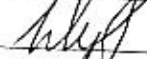


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

РЕКОМЕНДОВАНО К
УТВЕРЖДЕНИЮ

Декан, председатель совета

Факультета КТВТиЭ


 Ш.А.Юсуфов

16 10 2018

УТВЕРЖДАЮ

Проректор по учебной работе,
председатель методического

совета ДГТУ

 Н.С. Суракатов

18 10 2018

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина С1.Б.34 Информационная безопасность открытых систем

Специальность 10.05.03-«Информационная безопасность автоматизированных систем»

Специализация «Безопасность открытых информационных систем»

Факультет «Компьютерных технологий, вычислительной техники и энергетики»
наименование факультета, в котором ведется дисциплина

Кафедра Информационная безопасность
наименование кафедры, в которой ведется дисциплина

Квалификация выпускника (степень) Специалист по защите информации
связать с специальностью

Форма обучения очная; курс 4; семестр(ы) 7;

Всего трудоемкость в зачетных единицах (часах) 4 ЗЕТ(144);


Лекции 34 (час); Экзамен 7 (13Г-36 ЧАСОВ);

Практические (семинарские) занятия - (час); Зачет - (семестр);

Лабораторные занятия 34 (час); Курсовая работа - (семестр);

Самостоятельная работа 40 (час).

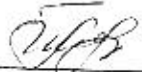
Зав. кафедрой ИБ  Г.Н. Качаева

Начальник УО  Д.В. Магомаева



Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Программа одобрена на заседании выпускающей кафедры ИБ протокол № 2 от 15.10.2018г.

Зав. выпускающей кафедрой по данному направлению  Г.И. Качаева

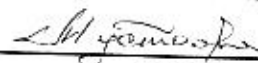
ОДОБРЕНО

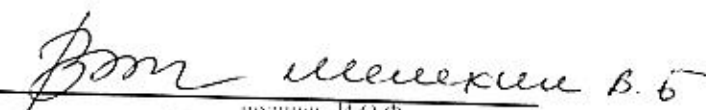
Методической комиссией по
укрупненным группам
специальностей и направлению
подготовки
10.00.00 Информационная безопасность.

Председатель МК

АВТОР ПРОГРАММЫ

М.Г. Мирзажанов, ст. преп.
И.О.Ф. и/или другие личные данные


подпись

 В.Б. Мамедов
подпись, И.О.Ф.
15.10 2018

1. Цели освоения дисциплины

Дисциплина «Информационная безопасность открытых систем» имеет целью ознакомление слушателей существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.

Задача дисциплины «Информационная безопасность открытых систем» – получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.

2. Место дисциплины в структуре ООП специалиста

Дисциплина «Информационная безопасность открытых систем» относится к дисциплинам базовой части учебного плана. Изучение её базируется на следующих дисциплинах: «Математическая логика и теория алгоритмов», «Методы программирования», «Дискретная математика».

Дисциплина «Информационная безопасность открытых систем» обеспечивает изучение следующих дисциплин: «Основы проектирования защищенных компьютерных сетей», «Защита в операционных системах». Знания и практические навыки, полученные из дисциплины «Информационная безопасность открытых систем», используются студентами при разработке дипломных работ.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Информационная безопасность открытых систем»

Изучение дисциплины «Информационная безопасность открытых систем» обеспечивает овладение следующими компетенциями:

- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
- способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);
- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);
- способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);
- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

В результате изучения дисциплины «Криптографические протоколы» студенты должны:

знать:

подходы к интеграции сетей в открытых информационных системах; принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах; основные методы и средства реализации удаленных сетевых атак на открытые информационные системы; о политиках безопасности и мерах защиты в открытых информационных системах; о комплексном подходе к построению эшелонированной защиты для открытых информационных систем систем;

уметь:

проектировать защищенные открытые информационные системы; определять и устранять основные угрозы информационной безопасности для открытых информационных систем; строить модель нарушителя информационной безопасности для открытых информационных систем; выявлять и устранять уязвимости в основных компонентах открытых информационных систем; применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество; используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для открытых информационных систем;

владеть:

терминологией и системным подходом построения защищенных открытых информационных систем; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем виртуальных сетей.

4. Структура и содержание дисциплины (модуля) «Информационная безопасность открытых систем»

Общая трудоемкость дисциплины составляет 4 зачетных единиц – 144 часов, в том числе: лекционных - 34 часа, лабораторных - 34 часа, СРС - 40 часов, форма отчетности экзамен в 7 семестре.

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля (по срокам текущей аттестации)
				ЛК	ПЗ	ЛР	СРС	
1	2	3	4	5	6	7	8	9
1.	<u>Лекция 1. Тема. Основные понятия.</u> Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Понятие криптографического протокола. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов.	7	1	2		2	2	Вх. Контр.
2.	<u>Лекция 2. Тема. Уязвимости и атаки на криптографический протокол.</u> Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов.		2	2		2	4	
3.	<u>Лекция 3. Тема Схемы цифровой подписи</u> Схемы цифровой подписи. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Схемы Эль-Гамала, Фиата-Фейга-Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамала.		3	2		2	4	
4.	<u>Лекция 4. Тема Схемы цифровой подписи</u> Стандарты США и России электронной цифровой подписи. Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки.		4	2		2	2	
5.	<u>Лекция 5. Тема: Протоколы идентификации</u> Протоколы идентификации на основе паролей, протоколы "рукопожатия" и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования. Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым		5	2		2	2	

	разглашением.						
6.	Лекция 6. Тема: Протоколы идентификации Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото. Связь между протоколами цифровой подписи и протоколами идентификации. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.	6	2		2	2	
7.	Лекция 7. Тема: Инфраструктура открытых ключей Управление открытыми ключами. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509.	7	2		2	4	
8.	Лекция 8.Тема: Инфраструктура открытых ключей Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа.	8	2		2	2	
9.	Лекция 9. Тема: Протоколы распределения ключей Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрестем. Двух и трех сторонние протоколы передачи и распределения ключей.	9	2		2	2	
10.	Лекция 10. Тема: Протоколы распределения ключей Функции доверенной третьей стороны и выполняемые ею роли. Схемы предварительного распределения ключей.	10	2		2	2	АКР №2
11.	Лекция 11. Тема: Протоколы распределения ключей Неравенство Блома. Схемы предварительного распределения ключей Блома и на основе пересечений множеств. Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине».	11	2		2	2	
12.	Лекция 12. Тема: Протоколы распределения ключей Аутентифицированные протоколы открытого распределения ключей. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.	12	2		2	2	
13.	Лекция 13. Тема: Прикладные протоколы	13	2		2	2	

	Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации.						
14.	Лекция 14. Тема: Прикладные протоколы Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации.	14	2		2	2	
15.	Лекция 15. Тема: Протоколы открытых сделок Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и "игры в покер" по телефону. Забывающая передача информации. Протокол подписания контракта.	15	2		2	2	АКР №3
16.	Лекция 16. Тема: Протоколы открытых сделок Протокол сертифицированной электронной почты. Протоколы электронного голосования. Свойства неотслеживаемости и несвязываемости. Протоколы электронных платежей и цифровых денег.	16	2		2	2	
17.	Лекция 17. Тема: Заключение Обзор государственных стандартов и стандартов организаций в области криптографических протоколов. Проблемы автоматизации анализа криптографических протоколов. Итоги изучения дисциплины.	17	2		2	2	
	Итого		34		34	40	Экзамен 1 ЗЕТ = 36 часов

4.2. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	№ литер. источника из списка литературы	Кол-во часов
1.	Лк№1	Основные понятия, термины и определения криптологии. Криптография и криптоанализ шифра Цезаря. Требования к шифрам. Ключевые системы.	№ 1-17	2
2.	Лк№ 2	Криптографические хэш-функции. Электронная цифровая подпись. Криптографические протоколы.	№ 1-17	2
3.	Лк№ 3	Поточные шифры. Барабанные машины. Шифр и табло Виженера.	№ 1-17	2
4.	Лк№ 4	Поточные шифры. Барабанные машины. Шифр и табло Виженера.	№ 1-17	2
5.	Лк№ 5	Шифрование, дешифрование, криптоанализ.	№ 1-17	2
6.	Лк№ 6	Шифрование, дешифрование, криптоанализ.	№ 1-17	2

7.	Лк№ 7	Шифр Вернама. Шифрование, дешифрование, криптоанализ.	№ 1-17	2
8.	Лк№ 8	Шифр Вернама. Шифрование, дешифрование, криптоанализ.	№ 1-17	2
9.	Лк№ 9	ГОСТы. Нормативно-правовая база криптографии. DES. Тройной DES.	№ 1-17	2
10.	Лк№ 10	ГОСТы. Нормативно-правовая база криптографии. DES. Тройной DES.	№ 1-17	2
11.	Лк№ 11	Дифференциальный и линейный криптоанализ блочных шифров.	№ 1-17	2
12.	Лк№ 12	Дифференциальный и линейный криптоанализ блочных шифров.	№ 1-17	2
13.	Лк№ 13	Криптосистемы с открытым ключом. Алгоритм RSA.	№ 1-17	2
14.	Лк№ 14	Криптосистемы с открытым ключом. Алгоритм RSA.	№ 1-17	2
15.	Лк№ 15	Управление ключами. Система Диффи-Хеллмана.	№ 1-17	2
16.	Лк№ 16	Управление ключами. Система Диффи-Хеллмана.	№ 1-17	2
17.	Лк№ 17	Схема шифрования El-Gamal. Схема Kerberos.	№ 1-17	2
Итого				34

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов по содержанию дисциплины	Рекомендуемая литература и источники информации	Форма контроля СРС
1.	Основные понятия. Примеры протоколов на основе симметричных и асимметричных криптографических систем.	2	№ 1-17	Опрос, реферат, статья
2.	Уязвимости и атаки на криптографический протокол.	4	№ 1-17	Опрос, реферат, статья
3.	Схемы цифровой подписи. Примеры схем цифровых подписей. Цифровые подписи DSA и ГОСТ.	4	№ 1-17	Опрос, реферат, статья
4.	Схемы цифровой подписи. Примеры схем цифровых подписей. Цифровые подписи DSA и ГОСТ.	2	№ 1-17	Опрос, реферат, статья
5.	Протоколы идентификации. Протоколы «рукопожатия» и идентификации типа «запрос-ответ». Протоколы доказательства знания с нулевым разглашением.	2	№ 1-17	Опрос, реферат, статья
6.	Протоколы идентификации. Протоколы «рукопожатия» и идентификации типа «запрос-ответ». Протоколы доказательства знания с нулевым разглашением.	2	№ 1-17	Опрос, реферат, статья
7.	Инфраструктура открытых ключей. Протоколы идентификации на основе самосертифицируемых ключей. Сертификаты	4	№ 1-17	Опрос, реферат, статья

	инфраструктуры открытых ключей и их структура. Функции удостоверяющего центра.			
8.	Инфраструктура открытых ключей. Протоколы идентификации на основе самосертифицируемых ключей. Сертификаты инфраструктуры открытых ключей и их структура. Функции удостоверяющего центра.	2	№ 1-17	Опрос, реферат, статья
9.	Протоколы распределения ключей. Порядок проверки сертификатов для различных архитектур инфраструктуры открытых ключей. Протоколы генерации и передачи ключей для симметричных шифрсистем.	2	№ 1-17	Опрос, реферат, статья
10.	Протоколы распределения ключей. Порядок проверки сертификатов для различных архитектур инфраструктуры открытых ключей. Протоколы генерации и передачи ключей для симметричных шифрсистем.	2	№ 1-17	Опрос, реферат, статья
11.	Протоколы распределения ключей. Протоколы генерации и передачи ключей для асимметричных шифрсистем. Схема предварительного распределения ключей Блома и ее устойчивость к компрометации ключей.	2	№ 1-17	Опрос, реферат, статья
12.	Протоколы распределения ключей. Протоколы генерации и передачи ключей для асимметричных шифрсистем. Схема предварительного распределения ключей Блома и ее устойчивость к компрометации ключей.	2	№ 1-17	Опрос, реферат, статья
13.	Прикладные протоколы. Схемы предварительного распределения ключей на основе пересечения множеств. Протокол Kerberos.	2	№ 1-17	Опрос, реферат, статья
14.	Прикладные протоколы. Схемы предварительного распределения ключей на основе пересечения множеств. Протокол Kerberos.	2	№ 1-17	Опрос, реферат, статья
15.	Протоколы открытого распределения ключей и их уязвимости. Протоколы семейства KryptoKnight для различных сетевых конфигураций и условий применения. Протоколы семейства IPsec.	2	№ 1-17	Опрос, реферат, статья
16.	Протоколы открытого распределения ключей и их уязвимости. Протоколы семейства KryptoKnight для различных сетевых конфигураций и условий применения. Протоколы семейства IPsec.	2	№ 1-17	Опрос, реферат, статья
17.	Заключение. Примеры прикладных протоколов (протоколы заключения сделок, платежных систем, сертифицированная электронная почта, голосования и др.).	2	№ 1-17	Опрос, реферат, статья
Итого		40		

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

При проведении занятий по учебной дисциплине рекомендуется следовать и традиционным технологиям, в частности, в каждом разделе курса выделять наиболее важные моменты, акцентировать на них внимание обучаемых.

При чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволит сделать изложение наглядным и продемонстрировать обучаемым приемы программирования.

При изучении всех разделов программы добиться точного знания обучаемыми основных исходных понятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Вопросы входного контроля для проверки знаний студентов

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).

Аттестационная контрольная работа №1

1. Понятие криптографического протокола.
2. Роль криптографических протоколов в системах защиты информации.
3. Понятие криптографического протокола.
4. Свойства протоколов, характеризующие их безопасность.
5. Основные виды уязвимостей. Подходы к классификации криптографических протоколов.
6. Подходы к моделированию криптографических протоколов.
7. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры.
8. Основные подходы к автоматизации анализа протоколов.
9. Схемы цифровой подписи.
10. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем.
11. Схемы Эль-Гамала, Фиата-Фейга-Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамала.
12. Стандарты США и России электронной цифровой подписи.
13. Одноуровневые подписи.
14. Схемы конфиденциальной цифровой подписи и подписи вслепую.
15. Подписи с обнаружением подделки.

16. Протоколы идентификации на основе паролей, протоколы "рукопожатия" и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования.
17. Понятие протоколов интерактивного доказательства и доказательства знания.
18. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.

Аттестационная контрольная работа №2

19. Протоколы Фиата-Шамира, Шаума, Шпорра и Окамото.
20. Связь между протоколами цифровой подписи и протоколами идентификации.
21. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.
22. Управление открытыми ключами.
23. Основы организации и основные компоненты инфраструктуры открытых ключей.
24. Сертификат открытого ключа.
25. Стандарт X.509.
26. Сервисы инфраструктуры открытых ключей.
27. Удостоверяющий центр, Центр регистрации.
28. Репозиторий.
29. Архив сертификатов. Конечные субъекты.
30. Архитектуры инфраструктуры открытых ключей.
31. Проверка и отзыв сертификата открытого ключа.
32. Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.
33. Двух и трех сторонние протоколы передачи и распределения ключей.
34. Функции доверенной третьей стороны и выполняемые ею роли.
35. Схемы предварительного распределения ключей.

Аттестационная контрольная работа №3

36. Неравенство Блома.
37. Схемы предварительного распределения ключей Блома и на основе пересечений множеств.
38. Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине».
39. Аутентифицированные протоколы открытого распределения ключей.
40. Групповые протоколы.
41. Протоколы разделения секрета и распределения ключей для телеконференции.
42. Особенности построения семейства протоколов IPsec.
43. Протоколы Oakley, ISAKMP, IKE.
44. Протоколы SKIP, SSL/TLS и особенности их реализации.
45. Особенности построения семейства протоколов IPsec.
46. Протоколы Oakley, ISAKMP, IKE.
47. Протоколы SKIP, SSL/TLS и особенности их реализации.
48. Протоколы битовых обязательств и их свойства.
49. Протоколы подбрасывания монеты и "игры в покер" по телефону.
50. Забывающая передача информации.
51. Протокол подписания контракта.

Перечень экзаменационных вопросов

1. Понятие криптографического протокола.
2. Роль криптографических протоколов в системах защиты информации.
3. Понятие криптографического протокола.
4. Свойства протоколов, характеризующие их безопасность.
5. Основные виды уязвимостей. Подходы к классификации криптографических протоколов.
6. Подходы к моделированию криптографических протоколов.
7. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры.
8. Основные подходы к автоматизации анализа протоколов.
9. Схемы цифровой подписи.
10. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем.
11. Схемы Эль-Гамала, Фиата-Фейга-Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамала.
12. Стандарты США и России электронной цифровой подписи.
13. Однообразные подписи.
14. Схемы конфиденциальной цифровой подписи и подписи вслепую.
15. Подписи с обнаружением подделки.
16. Протоколы идентификации на основе паролей, протоколы "рукопожатия" и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования.
17. Понятие протоколов интерактивного доказательства и доказательства знания.
18. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.
19. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото.
20. Связь между протоколами цифровой подписи и протоколами идентификации.
21. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.
22. Управление открытыми ключами.
23. Основы организации и основные компоненты инфраструктуры открытых ключей.
24. Сертификат открытого ключа.
25. Стандарт X.509.
26. Сервисы инфраструктуры открытых ключей.
27. Удостоверяющий центр. Центр регистрации.
28. Репозиторий.
29. Архив сертификатов. Конечные субъекты.
30. Архитектуры инфраструктуры открытых ключей.
31. Проверка и отзыв сертификата открытого ключа.
32. Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.
33. Двух и трех сторонние протоколы передачи и распределения ключей.
34. Функции доверенной третьей стороны и выполняемые ею роли.
35. Схемы предварительного распределения ключей.
36. Неравенство Блома.
37. Схемы предварительного распределения ключей Блома и на основе пересечений множеств.

38. Протокол открытого распределения ключей Диффи-Хеллмана и способы его защиты от атаки «противник в середине».
39. Аутентифицированные протоколы открытого распределения ключей.
40. Групповые протоколы.
41. Протоколы разделения секрета и распределения ключей для телеконференции.
42. Особенности построения семейства протоколов IPsec.
43. Протоколы Oakley, ISAKMP, IKE.
44. Протоколы SKIP, SSL/TLS и особенности их реализации.
45. Особенности построения семейства протоколов IPsec.
46. Протоколы Oakley, ISAKMP, IKE.
47. Протоколы SKIP, SSL/TLS и особенности их реализации.
48. Протоколы битовых обязательств и их свойства.
49. Протоколы подбрасывания монеты и "игры в покер" по телефону.
50. Забывающая передача информации.
51. Протокол подписания контракта.
52. Протокол сертифицированной электронной почты.
53. Протоколы электронного голосования.
54. Свойства неотслеживаемости и несвязываемости.
55. Протоколы электронных платежей и цифровых денег.
56. Обзор государственных стандартов и стандартов организаций в области криптографических протоколов.
57. Проблемы автоматизации анализа криптографических протоколов.
58. Итоги изучения дисциплины.

Вопросы проверки остаточных знаний

8. Предмет, цель и задачи криптографии.
9. История криптографии.
10. Краткие сведения о криптоанализе.
11. Простейшие шифры и их свойства.
12. Системы шифрования с открытыми ключами.
13. Виртуальные частные сети.
14. Электронные цифровые подписи (электронные подписи).
15. Основные подходы к реализации PKI.
16. Компоненты и сервисы инфраструктуры открытых ключей.
17. Архитектура и топология PKI.
18. Стандарты в области PKI 50.
19. Стандарты Internet X.509 PKI (PKIX).
20. Сертификаты открытых ключей X.509.
21. Списки аннулированных сертификатов. Атрибутные сертификаты.
22. Основные требования к политике PKI.
23. Политика применения сертификатов и регламент.
24. Краткая характеристика политики PKI.
25. Набор положений политики PKI.
26. Проблемы формирования политики PKI.
27. Симметричные криптосистемы.
28. Основы теории К. Шеннона.
29. Симметричные методы шифрования.
30. Алгоритмы блочного шифрования.
31. Асимметричные системы шифрования.
32. Применение асимметричных алгоритмов.
33. Хранилище сертификатов ОС MS Windows.

7. Учебно-методическое и информационное обеспечение дисциплины
 «Информационная безопасность открытых систем»
 7.1. Рекомендуемая литература и источники информации
 (основная и дополнительная)

Зав. библиотекой



№	Виды занятий (лек, пр, лаб, сре, прсе)	Комплект необходимой учебной литературы по дисциплинам (наименование учебника, учебного пособия, конспект лекций, учебно-методической литературы)	Автор	Издат. и год издания	Кол-во пособий, учебников и прочей литературы	
					в биб.по теке	на кафедре
1.	ЛК,СР, КР	Информационная безопасность и защита информации. Учебное пособие для ВУЗов.	Мельников В.П., Клейменов С.А., Петраков А.М.	М.: Академия, 2007г.-336с., ил. ISBN 978-5-7695-4884-0	47	
2.	ЛК,СР, КР	Инженерно-техническая защита информации [Электронный ресурс]	Рагозин Ю. Н.	СПб.: Интермедия, 2018 -- 168 с. -- 978-5-4383-0161-5.	http://www.iprbookshp.ru/73641.html	
3.	ЛК,СР, КР	Организационная защита информации [Электронный ресурс]	Аверченков В. И.	Брянск: Брянский государственный технический университет, 2012. - 184 с. 978-89838-489-0	http://www.iprbookshp.ru/7002.html	
4.	ЛК,СР, КР	Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: учебное пособие	Бескид П. П.	СПб.: Российский государственный гидрометеорологический университет, 2010. -- 95 с. 2227-8397	http://www.iprbookshp.ru/17925.html	
5.	ЛК,СР, КР	Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие	Бескид П. П.	СПб.: Российский государственный гидрометеорологический университет, 2010. -- 104 с. -- 2227-8397	http://www.iprbookshp.ru/17926.html	
6.	ЛК,СР, КР	Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие	Кремоналов В. В.	М.: Евразийский открытый институт, 2011. -- 278 с. -- 978-5-374-00507-3.	http://www.iprbookshp.ru/10871.html	
7.	ЛК,СР, КР	Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие	Башлы П. П.	М.: Евразийский открытый институт, 2012. -- 311 с. -- 978-5-374-00301-7.	http://www.iprbookshp.ru/10677.html	
8.	ЛК,СР, КР	Методы и средства криптографической защиты информации [Электронный ресурс]:	Алексеев В. А.	Липецк: Липецкий государственный технический университет. ЭБС АСВ, 2009. -- 16 с. - 2227-8397.		

<i>Дополнительная литература</i>						
9.	ЛК,СР, КР	Комплексная защита информации в компьютерных системах. Учебное пособие	Завороцкий В.П.	М.: Догос. Пбюол П.А.Егоров, 2001-264с.,		http://www.iprbookshop.ru/16510.html
10.	ЛК,СР, КР	Методы и средства защиты информации в компьютерных системах. Учебное пособие для ВУЗов.3-е издание	Хорев П.Б.	М.: Академия, 2007-256.: ил.-(выш.проф. образ.) ISBN 978-5-7695-4157-5		http://www.iprbookshop.ru/1723.html
11.	ЛК,СР, КР	Организационное обеспечение информационной безопасности. Учебник для ВУЗов.	Романов О.А., Бабин С.А., Жданов С.Г.	М.: Академия, 2008-190с. ISBN 978-5-7695-4272-5		http://www.iprbookshop.ru/17760.html
12.	ЛК,СР, КР	Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. Учебное пособие для ВУЗов	Белкин П.Б., Михальский О.О., Пернаков А.С. и др.	М.: Радио и связь, 1999.-168с.		http://www.iprbookshop.ru/17380.html
13.	ЛК,СР, КР	Основы криптографии. Учебное пособие – 2-е издание.		М.: Гелиос АРВ, 2002.-480с., ил.		http://www.iprbookshop.ru/17729.html
14.	ЛК,СР, КР	Криптография: скоростные шифры	Молдован А.А. и др.	СПб., БХВ-Петербург, 2002.-496с.		http://www.iprbookshop.ru/17010.html
<i>Интернет - источники</i>						
15.	ЛК,СР, КР	http://dsu.ru/nauka/biblioteka – образовательный портал университета				
16.	ЛК,СР, КР	http://www.elibrary.ru – научная электронная библиотека				
17.	ЛК,СР, КР	http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.				

8. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий и лабораторного практикума на основе интерактивных методов обучения необходим доступ в Интернет из компьютерного зала, наличие цифрового проектора для применения современных обучающих мультимедиа-технологий.

Программное обеспечение:

- операционная система Microsoft Windows;
- текстовый процессор Microsoft Word;
- web-браузер;
- среда программирования.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем».

Рецензент от выпускающей кафедры по специальности 10.05.03- «Информационная безопасность автоматизированных систем


подпись


Ф.И.О.

