# Лабораторная работа: изучение угроз сетевой безопасности

## Задачи

**Часть 1. Изучение веб-сайта SANS**

- Откройте веб-сайт SANS и определите имеющиеся ресурсы.

**Часть 2. Определение новых угроз сетевой безопасности**

- Определите несколько потенциальных угроз сетевой безопасности с помощью веб-сайта SANS.
- Определите, какие сайты, помимо SANS, содержат информацию о сетевых угрозах.

**Часть 3. Подробное описание отдельной угрозы сетевой безопасности**

- Выберите и подробно опишите какую-либо новую угрозу сетевой безопасности.
- Расскажите об этой угрозе классу.

## Исходные данные/сценарий

Чтобы защитить сеть от атак, администратор должен определить, какие внешние угрозы представляют опасность для сети. Для определения возникающих угроз и способов их устранения можно пользоваться специализированными веб-сайтами.

Одним из наиболее известных и проверенных ресурсов для защиты компьютера и сети является веб-сайт SANS (системное администрирование, проверка, сеть, безопасность). На веб-сайте SANS доступны несколько разных ресурсов, включая список 20 основных средств контроля безопасности для эффективной киберзащиты и еженедельную новостную рассылку по вопросам безопасности @Risk: The Consensus Security Alert. В рассылке подробно рассказывается о новых сетевых атаках и уязвимостях.

В ходе лабораторной работы вам необходимо открыть и изучить веб-сайт SANS, определить новые угрозы сетевой безопасности с его помощью, посетить другие аналогичные веб-ресурсы и подготовить подробное описание отдельной сетевой атаки.

## Необходимые ресурсы

- Устройство с выходом в Интернет
- Компьютер для презентации с установленной программой PowerPoint или другой программой для презентаций.

# Часть 1: Изучение веб-сайта SANS

В части 1 вам нужно открыть веб-сайт SANS и изучить предлагаемые ресурсы.

### Шаг 1: Найдите ресурсы SANS.

Откройте веб-сайт www.sans.org в браузере. На главной странице наведите указатель мыши на меню **Resources** (Ресурсы).

Назовите три доступных ресурса.

### Шаг 2: Выберите пункт меню Top 20 Critical Controls (20 основных средств контроля безопасности).

Список **20 основных средств контроля безопасности** на веб-сайте SANS был составлен в результате совместной работы государственных и частных компаний при участии Министерства обороны, Ассоциации национальной безопасности, Центра интернет-безопасности и Института SANS. Его задачей было определение приоритетности средств контроля кибербезопасности и связанных с ними расходов для Министерства обороны. На основе этого списка правительство США разработало эффективные программы обеспечения безопасности. В меню **Resources** (Ресурсы) выберите пункт **Top 20 Critical Controls** (20 основных средств контроля безопасности).

Выберите одно из 20 средств и назовите три предложения по его реализации.

### Шаг 3: Выберите меню «Newsletters» (Новостные рассылки).

Откройте меню **Resources** (Ресурсы) и выберите пункт **Newsletters** (Новостные рассылки). Кратко опишите каждую из трёх предлагаемых рассылок.

## Часть 2: Определение новых угроз сетевой безопасности

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

### Шаг 1: Выберите раздел «Archive» (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рядом с названием @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues** (Последние важные проблемы безопасности) и **Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из новых атак. При необходимости просмотрите несколько последних выпусков рассылки.

### Шаг 2: Найдите веб-сайты, которые содержат информацию о новых угрозах безопасности.

Выясните, на каких ещё сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозах сетевой безопасности.

Назовите некоторые новые угрозы безопасности, подробно описанные на этих веб-сайтах.

## Часть 3: Подробное описание отдельной угрозы сетевой безопасности

В части 3 вы займётесь изучением отдельной сетевой атаки, а затем на основе полученной информации подготовите презентацию. Используя полученные результаты, заполните приведённую ниже форму.

### Шаг 1: Заполните приведённую ниже форму данными выбранной сетевой атаки.

| | |
|---|---|
| **Имя атаки:** | |
| **Тип атаки:** | |
| **Даты атак:** | |
| **Пострадавшие компьютеры или организации:** | |
| **Механизм атаки и её последствия:** | |
| | |
| **Способы устранения:** | |
| | |
| **Источники и ссылки на информационные ресурсы:** | |
| | |

**Шаг 2: Для завершения презентации следуйте инструкциям инструктора.**

## Вопросы на закрепление

1. Какие меры можно предпринять для защиты собственного компьютера?

2. Какие важные меры могут предпринимать компании для защиты своих ресурсов?