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 2017

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. Цели дисциплины - получение знаний об основных методах защиты информации с использованием криптографических протоколов.

1.2. Задачи освоения дисциплины

- дать студентам основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических протоколов;
- изучение основных принципов реализации криптографических протоколов;
- изучение перспективных направлений и тенденций развития криптографических систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Криптографические протоколы» относится к дисциплинам обязательной части блока Б1 учебного плана.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

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

ОПК-10 - способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-10	**Знать:** - основные типы криптографические протоколы и принципов их построения с использованием шифрсистем; - основные стандарты, протоколы и интерфейсы, необходимые при сертификации средств защиты информации.
	Уметь: - проводить анализ криптографических протоколов; - применять криптографические средства и системы информационной безопасности.
	Владеть: - математическими методами при использовании

	криптографических протоколов; - государственными (национальными) стандартами, регулирующими криптографические протоколы.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Криптографические протоколы» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

Виды учебной работы	Всего часов	Семестры
		А
Контактная работа по видам занятий (всего)	72	72
В том числе:		
Лекции	36	36
Практические занятия (ПЗ)	36	36
Самостоятельная работа	108	108
Часы на контроль	-	-
Виды промежуточной аттестации		Зачет с оценкой
Общая трудоемкость час з.е.	180 5	180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ. зан.	СРС	Всего, час
9 семестр						
1	Криптографические протоколы и основные требования	Содержание и задачи дисциплины. Ее особенности и связь с другими дисциплинами. Понятие протокола. Организация связи с помощью симметричной криптографии. Однонаправленные функции. Цифровые подписи. Генераторы случайных последовательностей.	6	6	14	26
2	Протоколы “рукопожатия”. Протоколы установления подлинности	Протоколы “рукопожатия”. Основные положения. Практическое применение. Обмен ключами средствами симметричной криптографии. Формальный анализ протоколов проверки подлинности и обмена ключами. Разделение секрета.	6	6	14	26
3	Протоколы идентификации и аутентификации	Аутентификация с помощью однонаправленных функций. Атака по словарю. Подтверждение подлинности сообщений. Парольные системы разграничения доступа. Основы построения парольных систем. Безопасность алгоритмов. Протоколы генерации ключей. Сокращенные пространства ключей. Неправильно	6	6	20	32

		выбранные ключи. Случайные ключи. Ключевые фразы. Нелинейные пространства ключей. Стандарт генерации ключей X9.17. Пересылка ключей.				
4	Протоколы распределения ключей	Резервные копии ключей шифрования. Скомпрометированные ключи. Время жизни ключей. Уничтожение ключей. Управление ключами в системах с открытым ключом. Рекомендации X.509. Основные положения. Практическое применение.	6	6	20	32
5	Принципы построения и реализации криптографических алгоритмов	Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Датчики псевдослучайных последовательностей (регистры сдвига, линейный конгруэнтный метод, линейные рекуррентные последовательности, мультиплексорные методы). Периодичность случайных последовательностей. Распределение элементов в псевдослучайных последовательностях. Основные узлы и блоки криптосистем. Блоки выработки шифрующей последовательности и блоки шифрования.	6	6	20	32
6	Протоколы разделения секретов	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”. Протоколы "игры в покер". Мысленный покер с трёмя игроками. Атаки на протоколы мысленного покера. Анонимное распределение ключей.	6	6	20	32
		Итого	**36**	**36**	**108**	**180**

5.2 Перечень практических занятий

1. Цифровые подписи. Генераторы случайных последовательностей – 6 ч.
2. Протоколы «рукопожатия». Разделение секрета – 6 ч.
3. Атака по словарю. Безопасность алгоритмов – 6 ч.
4. Пересылка ключей. Уничтожение ключей – 6 ч.
5. Практическое применение рекомендации X.509. Гамильтоновы циклы – 6 ч.
6. Подписи “вслепую”. Атаки на протоколы мысленного покера – 6 ч.

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

Учебным планом по дисциплине «Криптографические протоколы» не предусмотрено выполнение курсового проекта (работы).

Предусмотрено выполнение контрольных работ по следующим темам:

- Цифровые подписи;
- Протоколы “рукопожатия”;
- Основы построения парольных систем;

- Аутентификация с помощью однонаправленных функций;
- Протоколы с нулевым разглашением;
- Мысленный покер с трёмя игроками.

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-10	**Знать:** - основные типы криптографические протоколы и принципов их построения с использованием шифрсистем; - основные стандарты, протоколы и интерфейсы, необходимые при сертификации средств защиты информации.	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - проводить анализ криптографических протоколов; - применять криптографические средства и системы информационной безопасности.	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - математическими методами при использовании криптографических протоколов; - государственными (национальными) стандартами, регулирующими криптографические протоколы.	Решение прикладных задач в конкретной предметной области	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 А семестре по четырехбальной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ОПК-10	**Знать:** - основные типы криптографические протоколы и принципов их построения с использованием шифрсистем; - основные стандарты, протоколы и интерфейсы, необходимые при сертификации средств защиты информации.	знание учебного материала и использование учебного материала в процессе выполнения заданий	Студент демонстрирует полное понимание учебного материала. Студент демонстрирует ярко выраженную способность использовать знания, умения, навыки в процессе выполнения заданий	Студент демонстрирует значительное понимание материала. Студент демонстрирует способность использовать знания, умения, навыки в процессе выполнения заданий	Студент демонстрирует частичное понимание материала. Способность студента продемонстрировать знание, умение, навык выражена слабо	1. Студент демонстрирует незначительное понимание материала. 2. Студент демонстрирует непонимание заданий. 3. У студента нет ответа. Не было попытки выполнить задания.
	Уметь: проводить анализ криптографических протоколов; - применять криптографические средства и системы информационной безопасности.	умение использовать учебный материал в процессе выполнения практических работ				
	Владеть: - математическими методами при использовании криптографических протоколов; - государственными (национальными) стандартами, регулирующими криптографические протоколы.	применение учебного материала при решении практических задач				

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

(минимум 10 вопросов для тестирования с вариантами ответов)

1) Наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей это:

- **криптография**
- криптоанализ
- криптология
- стеганография

2) Вскрытие (взламывание) шифра это:

- преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре
- **процесс получения защищаемой информации из шифрованного сообщения без знания примененного шифра**
- преобразование защищаемой информации в шифрованное сообщение с помощью определенных правил, содержащихся в шифре
- наука о способах преобразования информации с целью ее защиты от незаконных пользователей

3) Основными видами криптографического закрытия являются:

- замена (подстановка), перестановка, гаммирование защищаемых данных
- дешифрование и кодирование защищаемых данных
- **шифрование и кодирование защищаемых данных**
- шифрование и дешифрование защищаемых данных

4) Основной характеристикой меры защищенности информации криптографическим закрытием является:

- **стойкость шифра**
- структура шифра
- распад шифра
- совершеннность шифра

5) Что понимается под аутентификацией информации:

- **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

- установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети
- установление подлинности сети, к которой получен доступ
- 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

6) Аутентификация сети это:

- установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети
- установление подлинности содержания полученного по каналам связи сообщения и решение вопросов об авторстве сообщения.
- **установление подлинности сети, к которой получен доступ**
- установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации

7) Что понимается под аутентификацией хранящихся массивов программ и данных:

- 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
- установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети
- установление подлинности сети, к которой получен доступ
- **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**

8) Аутентификация пользователя сети это:

- **установление подлинности личности пользователя сети, которому требуется доступ к защищаемой информации или необходимо подключиться к сети**
- установление подлинности содержания полученного по каналам связи сообщения и решение вопросов об авторстве сообщения
- установление подлинности сети, к которой получен доступ
- установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации

9) Цифровая подпись обеспечивает:

- скрытие содержания сообщения
- **аутентификацию источника данных**
- **целостность сообщения**
- **юридическую значимость сообщения**

10) Имитозащита обеспечивает:

- **целостность сообщения в соответствии со свойствами контрольной суммы.**
- формировании контрольной суммы (имитовставки, кода аутентификации сообщения) по криптоалгоритму, добавляемой к сообщению
- разработку пакета программных средств обеспечения юридической значимости лицензий посредством цифровой подписи
- проверку получателем документа и независимой третьей стороной (арбитром) и обеспечением аутентификации создателя подписи

7.2.2 Примерный перечень заданий для решения стандартных задач

1) По способу использования средств шифрования информации различают:

- **поточное и блочное симметричное шифрование**
- симметричное и несимметричное
- канальное шифрование и оконечное (абонентское) шифрование.
- односторонней и взаимной идентификации

2) Какие криптосистемы используются для формирования цифровой подписи и шифрования (формирования) симметричных ключей при их рассылке по каналам связи:

- симметричные
- **несимметричные**
- блочные подстановки перестановки гаммирование
- Эль-Гамаля Ривестра-Шамира-Эйделмана Меркля-Хеллмана и Хора-Ривестра

3) Стандарт доступа и управления передачей файлов FTAM (File Transfer Access and Management) определяющий все необходимые правила работы с файлами:

- Triple-DES
- Advanced Encryption Standard (AES)
- OpenPGP
- **ISO-OSI**

4) Стандарт ISO 8571, протокол прикладного уровня OSI для передачи, доступа и управления файлами:

- SMB
- NFS
- **FTAM**
- Andrew File System

5) Процесс преобразования открытого текста в шифртекст с использованием ключа это:

- алгоритм шифрования
- **зашифрование**
- расшифрование
- дешифрование

6) Что такое шифр?

- **обратимый способ преобразования информации с целью защиты ее от просмотра, в котором используется некий секретный элемент**
- процесс преобразования открытого текста в шифртекст с использованием ключа

- процесс восстановления открытого текста из шифртекста с использованием ключа
- процесс восстановления открытого текста из шифртекста без знания ключа

7) Процесс восстановления открытого текста из шифртекста без знания ключа это:
- алгоритм шифрования
- зашифрование
- расшифрование
- **дешифрование**

8) Процесс восстановления открытого текста из шифртекста с использованием ключа это:
- алгоритм шифрования
- зашифрование
- **расшифрование**
- дешифрование

9) 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:
- **шифр Виженера**
- шифр Вернама
- шифр Цезаря
- шифр Гронсфельда

10) 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:
- метод цифрового конверта
- метода Эль-Гамаля
- **Диффи-Хеллмана**
- RSA

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Понятие протокола.
2. Организация связи с помощью симметричной криптографии.
3. Однонаправленные функции.
4. Цифровые подписи.
5. Генераторы случайных последовательностей.
6. Протоколы “рукопожатия”. Основные положения. Практическое применение.
7. Обмен ключами средствами симметричной криптографии.
8. Формальный анализ протоколов проверки подлинности и обмена ключами.
9. Разделение секрета.
10. Протоколы идентификации и аутентификации.

11. Аутентификация с помощью однонаправленных функций.
12. Атака по словарю.
13. Подтверждение подлинности сообщений.
14. Парольные системы разграничения доступа.
15. Основы построения парольных систем.
16. Безопасность алгоритмов.
17. Сокращенные пространства ключей.
18. Неправильно выбранные ключи.
19. Случайные ключи.
20. Ключевые фразы.
21. Нелинейные пространства ключей.
22. Стандарт генерации ключей X9.17.
23. Пересылка ключей.
24. Резервные копии ключей шифрования.
25. Скомпрометированные ключи.
26. Время жизни ключей.
27. Уничтожение ключей.
28. Управление ключами в системах с открытым ключом.
29. Рекомендации X.509.
30. Основные положения. Практическое применение.
31. Протоколы с нулевым разглашением
32. Доказательства нулевого разглашения.
33. Изоморфизм графов.
34. Базовый протокол с нулевым разглашением Гамильтоновы циклы.
35. Параллельные доказательства с нулевым разглашением.
36. Неинтерактивные доказательства с нулевым разглашением.
37. Идентификация с помощью доказательств с нулевым разглашением.
38. Подписи “вслепую”.
39. Мысленный покер с трёмя игроками.
40. Атаки на протоколы мысленного покера.
41. Анонимное распределение ключей.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Оценивание может осуществляться либо на основе тестирования, либо путем ответа на вопросы экзаменационного билета.

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-10	Контрольная работа, решение практических задач

2	Протоколы “рукопожатия”. Протоколы установления подлинности	ОПК-10	Контрольная работа, решение практических задач
3	Протоколы идентификации и аутентификации	ОПК-10	Контрольная работа, решение практических задач
4	Протоколы распределения ключей	ОПК-10	Контрольная работа, решение практических задач
5	Принципы построения и реализации криптографических алгоритмов	ОПК-10	Контрольная работа, решение практических задач
6	Протоколы разделения секретов	ОПК-10	Контрольная работа, решение практических задач

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

При преподавании дисциплины «Криптографические протоколы» в качестве формы оценки знаний студентов используются: контрольные работы, решение практических задач различной сложности, зачет с оценкой.

Контрольные работы выполняется в письменном виде, либо при помощи компьютерной системы ответом на вопросы. Время выполнения контрольной работы - 45 мин. Затем осуществляется проверка преподавателем и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных и прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Выполнение практических заданий осуществляется согласно учебного плана в соответствии с «Методическими указаниями по выполнению практических заданий…».

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная:

1. Алфёров А.П. Основы криптографии: учеб. пособие / А.П. Алферов, Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. - М.: Гелиос АРВ, 2002. - 480 с.: ил . - ISBN 5-85438-025-0
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ / В. В. Золотарев, Г. В. Овечкин. - М.:

Горячая линия - Телеком, 2004. - 126 с.: ил . - ISBN 5-93517-169-4: 130-00.

3. Петраков А.В. Основы практической защиты информации / А.В. Петраков. - 4-е изд., стереотип. - М.: Радио и связь, 2005. - 384 с. - ISBN 5-256-01507-9

Дополнительная:

1. Корниенко А.А. Криптографические протоколы учебное пособие / А. А. Корниенко, М.Л. Глухарев. - Санкт-Петербург: ПГУПС, 2020. - 74 с. - ISBN 978-5-7641-1509-2. - Текст: электронный // Лань: электронно-библиотечная система.
2. Диффи У. Защищенность и криптостойкость. Введение в криптографию/ У. Диффи, Э. Хеллмен. – М.: ТИИЭР, том 67, №3, 1979.
3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков. - Москва: НИЯУ МИФИ, 2012. - 400 с. - ISBN 978-5-7262-1676-8. - Текст: электронный // Лань: электронно-библиотечная система.
4. Хоффман Л.Дж. Современные методы защиты информации/ под ред. Ю.Н. Мельникова - М.: Сов. Радио, 2007. - 368 с.

Методические разработки:

1. Радько Н.М. Криптографические протоколы [Электронный ресурс]: учеб. пособие / Н. М. Радько, А. Н. Мокроусов. - Электрон. дан. (1 файл :770 560 байта). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2006. - 1 дискета. - 30-00.
2. Методические указания к практическим занятиям по дисциплине «Криптографические протоколы» для студентов специальности 090301 «Компьютерная безопасность», очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. А.Н. Мокроусов. - Электрон. текстовые, граф. дан. (1,0 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.
3. Радько Н. М. Основы криптографической защиты информации: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (1,04 Мб) / Н. М. Радько, А. Н. Мокроусов. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2014. – 1 электрон. опт. диск (CD-ROM).
4. Радько Н.М. Защита информации в беспроводных сетях: Учеб.пособие / Н.М. Радько, А.Н. Мокроусов. Воронеж: ГОУВПО “Воронежский государственный технический университет” 2010. - 100с.

5. Мокроусов А.Н. Основы криптографической защиты информации [Электронный ресурс]: учеб. пособие / А. Н. Мокроусов, Н. М. Радько. - Электрон. дан. (1 файл). - Воронеж: ВГТУ, 2004. - 1 дискета. - 30.00.
6. Методические указания к самостоятельным работам по дисциплине «Криптографические протоколы» студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. Н. М. Радько. - Электрон. текстовые, граф. дан. (407 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

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://www.eios.vorstu.ru (электронная информационно-обучающая система ВГТУ)
http://e.lanbook.com/ (ЭБС Лань)
http://znanium.com/ (ЭБС Знаниум)
http://IPRbookshop.ru/ (ЭБС IPRbooks (Айбукс))
http://urait.ru/ (Образовательная платформа «Юрайт»)

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.

На практических занятиях проводится решение стандартных и прикладных задач в соответствии с темой занятия. Методики решения задач

приведены в методических указаниях к практическим занятиям.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Контроль усвоения материала дисциплины производится проверкой выполнения контрольных работ и практических занятий. Освоение дисциплины оценивается на дифференцированном зачете А-ом семестре.

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.
Практические занятия	Практические занятия позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности практических занятий для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебного пособия по данной дисциплине, проработать дополнительную литературу и источники, решить задачи для самостоятельного решения из соответствующего раздела методических указаний к практическим занятиям.
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 экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.