СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Методические рекомендации и план проведения занятия

СПбГЭТУ «ЛЭТИ», 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции № «**Основные принципы построения защищенных систем**»

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

Учебное время **– 1 час**

1. **Вид занятия: Лекция**
2. **ТЕМА: Введение**
3. **Тема занятия:** Ведение. Основные принципы построения защищенных систем.

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.
Цели, задачи, контрольные мероприятия по изучаемой дисциплине	10 мин.
Основные принципы построения защищенных систем	25мин.
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 «Основы построения защищенных компьютерных сетей».

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 Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской федерации и обеспечению их функционирования».

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции«**Виды нарушений сетевой безопасности**»

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

Учебное время **– 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: Виды нарушений сетевой безопасности**
3. **Тема занятия:** Модель угроз и модель нарушителя информационной безопасности компьютерной сети. Сетевые атаки. Основные этапы разработки проектных решений по системам обеспечения информационной безопасности на базе компьютерных сетей.

Целевая установка: ознакомить студентов с этапами разработки проектных решений по системам обеспечения информационной безопасности сети.

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 75 мин.

1. Модель угроз и модель нарушителя информационной безопасности компьютерной сети. Сетевые атаки 30 минут
2. Формирование требования к средствам защиты при построении защищённых компьютерных сетей 20 минут
3. Основные этапы разработки проектных решений по системам обеспечения информационной безопасности на базе компьютерных сетей… 25 минут

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 «Основы построения защищенных компьютерных сетей».

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. ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт российской федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.
2. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.
3. ГОСТ Р ИСО/МЭК 27033-4-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности" утвержден приказом Росстандарта от 19 мая 2021 года N 391-ст.
4. ГОСТ Р 56045-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности" утвержден приказом Росстандарта от 20 мая 2021 года N 421-ст.
5. 1Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции «**Сетевые протоколы передачи информации**»

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

Учебное время **– 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Сетевые протоколы передачи информации»**
3. **Тема занятия:** Способы и основные протоколы передачи данных по сети.

Целевая установка: ознакомить студентов с основными способами передачи данных по сети, применением эталонной модели взаимодействия открытых систем (ISO OSI), основными уязвимостями стека протоколов TCP/IP.

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	75 мин.
1. Способы передачи данных по сети	5 мин.
2. Эталонная модель взаимодействия открытых систем (ISO OSI). Уровни и протоколы	15 мин.
3. Стек протоколов TCP/IP	55 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 «Основы построения защищенных компьютерных сетей».

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 особенности функционирования сетевого оборудования для построения сегментированной сети (сетевые адаптеры, коммутаторы, маршрутизаторы) согласно стеку протокола TCP/IP.

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции № «**Межсетевое экранирование**»

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

Учебное время **- 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА:** «Межсетевое экранирование»
3. **Тема занятия:** Основные принципы построения защищенных систем на базе межсетевых экранов.

Целевая установка: ознакомить студентов с основными компонентами и особенностями функционирования межсетевых экранов. Сформировать представление о правилах фильтрации сетевого контента и способах ограничения доступа к сетевой инфраструктуре.

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. Основные компоненты межсетевых экранов и особенности их функционирования. Классификации межсетевых экранов	20 мин.
2. Технология NAT	20 мин.
3. Правила фильтрации сетевого контента	20 мин.
4. Способы ограничения доступа к сетевой инфраструктуре	20 мин.
Заключительная часть	10 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 «Основы построения защищенных компьютерных сетей».

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. Приказ ФСТЭК № 17 от 11 февраля 2013 года
2. Приказ ФСТЭК № 21 от 18 февраля 2013 года
3. Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждёнными Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119
4. Приказ ФСТЭК России от 9 февраля 2016 г. №9 Требования к межсетевым экранам
5. Информационное сообщение ФСТЭК «Об утверждении требований к межсетевым экранам» от 28 апреля 2016 г. N 240/24/1986

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции «**Виртуальные частные сети**»

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

Учебное время **– 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Виртуальные частные сети»**
3. **Тема занятия:** Туннелирование. Основные принципы построения защищенных каналов передачи данных.

Целевая установка: ознакомить студентов с технологиями туннелирования и построения VPN на различных уровнях стека протокола TCP/IP.

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. Определение виртуальной частной сети (VPN). Преимущества VPN	10 мин.
2. Типы VPNсетей	10 мин.
3. Протоколы PPTP, L2TP принцип работы	20 мин.
4. Протоколы IPSec	20 мин.
5. Сервисы безопасности IPSec	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 «Основы построения защищенных компьютерных сетей».

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. Особенности функционирования протокола TSL.
2. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (утверждены приказом ФСТЭК России от 30 июля 2018 г).

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции «**Протоколы идентификации, аутентификации и авторизации**»

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

Учебное время **- 1 час**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Протоколы идентификации, аутентификации и авторизации»**
3. **Тема занятия:** Основные принципы аутентификации для защищенных каналов передачи данных.

Целевая установка: ознакомить студентов с методами аутентификации на базе технологии AAA.

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. Средства и методы хранения и передачи аутентификационной информации	5 мин.
2. Протоколы PAP, CHAP	5 мин.
3. Аутентификация в протоколе HTTP	5 мин.
4. Аутентификация NAS. Протокол DHCP	5 мин.
5. Протокол RADIUS	10 мин.
6. Протокол Kerberos	5 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 «Основы построения защищенных компьютерных сетей».

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 особенности работы протокола TACACS+.

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции «**Средства и методы интеллектуального обнаружения и предотвращения вторжений**»

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

Учебное время **– 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Средства и методы интеллектуального обнаружения и предотвращения вторжений».**
3. **Тема занятия:** Архитектура систем мониторинга сети.

Целевая установка: ознакомить студентов с архитектурой систем обнаружения вторжения, в том числе особенностями и отличиями функционирования пассивных, активных и многоагентных систем обнаружения вторжений.

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	75 мин.
1. Актуальность. Проблемы традиционного подхода	10 мин.
2. Архитектура систем обнаружения вторжения	10 мин.
3. Пассивные и активные системы обнаружения вторжения	10 мин.
4. Системы мониторинга	10 мин.
5. Многоагентные системы	15 мин.
6. Классификация методов, применяемых в системах обнаружения вторжений	20 мин.
Заключительная часть	5 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 «Основы построения защищенных компьютерных сетей».

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 Приказ ФСТЭК России № 638 от 6 декабря 2011 года

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции «**Средства и методы интеллектуального обнаружения и предотвращения вторжений**»

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

Учебное время **– 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Средства и методы интеллектуального обнаружения и предотвращения вторжений»**
3. **Тема занятия:** Методы, применяемые для обнаружения вторжений.

Целевая установка: ознакомить студентов с методами, применяемыми в системах обнаружения вторжений. Сформировать представление о программно-конфигурируемых сетях, их целевом назначении.

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	75 мин.
1. Статистические методы оценки нарушений сетевого взаимодействия	20 мин.
2. Сигнатурные методы оценки нарушений сетевого взаимодействия	20 мин.
3. Нейросетевые методы обнаружения вторжений	10 мин.
4. Методы прогнозирования сетевого трафика	5 мин.
5. SIEM	10 мин.
6. Протокол SMNP	10 мин.
Заключительная часть	10 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 «Основы построения защищенных компьютерных сетей».

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 особенности работы методов машинного обучения: байесовский классификатор и ансамбля решающих деревьев.

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции «**Беспроводные технологии**»

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

Учебное время **– 2 часа**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Беспроводные технологии»**
3. **Тема занятия:** Основные принципы беспроводной передачи данных.

Целевая установка: формирование представлений о методах обеспечения безопасности передачи данных в беспроводных сетях.

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	75 мин.
1. Классификация беспроводных сетей передачи данных	5 мин.
2. Технология Wi-Fi. Режимы доступа к сети	25 мин.
3. Технология Wi-Fi. Вопросы безопасности и методы защиты	25 мин.
4. Технология Bluetooth.. Вопросы безопасности и методы защиты	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 «Основы построения защищенных компьютерных сетей».

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 стандарт «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей».

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.

Методические рекомендации и план проведения занятия по дисциплине «**Основы построения защищенных компьютерных сетей**» к лекции «**Модернизации объектов информатизации на базе компьютерных сетей в защищенном исполнении**»

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

Учебное время **– 1 час**

1. **Вид занятия: Лекция**
2. **ТЕМА: «Протоколы идентификации, аутентификации и авторизации»**
3. **Тема занятия:** Основные принципы аутентификации для защищенных каналов передачи данных.

Целевая установка: ознакомить студентов с методами аутентификации на базе технологии AAA.

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. Обоснование необходимости модернизации сетевой инфраструктуры	15 мин.
2. Методы реконфигурации	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 «Основы построения защищенных компьютерных сетей».

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 Приказ ФСТЭК от 29 апреля 2021 г. № 77. Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.

План составила
доцент кафедры ИБ

Р.Р. Фаткиева

"____" _____ 2021 г.