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

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ
Декан, председатель совета
Факультета КТВТиЭ
_____ Ш.А.Юсуфов
17 10 2018

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического
совета ДГТУ
_____ Н.С. Суракатов
22 10 2018

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина Б1.В.ДВ.3 Криптографические протоколы

Направление 10.03.01 – Информационная безопасность

Профиль Безопасность автоматизированных систем

Факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина

Кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) бакалавр

Форма обучения очная ; курс 2 ; семестр(ы) 4;

Всего трудоемкость в зачетных единицах (часах) 5 ЗЕТ(180);

Лекции 17 (час); Экзамен 4 (1ЗЕТ=36 ЧАСОВ) ;

Практические (семинарские) занятия 34 (час); Зачет - (семестр);

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

Самостоятельная работа 59 (час).

Зав. кафедрой ИБ _____ **Г.И. Качаева**

Начальник УО _____ **Э.В.Магомаева**

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных систем».

Программа одобрена на заседании выпускающей кафе́дры 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

_____ Мещеряков В.А.
подпись, И.О.Ф.
15.10
2018

АВТОР ПРОГРАММЫ

М.Г. Мирзажанов, ст. преп.
И.О.Ф., уч. степень, ученое звание

_____
подпись

1. Цели освоения дисциплины

Дисциплина «Криптографические протоколы» 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 «Криптографические протоколы» – 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 бакалавриата

Дисциплина «Криптографические протоколы» относится к дисциплинам по выбору вариативной части. Изучение её базируется на следующих дисциплинах: «Математическая логика и теория алгоритмов», «Методы программирования», «Дискретная математика».

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

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Криптографические протоколы»

Изучение дисциплины «Криптографические протоколы» обеспечивает овладение следующими компетенциями:

общепрофессиональные компетенции (ОПК):

способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);

профессиональные компетенции (ОПК):

способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

В результате изучения дисциплины «Криптографические протоколы» студенты должны:

знать:

- формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям;
- криптографические стандарты;
- типовые криптографические протоколы и основные требования к ним;
- принципы построения криптографических хеш-функций;
- основные схемы цифровой подписи;
- протоколы идентификации;
- протоколы передачи и распределения ключей;

уметь:

- использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов;
- формулировать свойства безопасности криптографических протоколов;

- проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;

владеть:

- криптографической терминологией;
- простейшими подходами к анализу безопасности криптографических протоколов.

4. Структура и содержание дисциплины (модуля) «Криптографические протоколы

Общая трудоемкость дисциплины составляет 5 зачетных единиц – 180 часов, в том числе: лекционных -17 часов, лабораторных - 34 часа, практических – 34 часа, СРС – 59 часов, форма отчетности экзамен в 4 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.	**Лекция 1.** Тема. Основные понятия 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. Понятие уязвимости и атаки на криптографический протокол. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов.	4	1,2	2	4	4	6	Вх. Контр.
2.	**Лекция 2.** Тема Схемы цифровой подписи Схемы цифровой подписи. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Схемы Эль-Гамаля, Фиата-Фейга-Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамаля. Стандарты США и России электронной цифровой подписи. Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки.		3,4	2	4	4	7	
3.	**Лекция 3.** **Тема:** Протоколы идентификации 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		5,6	2	4	4	7	АКР №1

	доказательства знания с нулевым разглашением. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото. Связь между протоколами цифровой подписи и протоколами идентификации. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.							
4.	**Лекция 4.** **Тема:** Инфраструктура открытых ключей Управление открытыми ключами. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509. Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа.	3	7,8	2	4	4	7	
5.	**Лекция 5.** **Тема:** Протоколы распределения ключей Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем. Двух и трех сторонние протоколы передачи и распределения ключей. Функции доверенной третьей стороны и выполняемые ею роли. Схемы предварительного распределения ключей.	3	9,10	2	4	4	7	АКР №2
6.	**Лекция 6.** **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». Аутентифицированные протоколы открытого распределения ключей. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.	3	11,12	2	4	4	7	
7.	**Лекция 7.** **Тема:** Прикладные протоколы Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей. Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации.	3	13,14	2	4	4	7	
8.	**Лекция 8.**	4	15,16	2	4	4	7	АКР №3

	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. Протокол сертифицированной электронной почты. Протоколы электронного голосования. Свойства неотслеживаемости и несвязываемости. Протоколы электронных платежей и цифровых денег.							
9.	**Лекция 9.** **Тема:** Заключение Обзор государственных стандартов и стандартов организаций в области криптографических протоколов. Проблемы автоматизации анализа криптографических протоколов. Итоги изучения дисциплины.		17	1	2	2	4	
	Итого			**17**	**34**	**34**	**59**	**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. Криптографические хэш-функции. Электронная цифровая подпись. Криптографические протоколы.	1	4
2	Лк№2	Поточные шифры. Барабанные машины. Шифр и табло Виженера.	2	4
3	Лк№ 2	Шифрование, дешифрование, криптоанализ.	2	4
4	Лк№ 3	Шифр Вернама. Шифрование, дешифрование, криптоанализ.	2-3	4
5	Лк№4 и5	ГОСТы. Нормативно-правовая база криптографии. DES. Тройной DES.	4-5	4
6	Лк№ 5,6	Дифференциальный и линейный криптоанализ блочных шифров.	4-5	4
7	Лк№ 6,7	Криптосистемы с открытым ключом. Алгоритм RSA.	4-5	4
8	Лк№ 8	Управление ключами. Система Диффи-Хеллмана.	4-5	4
9	Лк№ 9	Схема шифрования El-Gamal. Схема Kerberos.	4-5	2
Итого				**34**

4.3. Содержание практических занятий

№ п/п	№ лекции из рабочей программы	Наименование практического занятия	№ литер. источника из списка литературы	Кол-во часов
1	Лк№ 1	Основные понятия. Примеры протоколов на основе симметричных и асимметричных криптографических систем.	№1-17	4
2	Лк№2	Схемы цифровой подписи. Примеры схем цифровых подписей. Цифровые подписи DSA и ГОСТ.	№1-17	4
3	Лк№ 2	Протоколы идентификации. Протоколы «рукопожатия» и идентификации типа «запрос-ответ». Протоколы доказательства знания с нулевым разглашением.	№1-17	4
4	Лк№ 3	Инфраструктура открытых ключей. Протоколы идентификации на основе самосертифицируемых ключей. Сертификаты инфрастуктуры открытых ключей и их структура. Функции удостоверяющего центра.	№1-17	4
5	Лк№4 и5	Протоколы распределения ключей. Порядок проверки сертификатов для различных архитектур инфрастуктуры открытых ключей. Протоколы генерации и передачи ключей для симметричных шифрсистем.	№1-17	4
6	Лк№ 5	Протоколы распределения ключей. Протоколы генерации и передачи ключей для асимметричных шифрсистем. Схема предварительного распределения ключей Блома и ее устойчивость к компрометации ключей.	№1-17	4
7	Лк№ 6,7	Прикладные протоколы. Схемы предварительного распределения ключей на основе пересечения множеств. Протокол Kerberos.	№1-17	4
8	Лк№ 7,8	Протоколы открытого распределения ключей и их уязвимости. Протоколы семейства KriptoKnight для различных сетевых конфигураций и условий применения. Протоколы семейства IPSec.	№1-17	4
9	Лк№ 9	Заключение. Примеры прикладных протоколов (протоколы заключения сделок, платежных систем, сертифицированная электронная почта, голосования и др.).	№1-17	2
Итого				**34**

4.4. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Форма контроля СРС
1	Основные понятия	6	№1-17	Опрос, реферат, статья
2	Схемы цифровой подписи	7	№1-17	Опрос, реферат, статья
3	Протоколы идентификации	7	№1-17	Опрос, реферат, статья
4	Инфраструктура открытых ключей	7	№1-17	Опрос, реферат, статья
5	Протоколы распределения ключей	7	№1-17	Опрос, реферат, статья
6	Протоколы распределения ключей	7	№1-17	Опрос, реферат, статья
7	Прикладные протоколы	7	№1-17	Опрос, реферат, статья
8	Протоколы открытых сделок	7	№1-17	Опрос, реферат, статья
9	Заключение	4	№1-17	Опрос, реферат, статья
	Итого	**59**		

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-Гамаля, Фиата-Фейга-Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамаля.
12. Стандарты США и России электронной цифровой подписи.
13. Одноразовые 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

1. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото.
2. Связь между протоколами цифровой подписи и протоколами идентификации.
3. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.
4. Управление открытыми ключами.
5. Основы организации и основные компоненты инфраструктуры открытых ключей.
6. Сертификат открытого ключа.
7. Стандарт X.509.
8. Сервисы инфраструктуры открытых ключей.
9. Удостоверяющий центр. Центр регистрации.
10. Репозиторий.
11. Архив сертификатов. Конечные субъекты.
12. Архитектуры инфраструктуры открытых ключей.
13. Проверка и отзыв сертификата открытого ключа.

14. Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.
15. Двух и трех сторонние протоколы передачи и распределения ключей.
16. Функции доверенной третьей стороны и выполняемые ею роли.
17. Схемы предварительного распределения ключей.

Аттестационная контрольная работа №3

1. Неравенство Блома.
2. Схемы предварительного распределения ключей Блома и на основе пересечений множеств.
3. Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине».
4. Аутентифицированные протоколы открытого распределения ключей.
5. Групповые протоколы.
6. Протоколы разделения секрета и распределения ключей для телеконференции.
7. Особенности построения семейства протоколов IPsec.
8. Протоколы Oakley, ISAKMP, IKE.
9. Протоколы SKIP, SSL/TLS и особенности их реализации.
10. Особенности построения семейства протоколов IPsec.
11. Протоколы Oakley, ISAKMP, IKE.
12. Протоколы SKIP, SSL/TLS и особенности их реализации.
13. Протоколы битовых обязательств и их свойства.
14. Протоколы подбрасывания монеты и “игры в покер” по телефону.
15. Забывающая передача информации.
16. 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-Гамаля, Фиата-Фейга-Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамаля.
12. Стандарты США и России электронной цифровой подписи.
13. Одноразовые 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-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.
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

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).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.

12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой _____

№	Виды занятий (лк, пз, лб, срс, ирс)	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 библиотеке	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 c. — 978-5-4383-0161-5.	http://www.iprbookshop.ru/73641.html	
3.	ЛК,СР, КР	Организационная защита информации [Электронный ресурс]	АверченковВ. И.	Брянск: Брянский государственный технический университет, 2012. — 184 c. — 978-89838-489-0	http://www.iprbookshop.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 c. — 2227-8397	http://www.iprbookshop.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 c. — 2227-8397	http://www.iprbookshop.ru/17926.html	
6.	ЛК,СР, КР	Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие	Креопалов В. В.	М.: Евразийский открытый институт, 2011. — 278 c. — 978-5-374-00507-3.	http://www.iprbookshop.ru/10871.html	
7.	ЛК,СР, КР	Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие	Башлы П. Н.	М.: Евразийский открытый институт, 2012. — 311 c. — 978-5-374-00301-7.	http://www.iprbookshop.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 c. — 2227-8397.		

		Дополнительная литература			
9.	ЛК,СР, КР	Комплексная защита информации в компьютерных системах. Учебное пособие	Завгородний В.И.	М.: Логос, Пбоюл Н.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.-(высш.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., Першаков 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	Молдовян А.А. и др.	СПб., БХВ-Петербург, 2002.-496с.	http://www.iprbookshop.ru/17010.html
		Интернет - источники			
15.	ЛК,СР, КР	http://dstu.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 с учетом рекомендаций ООП ВО по направлению 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных систем».

Рецензент рабочей программы от выпускающей кафедры по направлению 10.03.01 – «Информационная безопасность», профилю «Безопасность автоматизированных систем».

З.Р. Радиславова