполняется в качестве четвертого задания для текущего контроля успеваемости. Выполнение каждого практического задания текущего контроля успеваемости может принести максимум 25 баллов, в итоге по результатам работы в семестре учащийся может набрать максимум 100 баллов. На промежуточной аттестации можно также набрать 100 баллов – 60 баллов максимум по итогам индивидуального собеседования и 40 баллов максимум за выполнение практического контрольного задания. Итоговая сумма, не меньшая 170, соответствует оценке «отлично», от 135 до 169 – оценке «хорошо», от 90 до 134 – оценке «удовлетворительно», меньшая 90 – оценке «неудовлетворительно».