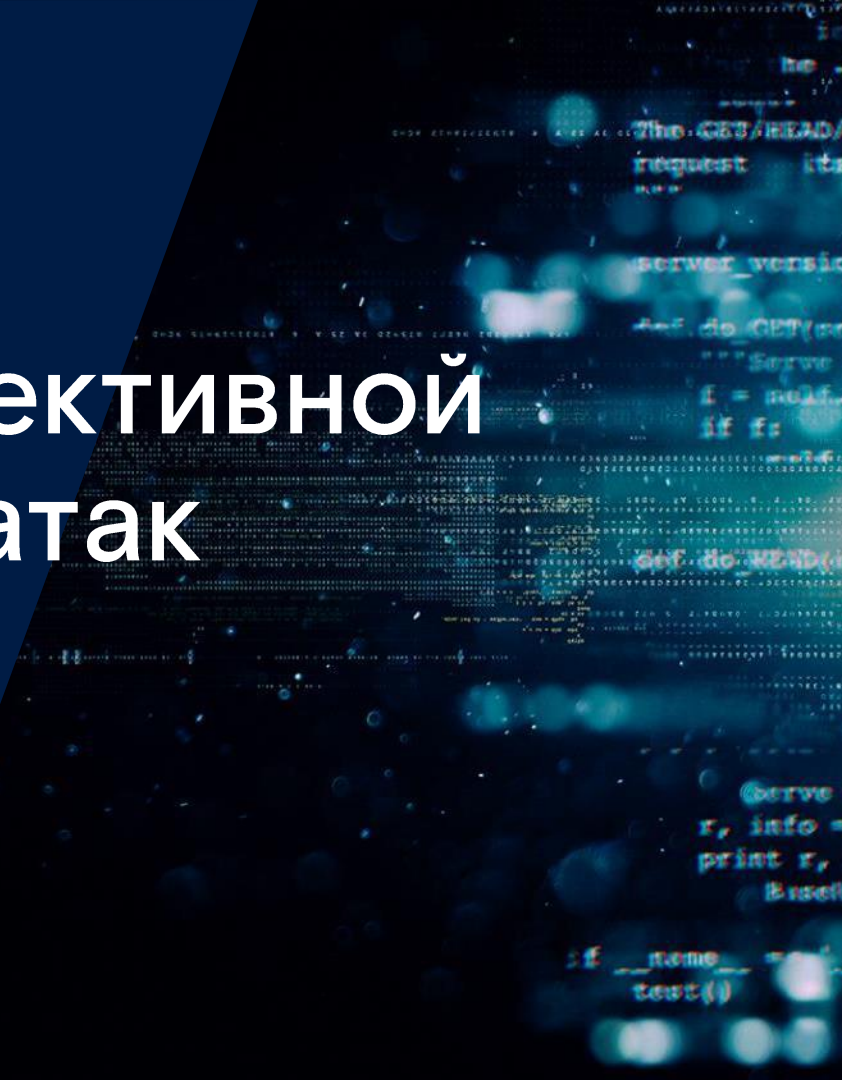


Организация эффективной защиты от DDOС атак



Актуальность защиты от DDOS атак



Взрывной рост
интернет сервисов

Удаленная работа
сотрудников

Доступный
инструментарий

Не требует высоких
компетенций

Высокопропускные
пользовательские каналы

Интересна и финансово- и
политически мотивированным
злоумышленникам

Сложная политическая ситуация

Основные подходы к построению систем защиты от DDOS

Решение On-Premise

Сервис от Интернет
провайдера

Услуга от провайдера
облачного сервиса или
хостинга

Использование
специализированных
сервисов защиты от DDOS

Специализированные средства защиты от DDOS атак

Межсетевой экран + система предотвращения атак (FW+IPS)

Системы защиты веб-приложений (WAF)

Специализированные программно-аппаратные комплексы



Ключевые моменты системы защиты от DDOS атак

Защита от DDOS атак,
как сетевого, так и
прикладного уровня

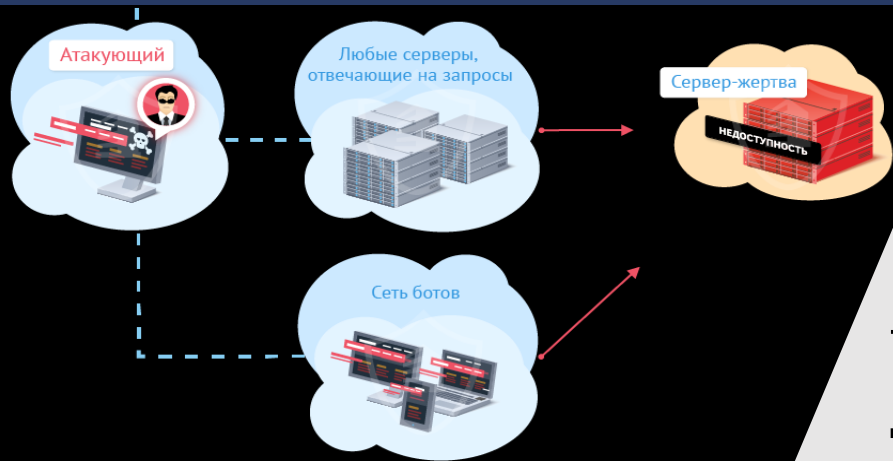
Настройки МСЭ должны
выверены

Интернет сервисы имеют
значительный запас по
мощности и ресурсам

Определены предельные
нагрузки на сервисы

Интернет каналы расширены и
зарезервированы

Тонкая настройка защиты проведена
для каждого сервиса отдельно





Ошибки тестирования систем защиты от DDOS атак

Отсутствие
тестирования

Ограниченный набор
атак

Тестовый стенд не
соответствует «бою»

Очень ограниченное время
тестирования

Отсутствие полноценного
мониторинга систем

Пассивное участие команд
провайдера и заказчика

Отсутствие анализа результатов
тестирования

Цели тестирования

Оценка эффективности

Отработка действий персонала

Выявление и устранение проблемных мест

Определение предельных нагрузок

Совершенствование процедур реагирования

Разработка тактики масштабирования ИТ-активов



Подготовка и проведение тестирования



Список узлов и атак на каждый из них

Определение условий тестирования и предельных нагрузок

Согласование работ по тестированию внутри компании

Определение ролей участников и каналов взаимодействия

Настройки средств регистрации событий и мониторинга

Фиксация действий всех участников тестирования

Фиксация результатов каждого этапа тестирования

Спасибо за внимание!

Скородумов Анатолий Валентинович

E-mail: skorodumov@mail.ru

