СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

А.Б. Левина

Криптография и криптографические протоколы

Методические рекомендации и план проведения занятия

СПбГЭТУ «ЛЭТИ», 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «Криптография и криптографические протоколы» к лекции «**Введение**»

_____ учебная группа "_____"_____ _____ г. аудитория №____

Учебное время **- 1 час**

1. **Вид занятия: Лекция**
2. **ТЕМА: Введение**
3. **Тема занятия:** Ведение. Основные принципы криптографии и криптографические протоколы.

Целевая установка: ознакомить студентов с целями, структурой, объемом, контрольными мероприятиями по изучаемой дисциплины.

4. **Основные вопросы занятия и планируемое время**

Вводная часть	5 мин.
Объявление темы, цели и порядка проведения занятия	
Выдача раздаточных материалов (электронные материалы, ссылки)	
Основная часть	35 мин.
1. Цели, задачи, контрольные мероприятия по изучаемой дисциплине	10 мин.
2. Основные принципы построения защищенных систем	25мин.
Заключительная часть	5 мин.

Контрольные вопросы

Подведение итогов занятия

Задание на самостоятельную работу.

3. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

Литература для самостоятельной подготовки

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Криптография и криптографические протоколы».

Методические приемы

1. Использование комплекта слайдов по теме занятия.

2. Использование раздаточного материла: (электронные материалы, ссылки).
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

Контрольные вопросы по пройденному материалу и теме занятия
(с учетом применения соответствующих ТСО)

Задание на самостоятельную работу:
Изучение основных понятий, используемых в криптографии, знакомство с литературой, изучение материалов, представленных на лекции.

План составила
доцент кафедры ИБ

А.Б. Левина

"____" _____ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине «Криптография и криптографические протоколы» к лекции «Симметричное шифрование»

_____ учебная группа "_____"_____ _____ г. аудитория №____

Учебное время – 3 часа

1. **Вид занятия: Лекция**
2. **ТЕМА: Симметричное шифрование**
3. **Тема занятия:** Основные алгоритмы симметричного шифрования.

Целевая установка: Рассмотрение основных алгоритмов блочного и поточного симметричного шифрования (DES, Rijndael, A5), изучены проблема распределения и аутентификации секретных ключей. Рассмотрены протоколы передачи ключей через ЦД, схемы построения ключа. Изучены пороговые схемы разделения секрета на основе китайской теоремы об остатках и схема Шамира, построение протоколов шифрования на основе пороговых схем разделения секрета.

4. **Основные вопросы занятия и планируемое время**

Вводная часть	10 мин.
Объявление темы, цели и порядка проведения занятия	
Выдача раздаточных материалов (электронные материалы, ссылки)	
Основная часть	125 мин.
1. Принципы работы симметричных алгоритмов шифрования, знакомство с основными алгоритмами	60 мин.
2. Алгоритмы распределения ключей	40 мин.
3. Пороговые схемы разделения секрета	20 мин.
Заключительная часть	5 мин.
Контрольные вопросы	
Подведение итогов занятия	
Задание на самостоятельную работу.	

5. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

Литература для самостоятельной подготовки

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Криптография и криптографические протоколы».

Методические приемы

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материла: (электронные материалы, ссылки).
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

Контрольные вопросы по пройденному материалу и теме занятия

(с учетом применения соответствующих ТСО)

Задание на самостоятельную работу:

Изучить:

1. Материалы, представленные на лекции.
2. Литературу, рекомендованную во время лекции.

План составила
доцент кафедры ИБ

А.Б. Левина

"____" _____ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине «Криптография и криптографические протоколы» к лекции «Асимметричное шифрование»

_____ учебная группа "_____"_____ _____ г. аудитория №_____

Учебное время **– 3 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА:** «Асимметричное шифрование»
3. **Тема занятия:** Принципы построения алгоритмов асимметричного шифрования

Целевая установка: Рассмотреть основные задачи ловушки, используемые в криптографии, принципы построения задач ловушек, их применимость. Протоколы асимметричного шифрования, алгоритм RSA, его сферы использования, сравнение с другими алгоритмами асимметричного шифрования.
Алгоритм рюкзак, криптосистема Рабина, криптосистема Эль Гамаль, их сферы применимость в различных протоколах.
Сравнение протоколов, использующих асимметричное и симметричное шифрование.
Основные критерии выбора алгоритмов для дальнейшего построения протокола. Требование контроля корректности формирования открытого ключа.

4. Основные вопросы занятия и планируемое время

Вводная часть 10 мин.
Объявление темы, цели и порядка проведения занятия
Выдача раздаточных материалов (электронные материалы, ссылки)
Основная часть 125 мин.

1. Алгоритмы асимметричного шифрования, задачи ловушки, принципы построения 40 мин.
2. Основные алгоритмы асимметричного шифрования (RSA, Эль-Гамаль, Алгоритм рюкзак, криптосистема Рабина) 40 мин.
3. Сравнение с симметричным шифрованием и правила выбора ключа 40 мин.

Заключительная часть 5 мин.

Контрольные вопросы
Подведение итогов занятия
Задание на самостоятельную работу.

5. Перечень применяемых наглядных пособий и технических средств

ПЭВМ, проектор, экран.
Опорный конспект.

Литература для самостоятельной подготовки

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Криптография и криптографические протоколы».

Методические приемы

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материла: (электронные материалы, ссылки).
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

Контрольные вопросы по пройденному материалу и теме занятия
(с учетом применения соответствующих ТСО)

Задание на самостоятельную работу:

Изучить:

1. Материалы, представленные на лекции.
2. Литературу, рекомендованную во время лекции.

План составила
доцент кафедры ИБ

А.Б. Левина

"____" _____ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине «Криптография и криптографические протоколы» к лекции «Протоколы гибридного шифрования»

_____ учебная группа "_____"_____ _____ г. аудитория №____

Учебное время **– 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Протоколы гибридного шифрования»**
3. **Тема занятия:** Основные принципы построения гибридных криптосистем.

Целевая установка: Основные принципы и суть гибридного шифрования, протокол передачи ключей Диффи-Хеллмана и протоколы гибридного шифрования на основе алгоритма Диффи-Хеллмана. Изучение протоколов SSL/TLS как одних из наиболее демонстративных систем гибридного шифрования, принципы их «сбора».

Основные вопросы занятия и планируемое время

Вводная часть	5 мин.
Объявление темы, цели и порядка проведения занятия	
Выдача раздаточных материалов (электронные материалы, ссылки)	
Основная часть	80 мин.
1. Понятие гибридной криптосистемы	20 мин.
2. Протокол Диффи-Хеллмана	20 мин.
3. Протокол SSL/TLS	40 мин.
Заключительная часть	10 мин.

Контрольные вопросы

Подведение итогов занятия

Задание на самостоятельную работу.

4. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

Литература для самостоятельной подготовки

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Криптография и криптографические протоколы».

Методические приемы

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материла: (электронные материалы, ссылки).
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

Контрольные вопросы по пройденному материалу и теме занятия
(с учетом применения соответствующих ТСО)

Задание на самостоятельную работу:

Изучить

1. Материалы, представленные на лекции.
2. Литературу, рекомендованную во время лекции.

План составила
доцент кафедры ИБ

А.Б. Левина

"____" _____ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине «Криптография и криптографические протоколы» к лекции «Протоколы аутентификации»

_____ учебная группа "_____"_____ _____ г. аудитория №____

Учебное время **– 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА:** «Протоколы аутентификации»
3. **Тема занятия:** Изучение задачи аутентификации, как одной из составных частей криптопротокола.

Целевая установка: аутентификация пользователя и информации, простая и строгая аутентификация, достоинства и недостатки, принципы выбора алгоритма аутентификации при построении протокола.
Изучение основных понятия электронной цифровой подписи (ЭЦП), использование RSA для ЭЦП. Изучение работы подписи DSA. Изучение работы и принципы построения хэшфункий, как основного примитива, используемого при построении ЭЦП. Изучение протокола «рукопожатия», протоколы установления подлинности.
Протоколы «рукопожатия» с использованием симметричных и асимметричных алгоритмов.

4. Основные вопросы занятия и планируемое время

Вводная часть	5 мин.
Объявление темы, цели и порядка проведения занятия	
Выдача раздаточных материалов (электронные материалы, ссылки)	
Основная часть	80 мин.
1. Понятие аутентификации	20 мин.
2. Основные понятия ЭЦП	20 мин.
3. Принцип работы хэш-функций	20 мин.
4. Протоколы рукопожатия	20 мин.
Заключительная часть	5 мин.
Контрольные вопросы	
Подведение итогов занятия	
Задание на самостоятельную работу.	

Перечень применяемых наглядных пособий и технических средств
ПЭВМ, проектор, экран.
Опорный конспект.

5. Литература для самостоятельной подготовки

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Криптография и криптографические протоколы».

Методические приемы

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материла: (электронные материалы, ссылки).
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

Контрольные вопросы по пройденному материалу и теме занятия
(с учетом применения соответствующих ТСО)

Задание на самостоятельную работу:

Изучить:

1. Материалы, представленные на лекции.
2. Литературу, рекомендованную во время лекции.

План составила
доцент кафедры ИБ

А.Б. Левина

"____" _____ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине «Криптография и криптографические протоколы» к лекции «Протоколы индивидуальной и коллективной цифровой подписи»

_____ учебная группа "_____"_____ _____ г. аудитория №____

Учебное время **– 2 час**

1. **Вид занятия: Лекция**
2. **ТЕМА:** «Протоколы индивидуальной и коллективной цифровой подписи»
3. **Тема занятия:** Основные принципы построения индивидуальной и коллективной подписи.

   Целевая установка: ознакомить студентов с протоколами мультиподписи, знакомство с коллективной и композиционной подписью. Целостность коллективной подписи, атаки на протоколы коллективной подписи.
4. **Основные вопросы занятия и планируемое время**

Вводная часть	5 мин.
Объявление темы, цели и порядка проведения занятия	
Выдача раздаточных материалов (электронные материалы, ссылки)	
Основная часть	80 мин.
1. Понятие мультиподписи	15 мин.
2. Протоколы мультиподписи	15 мин.
3. Протоколы коллективной и композиционной подписи	25 мин.
4. Атаки на протоколы коллективной подписи	25 мин.
Заключительная часть	5 мин.

Контрольные вопросы

Подведение итогов занятия

Задание на самостоятельную работу.

5. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

Литература для самостоятельной подготовки

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Криптография и криптографические протоколы».

Методические приемы

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материла: (электронные материалы, ссылки).
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

Контрольные вопросы по пройденному материалу и теме занятия
(с учетом применения соответствующих ТСО)

Задание на самостоятельную работу:

1. Материалы, представленные на лекции.
2. Литературу, рекомендованную во время лекции.

План составила
доцент кафедры ИБ

А.Б. Левина

"____" _____ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине «Криптография и криптографические протоколы» к лекции «**Криптоанализ и криптостойкость** »

_____ учебная группа "_____"_____ _____ г. аудитория №____

Учебное время **– 3 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Криптоанализ и криптостойкость».**
3. **Тема занятия:** Основные методы криптоанализа.

Целевая установка: ознакомить студентов с основными понятиями криптоанализа, криптоатак на пройденные алгоритмы/протоколы, классическим криптоанализом, навыкиамми для нахождения уязвимостей в криптоалгоритмах/криптомодулях.
Атаки по сторонним каналам, основные понятия и принципы, изучение наиболее известных и перспективных атак. Атаки по акустике, электромагнитному излучению, времени. Способы защиты от данных атак.

Основные вопросы занятия и планируемое время

Вводная часть	5 мин.
Объявление темы, цели и порядка проведения занятия	
Выдача раздаточных материалов (электронные материалы, ссылки)	
Основная часть	130 мин.
1. Основные понятия криптоанализа и криптоатак	20 мин.
2. Классический криптоанализ	30 мин.
3. Атаки по сторонним каналам	50 мин.
4. Методы защиты	10 мин.
Заключительная часть	10 мин.

Контрольные вопросы
Подведение итогов занятия
Задание на самостоятельную работу.

4. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.
Опорный конспект.

Литература для самостоятельной подготовки

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Криптография и криптографические протоколы».

Методические приемы

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материла: (электронные материалы, ссылки).
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

Контрольные вопросы по пройденному материалу и теме занятия
(с учетом применения соответствующих ТСО)

Задание на самостоятельную работу:

1. Материалы, представленные на лекции.
2. Литературу, рекомендованную во время лекции.

План составила
доцент кафедры ИБ

А.Б. Левина

"____" _____ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине «Криптография и криптографические протоколы» к лекции «**Заключение**»

_____ учебная группа "_____"_____ _____ г. аудитория №____

Учебное **время - 1 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Заключение»**
3. **Тема занятия: Подведение итогов, разбор направлений для дальнейших научных исследований, обсуждение курса.**

Целевая установка: Обсудить перспективы дальнейших исследований.

Основные вопросы занятия и планируемое время

Вводная часть	5 мин.
Объявление темы, цели и порядка проведения занятия	
Выдача раздаточных материалов (электронные материалы, ссылки)	
Основная часть	40 мин.
1. Обсуждение пройденного материала	20 мин.
2. Обсуждение перспективных дальнейших исследований	20 мин.
Заключительная часть	5 мин.

Контрольные вопросы

Подведение итогов занятия

Задание на самостоятельную работу.

1. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

Литература для самостоятельной подготовки

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Криптография и криптографические протоколы».

Методические приемы

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материла: (электронные материалы, ссылки).
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

Контрольные вопросы по пройденному материалу и теме занятия (с учетом применения соответствующих ТСО)

Задание на самостоятельную работу:

1. Материалы, представленные на лекции.
2. Литературу, рекомендованную во время лекции.

План составила
доцент кафедры ИБ

А.Б. Левина

"____" _____ 2022 г.