МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ С.М. Пасмурнов

«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Криптографические протоколы»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация Безопасность распределённых компьютерных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ /Радько Н.М./

Заведующий кафедрой
Систем информационной
безопасности _____ /Остапенко А. Г./

Руководитель ОПОП _____ / Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Целью дисциплины являются формирование у студентов теоретических знаний и практических навыков по основам криптологии, базовым криптографическим примитивам, по синтезу и анализу стойкости криптографических протоколов.

1.2. Задачи освоения дисциплины

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 ОПОП

Дисциплина «Криптографические протоколы» относится к дисциплинам базовой части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Криптографические протоколы» направлен на формирование следующих компетенций:

ОПК-2 - способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов

ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

ПК-10 - способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

ПК-11 - способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-2	**Знать:** - структуру парольных систем разграничения доступа.
	Уметь: - использовать свойства криптографических средств при анализе комплексных систем защиты информации.

	Владеть: - основными характеристиками криптографических протоколов.
ПК-5	**Знать:** - принципиальные подходы к криптографическим протоколам.
	Уметь: - практически решать задачи защиты программ и данных криптографическими средствами.
	Владеть: - основными требованиями, предъявляемыми к криптографическим протоколам.
ПК-10	**Знать:** - современные тенденции развития криптографической защиты информации.
	Уметь: - оценивать уязвимость протоколов и интерфейсов компьютерных систем.
	Владеть: - типовыми криптографическими протоколами и их криптографическими качествами.
ПК-11	**Знать:** - основные стандарты, протоколы и интерфейсы, необходимые при сертификации средств защиты информации.
	Уметь: - применять криптографические средства и системы информационной безопасности.
	Владеть: - государственными (национальными) стандартами, регулирующими криптографические протоколы.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Криптографические протоколы» составляет 4 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		8
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	36	36
Практические занятия (ПЗ)	18	18
Самостоятельная работа	90	90
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы	144	144

зач.ед.	4	4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ зан.	СРС	Всего, час
1	Криптографические протоколы и основные требования	Содержание и задачи дисциплины. Ее особенности и связь с другими дисциплинами. Методические рекомендации по ее изучению и требования, предъявляемые при проверке знаний (сдаче зачета). Понятие протокола. Организация связи с помощью симметричной криптографии. Однонаправленные функции. Цифровые подписи. Генераторы случайных последовательностей.	6	2	14	22
2	Протоколы “рукопожатия”. Протоколы генерации ключей	Протоколы установления подлинности Обмен ключами средствами симметричной криптографии. Формальный анализ протоколов проверки подлинности и обмена ключами. Разделение секрета.	6	2	14	22
3	Протоколы идентификации и аутентификации Парольные системы разграничения доступа	Протоколы идентификации и аутентификации Аутентификация с помощью однонаправленных функций. Атака по словарю. Подтверждение подлинности сообщений. Самостоятельное изучение. Парольные системы разграничения доступа.	6	2	14	22

		Основы построения парольных систем. Безопасность алгоритмов.				
4	Протоколы генерации ключей. Протоколы распределения ключей	Сокращенные пространства ключей. Неправильно выбранные ключи. Случайные ключи. Ключевые фразы. Нелинейные пространства ключей. Стандарт генерации ключей X9.17. Пересылка ключей.. Протоколы распределения ключей Резервные копии ключей шифрования. Скомпрометированные ключи. Время жизни ключей. Уничтожение ключей. Управление ключами в системах с открытым ключом.	6	4	16	26
5	Рекомендации X.509	Рекомендации X.509. Основные положения. Практическое применение.	6	4	16	26
6	Протоколы разделения секретов. Протоколы "игры в покер"	Протоколы с нулевым разглашением Доказательства нулевого разглашения. Изоморфизм графов. Базовый протокол с нулевым разглашением Гамильтоновы циклы. Параллельные доказательства с нулевым разглашением. Неинтерактивные доказательства с нулевым разглашением. Идентификация с помощью доказательств с нулевым разглашением. Подписи “вслепую”. Мысленный покер с трѐмя игроками. Атаки на протоколы мысленного покера. Анонимное распределение ключей.	6	4	16	26
		Итого	**36**	**18**	**90**	**144**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-2	**Знать:** - структуру парольных систем разграничения доступа.	Знание структуры парольных систем разграничения доступа.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - использовать свойства криптографических средств при анализе комплексных систем защиты информации.	Умение использовать свойства криптографических средств при анализе комплексных систем защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - основными характеристиками криптографических протоколов.	Владение основными характеристиками криптографических протоколов.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	**Знать:** - принципиальные подходы к криптографическим протоколам.	Знание принципиальных подходов к криптографическим протоколам.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - практически решать задачи защиты программ и данных	Умение практически решать задачи защиты программ и данных криптографическими средствами.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	криптографическим и средствами.			
	Владеть: - основными требованиями, предъявляемыми к криптографическим протоколам.	Владение основными требованиями, предъявляемыми к криптографическим протоколам.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-10	**Знать:** - современные тенденции развития криптографической защиты информации.	Знание современные тенденции развития криптографической защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - оценивать уязвимость протоколов и интерфейсов компьютерных систем.	Умение оценивать уязвимость протоколов и интерфейсов компьютерных систем.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - типовыми криптографическим и протоколами и их криптографическим и качествами.	Владение типовыми криптографическими протоколами и их криптографическими качествами.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-11	**Знать:** - основные стандарты, протоколы и интерфейсы, необходимые при сертификации средств защиты информации.	Знание основные стандарты, протоколы и интерфейсы, необходимые при сертификации средств защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - применять криптографические средства и системы информационной безопасности.	Умение применять криптографические средства и системы информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - государственными (национальными) стандартами, регулирующими криптографические протоколы.	Владение государственными (национальными) стандартами, регулирующими криптографические протоколы.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре

для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-2	**Знать:** - структуру парольных систем разграничения доступа.	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - использовать свойства криптографических средств при анализе комплексных систем защиты информации.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - основными характеристиками криптографических протоколов.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-5	**Знать:** - принципиальные подходы к криптографическим протоколам.	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - практически решать задачи защиты программ и данных криптографическими средствами.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - основными требованиями, предъявляемыми к криптографическим протоколам.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-10	**Знать:** - современные тенденции развития криптографической	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	защиты информации.					
	Уметь: - оценивать уязвимость протоколов и интерфейсов компьютерных систем.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - типовыми криптографическими протоколами и их криптографическими качествами.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-11	**Знать:** - основные стандарты, протоколы и интерфейсы, необходимые при сертификации средств защиты информации.	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: - применять криптографические средства и системы информационной безопасности.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - государственными (национальными) стандартами, регулирующими криптографические протоколы.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1.Что в переводе с греческого языка означает слово «криптография»?

шифр

тайнопись +

преобразование

расшифровка

2. Как называется «исторический» шифр, в котором каждая буква

исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?

шифр Маркова

шифр Цезаря +

шифр Энигма

шифр Бэбиджа

3. Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?

алгоритм

ключ

протокол

шифр+

4. Как называется сообщение, полученное после преобразования с использованием любого шифра?

закрытым текстом +

имитовставкой

ключом

открытым текстом

5. Что в криптографии называют открытым текстом?

исходное сообщение (сообщение до шифрования) +

открытый ключ шифрования

сообщение, получение после преобразования с использованием любого шифра

электронную цифровую подпись

6. Гарантирование невозможности несанкционированного изменения информации - это:

обеспечение целостности +

обеспечение конфиденциальности

обеспечение аутентификации

обеспечение шифрования

7. Под конфиденциальностью понимают (выберите продолжение)

решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, имеющих права доступа к ней

решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней +

решение проблемы защиты информации от ее изменения со стороны лиц, не имеющих права доступа к ней

решение проблемы запуска программ со стороны лиц, не имеющих права доступа к ним

разрешение пользоваться информацией только одному лицу

8. Выберите правильное определение термина «криптоанализ»

криптоанализ – это наука о преодолении криптографической защиты информации

криптоанализ – это наука, занимающаяся шифрованием данных при

передаче по открытым каналам связи +

криптоанализ изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия

криптоанализ изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации

9. Какие задачи решает криптография?

защита передаваемых сообщений от прочтения +

защита передаваемых сообщений от модификации +

сжатие передаваемых сообщений

помехоустойчивое кодирование передаваемых сообщений

10. Какой способ реализации криптографических методов обладает максимальной скоростью обработки данных?

аппаратный +

программный

ручной

электромеханический

7.2.2 Примерный перечень заданий для решения стандартных задач

ОПК-2 - способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов
1. Основные алгоритмы шифрования. 2. Цифровые подписи. 3. Криптографические хеш-функции. 4. Криптографические генераторы случайных чисел. 5. Обеспечиваемая шифром степень защиты. 6. Криптоанализ и атаки на криптосистемы.
ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
1. Классификация шифров. 2. Блочные шифры. 3. Поточные шифры. 4. Алфавиты открытых сообщений. 5. Частотные характеристики текстовых сообщений. 6. Основные положения.
ПК-10 – способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
1. Пример функции хэширования – ГОСТ Р 34.11-94. 2. Цифровая подпись.

3. Основные положения криптосистемы RSA. 4. Построение кодирующей процедуры E для криптосистемы RSA. 5. Построение декодирующей процедуры D для криптосистемы RSA. 6. Алгоритмические задачи, связанные со схемой RSA.
ПК-11 - способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации
1. Общая идея шифра Эль-Гамаля. 2. Пароли шифра Эль-Гамаля. 3. Электронная подпись шифра Эль-Гамаля. 4. Задача аутентификации данных. 5. Задача имитозащиты данных. 6. Подходы к контролю неизменности данных.

7.2.3 Примерный перечень заданий для решения прикладных задач

ОПК-2 - способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	
1	Цифровая подпись обеспечивает: o скрытие содержания сообщения o **аутентификацию источника данных** o **целостность сообщения** o **юридическую значимость сообщения**
2	Какие криптосистемы используются для формирования цифровой подписи и шифрования (формирования) симметричных ключей при их рассылке по каналам связи: o симметричные o **несимметричные** o блочные подстановки перестановки гаммирование o Эль-Гамаля, Ривестра-Шамира-Эйделмана, Меркля-Хеллмана и Хора-Ривестра
3	Какой шифр является модификацией шифра Цезаря, в котором величина сдвига является переменной и зависит от ключевого слова. Например, если в качестве ключевого слова использовать слово "ТАЙНА", то это будет означать, что первую букву сообщения необходимо сдвинуть на 20 (порядковый номер буквы "Т"), вторую - на 1 (порядковый номер буквы "А"), третью - на 11, четвертую - на 15, пятую - на 1, шестую - снова на 20 (ключевое слово начинаем использовать с начала) и т.д. Таким образом, ключевое слово "накладывается" на защищаемый текст: o **шифр Виженера** o шифр Вернама o шифр Цезаря o шифр Гронсфельда
4	Стандарт доступа и управления передачей файлов FTAM (File Transfer Access and Management) определяющий все необходимые правила работы с файлами: o Triple-DES o Advanced Encryption Standard (AES)

	o OpenPGP o **ISO-OSI**
ПК-5 - способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	
1	Наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей это: o **криптография** o криптоанализ o криптология o стеганография
2	Вскрытие (взламывание) шифра это: o преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре o **процесс получения защищаемой информации из шифрованного сообщения без знания примененного шифра** o преобразование защищаемой информации в шифрованное сообщение с помощью определенных правил, содержащихся в шифре o наука о способах преобразования информации с целью ее защиты от незаконных пользователей
3	Основными видами криптографического закрытия являются: o замена (подстановка), перестановка, гаммирование защищаемых данных o дешифрование и кодирование защищаемых данных o **шифрование и кодирование защищаемых данных** o шифрование и дешифрование защищаемых данных
4	Что понимается под аутентификацией информации: o **установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена** o установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети o установление подлинности сети, к которой получен доступ o установление факта, что данный массив не был изменен в течение времени, когда он был вне посредственного контроля, а также решение вопросов об авторстве этого массива данных
ПК-10 – способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	
1	Основной характеристикой меры защищенности информации криптографическим закрытием является: o **стойкость шифра**

	o структура шифра o распад шифра o совершеннность шифра
2	Имитозащита обеспечивает: o **целостность сообщения в соответствии со свойствами контрольной суммы.** o формировании контрольной суммы (имитовставки, кода аутентификации сообщения) по криптоалгоритму, добавляемой к сообщению o разработку пакета программных средств обеспечения юридической значимости лицензий посредством цифровой подписи o проверку получателем документа и независимой третьей стороной (арбитром) и обеспечением аутентификации создателя подписи
3	Процесс восстановления открытого текста из шифртекста без знания ключа это: o алгоритм шифрования o зашифрование o расшифрование o **дешифрование**
4	Процесс восстановления открытого текста из шифртекста с использованием ключа это: o алгоритм шифрования o зашифрование o **расшифрование** o дешифрование
ПК-11 - способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	
1	Что понимается под аутентификацией хранящихся массивов программ и данных: o установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена o установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети o установление подлинности сети, к которой получен доступ o **установление факта, что данный массив не был изменен в течение времени, когда он был вне посредственного контроля, а также решение вопросов об авторстве этого массива данных** o
2	Аутентификация пользователя сети это: o **установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети** o установление подлинности содержания полученного по каналам связи

	сообщения и решение вопросов об авторстве сообщения o установление подлинности сети, к которой получен доступ o установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации
3	Алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены, канал связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования: o метод цифрового конверта o метода Эль-Гамаля o **Диффи-Хеллмана** o RSA
4	По способу использования средств шифрования информации различают: o **поточное и блочное симметричное шифрование** o симметричное и несимметричное o канальное шифрование и оконечное (абонентское) шифрование. o односторонней и взаимной идентификации

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

1.Содержание и задачи дисциплины. Ее особенности и связь с другими дисциплинами.

2. Понятие протокола. Организация связи с помощью симметричной криптографии. Однонаправленные функции. Цифровые подписи. Генераторы случайных последовательностей.

3.Протоколы “рукопожатия”. Протоколы генерации ключей

4.Протоколы идентификации и аутентификации

5. Парольные системы разграничения доступа

6. Протоколы генерации ключей

7. Протоколы распределения ключей

8.Протоколы разделения секретов.

9.Протоколы "игры в покер"

10.Протоколы установления подлинности

11. Обмен ключами средствами симметричной криптографии. Формальный анализ протоколов проверки подлинности и обмена ключами. Разделение секрета.

12.Аутентификация с помощью однонаправленных функций. Атака по словарю. Подтверждение подлинности сообщений.

13.Основы построения парольных систем. Безопасность алгоритмов.

14.Сокращенные пространства ключей. Неправильно выбранные ключи. Случайные ключи. Ключевые фразы. Нелинейные пространства ключей.

15.Стандарт генерации ключей X9.17. Пересылка ключей.

16.Протоколы распределения ключей

17. Резервные копии ключей шифрования. Скомпрометированные ключи. Время жизни ключей. Уничтожение ключей. Управление ключами в системах с открытым ключом.

18.Протоколы с нулевым разглашением Доказательства нулевого разглашения.

19.Изоморфизм графов. Базовый протокол с нулевым разглашением Гамильтоновы циклы.

20.Параллельные доказательства с нулевым разглашением. Неинтерактивные доказательства с нулевым разглашением.

21. Идентификация с помощью доказательств с нулевым разглашением. Подписи “вслепую”.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Криптографические протоколы и основные требования	ОПК-2, ПК-5, ПК- 10, ПК-11	Тест, контрольная работа, защита практических работ
2	Протоколы “рукопожатия”. Протоколы генерации ключей	ОПК-2, ПК-5, ПК- 10, ПК-11	Тест, контрольная работа, защита практических работ
3	Протоколы идентификации и аутентификации Парольные системы разграничения доступа	ОПК-2, ПК-5, ПК- 10, ПК-11	Тест, контрольная работа, защита практических работ
4	Протоколы генерации ключей. Протоколы распределения ключей	ОПК-2, ПК-5, ПК- 10, ПК-11	Тест, контрольная работа, защита практических работ
5	Рекомендации X.509	ОПК-2, ПК-5,	Тест, контрольная

		ПК- 10, ПК-11	работа, защита практических работ
6	Протоколы разделения секретов. Протоколы "игры в покер"	ОПК-2, ПК-5, ПК- 10, ПК-11	Тест, контрольная работа, защита практических работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная

Молдовян А.А. Протоколы аутентификации с нулевым разглашением секрета [Электронный ресурс]/ Молдовян А.А., Молдовян Д.Н., Левина А.Б.— Электрон. текстовые данные.— Санкт-Петербург: Университет ИТМО, 2016.— 55 с.— Режим доступа: http://www.iprbookshop.ru/68058.html.

Дополнительная

1.Косолапов Ю.В. Криптографические протоколы на основе линейных кодов [Электронный ресурс]: учебное пособие/ Косолапов Ю.В.— Электрон. текстовые данные.— Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2020.— 98 с.— Режим доступа: http://www.iprbookshop.ru/100176.html.

2.Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс]: учебное пособие/ Лапонина О.Р.— Электрон. текстовые данные.— Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 605 с.— Режим доступа: http://www.iprbookshop.ru/97571.html.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://infoprotect.net/varia/kriptograficheskie_protokolyi

Основные виды криптографических протоколов

https://habr.com/ru/post/475218/

Криптографические протоколы: определения, запись, свойства, классификация, атаки

https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB

Криптографический протокол

http://padaread.com/?cat=9814

Список ресурсов по криптопротоколам

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения практических занятий

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Криптографические протоколы» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на:

Неделя семе-стра	Тема и содержание практического занятия	Объем часов	В том чис-ле, в инте-рактивной форме (ИФ)	Виды контро-ля
1-3	Цифровые подписи	2	1	
3-4	Генераторы случайных последовательностей	2	1	
4-5	Протоколы “рукопожатия	2	1	
5-6	Разделение секрета	2	1	
6-17	Атака по словарю	2	1	
7-8	Безопасность алгоритмов	1		
9	**Контрольная работа**	2	1	Контр. раб.
10-11	Пересылка ключей	2	1	
12-13	Уничтожение ключей	2		
13-14	Практическое применение рекомендации X.509	2	1	

14-15	Гамильтоновы циклы	2		
15-16	Подписи “вслепую”.	2		
16-17	Атаки на протоколы мысленного покера	1		
Итого часов		**34**	**8**	

Занятия проводятся путем решения конкретных задач в аудитории.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.