# Сетевые технологии. Рекомендации по проведению лекций.

Данные рекомендации прилагаются к презентации лекции «Сетевые технологии, атаки и аномалии».

Структура рекомендаций устроена следующим образом:

* Номер слайда
* Тезисы, рекомендуемые к обсуждению
* Дополнительная информация, ссылки на источники (опционально)

1. Тема лекции.
2. Что представлено на слайде?

Вопрос в аудиторию, рассуждения студентов, требуется для понимания общего уровня подготовки группы.

1. Модель OSI.

Рассказ на данном слайде поверхностный, для общего понимания.

<https://docs.cntd.ru/document/1200007766>

1. Модель OSI в реальности. Или Department of Defense модель TCP/IP.

Модель OSI это идеальная модель, но избыточная. Была обобщена к модели TCP/IP. Начинать рассказ следует с 4 и 1 уровня – то, что студенты «ощущают» глазами. Далее, подниматься от 4 к 1 на конкретных примерах. Коммутатор, маршрутизатор, тип управления потоками данных и порты приложений.

<https://youtu.be/BJSITWkSDQg>

1. Network Access Layer. Погружение в работу канального уровня. Что такое MAC-адрес? Где он в оборудовании и в фрейме?

<https://youtu.be/9eH16Fxeb9o?t=545>

1. Network Access Layer. Развитие соединений устройств.
2. Internet. Что такое IP-адрес? Потребность в сетях, локальные и глобальные сети. Route table.

<https://youtu.be/zeArDrC2xPg>

<https://docs.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting>

1. Internet. Как связаны IP и MAC? Устройство ARP-таблиц. Процесс ARP и RARP-запроса.

<https://youtu.be/cn8Zxh9bPio>

1. Internet. Визуализация Ucast, Bcast, Mcast. Устройство DHCP.

<https://youtu.be/e6-TaH5bkjo>

<https://youtu.be/4pkDL1pgCgQ>

<https://youtu.be/S43CFcpOZSI>

1. Transport. Различие управления пакетами при UDP и TCP. Устройство TCP. Потоки данных.

<https://youtube.com/playlist?list=PLW8bTPfXNGdAZIKv-y9v_XLXtEqrPtntm>

1. Application. Что такое порт, как он используется, стандартные протоколы по RFC 1340. Зачем нужен DNS? Устройство DNS LOOKUP.

<https://youtu.be/72snZctFFtA>

1. Application. Устройство SMTP. Различие POP3 и IMAP.

<https://youtu.be/PJo5yOtu7o8>

<https://youtu.be/SBaARws0hy4>

<https://www.javatpoint.com/simple-mail-transfer-protocol>

<https://medium.com/@jonathansychan/smtp-simple-mail-transfer-protocol-ed443b1f51d7>

<https://medium.com/@imranshaikh2124/how-smtp-works-3c5aa6e81779>

<https://postmarkapp.com/guides/everything-you-need-to-know-about-smtp>

1. Мониторинг. Варианты мониторинга сети. Устройство SNMP. Устройство Syslog.

<http://math.gsu.by/wp-content/uploads/courses/networks/r7.3.html>

<https://www.securitylab.ru/analytics/301808.php>

<https://youtu.be/2IXP0TkwNJU>

<https://youtu.be/Lq7j-QipNrI?t=17>

<https://youtu.be/BMVHHX02T4Q?t=17>

1. Основы анализа трафика. Каткий обзор инструментов для анализа. Пакетный и потоковый подход.

<https://www.tcpdump.org/>

<https://www.wireshark.org/>

<https://www.ntop.org/>

<https://zeek.org/>

<https://github.com/phaag/nfdump>

1. IDS vs IPS. Основное отличие и принцип работы.

<https://youtu.be/rvKQtRklwQ4>

<https://youtu.be/_gHMkEKGwBM?t=56>

1. DLP. Что такое DLP и зачем это необходимо.

<https://youtu.be/S-5oLGrTHcU>

<https://youtu.be/jf-GSmiQZgw>

<https://youtu.be/-Jpec7tOQqM?t=262>

1. (NextGen) SIEM. Событийный подход к данным безопасности. Инциденты. Расследование атак.

<https://youtu.be/GbFtSDnPZBQ?t=75>

<https://youtu.be/sgMxl2dmkOQ>

1. Выявление аномалий в сетевом трафике. Ошибки в передаче. Аномальное поведение систем.

<https://izv.etu.ru/assets/files/izvestiya-4_2021-36-41.pdf>

<https://www.ussc.ru/news/novosti/na-chto-sposoben-ii-v-sfere-ib/>

<http://uzulo.su/prav-inf/pdf-jpg/pi-2020-1-st7-s67-75.pdf>

1. Сетевые атаки. Некоторые виды атак, которые будут рассмотрены далее.

<https://www.smart-soft.ru/blog/tipy_setevyh_atak_i_sposoby_borjby_s_nimi/>

<http://teacherbox.ru/kompseti/pm02/2-1-25-vidyi-i-tipyi-setevyih-atak/.html>

1. Сетевые атаки (Malware). Виды Malware.

<https://www.wallarm.com/what/malware-types-and-detection>

1. Сетевые атаки (Phishing). Принцип атаки.

<https://www.wallarm.com/what/types-of-phishing-attacks-and-business-impact>

1. Сетевые атаки (SQL Injection Attack). Принцип атаки.

<https://www.acunetix.com/blog/articles/exploiting-sql-injection-example/>

<https://www.wallarm.com/what/types-of-phishing-attacks-and-business-impact>

1. Сетевые атаки (Cross-Site Scripting). Принцип атаки.

<https://www.wallarm.com/what/what-is-xss-cross-site-scripting>

1. Сетевые атаки (Denial of Service). Принцип атаки.

<https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/introduction-denial-of-service-attacks.html>

<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

<https://www.coursera.org/lecture/it-security/denial-of-service-lH7Y7>

1. Сетевые атаки (MitM). Принцип атаки.

<https://www.varonis.com/blog/man-in-the-middle-attack/>

<https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack>

<https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack>

<https://www.apriorit.com/dev-blog/723-qa-mitm-tools-for-penetration-testing-and-cybersecurity-enhancement>

1. Сетевые атаки (ARP spoofing). Принцип атаки.
2. Сетевые атаки (DNS spoofing). Принцип атаки.
3. Вопросы.