СПЕКТР ФОРУМ 25-26.10 2022

spectr-forum.com

Готовность российского сегмента сети «Интернет» к автономной работе. Роль ЦМУ ССОП в обеспечении устойчивости ССОП

Хуторцев Сергей Сергеевич
Директор ЦМУ ССОП
ФГУП «ГРЧЦ»

Функции и задачи ЦМУ ССОП

ОБЕСПЕЧЕНИЕ УСТОЙЧИВОГО, БЕЗОПАСНОГО И ЦЕЛОСТНОГО ФУНКЦИОНИРОВАНИЯ РОССИЙСКОГО СЕГМЕНТА СЕТИ «ИНТЕРНЕТ» И СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

МОНИТОРИНГ РЕСУРСОВ СВЯЗИ

ВЫЯВЛЕНИЕ УГРОЗ ЦЕЛОСТНОСТИ, УСТОЙЧИВОСТИ И БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ССОП НА ТЕРРИТОРИИ РФ

ЗАМЕЩАЮЩАЯ ИНФРАСТРУКТУРА

НАЦИОНАЛЬНАЯ СИСТЕМА ДОМЕННЫХ ИМЕН (НСДИ)

РЕЕСТР АДРЕСНО-НОМЕРНЫХ РЕСУРСОВ (РАНР)

АКТИВНОЕ РЕАГИРОВАНИЕ

УПРАВЛЕНИЕ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ (ТСПУ)

БОРЬБА С МОШЕННИЧЕСТВОМ В ТЕЛЕФОННЫХ СЕТЯХ

СИСТЕМА «АНТИФРОД»

КОНТРОЛЬ СИМ-КАРТ

УЧЕТ РЕСУРСОВ СВЯЗИ	МОНИТОРИНГ	ВЫЯВЛЕНИЕ УГРОЗ	ИНФОРМИРОВАНИЕ ОС	ПЕРЕДАЧА УКАЗАНИЙ	ЦЕНТР КООРДИНАЦИИ
• Сетевая инфраструктура • Трансграничные ЛС • Точка обмена трафиком • Используемая IP-адресация	• Маршрутной информации • Данных по интернет-трафику • Доступности IP-ресурсов • Доступности веб-ресурсов	• Управление ТСПУ • Противодействие DDoS • Блокировка запрещенных и вредоносных ресурсов	• О выявленных угрозах и уязвимостях • Об угрозах нарушения маршрутизации	• Операторам связи • Иным владельцам АС	• Межоператорское взаимодействие при выявлении угроз и аварий на ССОП

Меры ЦМУ ССОП

В рамках обеспечения устойчивости, безопасности и целостности ССОП

СПЕКТР ФОРУМ 25-26.10 2022
spectr-forum.com

1 УСИЛЕННЫЙ КРУГЛОСУТОЧНЫЙ КОНТРОЛЬ

Организован усиленный круглосуточный мониторинг и реагирование на инциденты информационной безопасности

2 ОПЕРАТИВНОЕ ПРОТИВОДЕЙСТВИЕ УГРОЗАМ

На ТСПУ применяются меры по выявлению и подавлению DDoS-атак, блокировке ресурсов, используемых для реализации и координации компьютерных атак

3 МОНИТОРИНГ ЗНАЧИМЫХ РЕСУРСОВ

Ведется мониторинг и анализ доступности ключевых ресурсов

4 ОПОВЕЩЕНИЯ И УВЕДОМЛЕНИЯ

Оповещение ОС, специалистов центров кибербезопасности и владельцев информационных ресурсов о выявлении критических уязвимостей и наличии потенциальных угроз

5 КОРРЕКТНЫЕ СПИСКИ АС И IP-АДРЕСОВ

Списки оперативно актуализируются и направляются ответственным подразделениям ИБ владельцев ресурсов и операторов связи

6 000+
РЕСУРСОВ ЗАЩИЩЕНО ОТ ВНЕШНЕГО ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ПОСРЕДСТВОМ ФИЛЬТРАЦИИ ИНОСТРАННОГО ТРАФИКА НА ТСПУ

6 500+
АНОМАЛИЙ ТИПА «ПЕТЛЯ ЧЕРЕЗ ГРАНИЦУ РФ» УСТРАНЕНО

60+
РЕСУРСОВ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПОДМЕНЫ АБОНЕНТСКОГО НОМЕРА, ЗАБЛОКИРОВАНО

30+
ОПЕРАТИВНЫХ УКАЗАНИЙ НАПРАВЛЕНО ОПЕРАТОРАМ СВЯЗИ О ВЫЯВЛЕННЫХ УГРОЗАХ

40+
DDoS-АТАК ЗАФИКСИРОВАНО И ОТРАБОТАНО

ПОЧТА РОССИИ

Оперативное взаимодействие

Статистика использования
Информационных систем ЦМУ ССОП

СПЕКТР ФОРУМ 25-26.10 2022
spectr-forum.com

ЗАМЕЩАЮЩАЯ ИНФРАСТРУКТУРА

РЕЕСТР АДРЕСНО-НОМЕРНЫХ РЕСУРСОВ

- **97%** владельцев автономных систем представили информацию
- **70 млн** запросов в публичному Web-WHOIS сервису РАНР за год
- **300 тыс.** количество скачиваний дампов базы данных РАНР за год

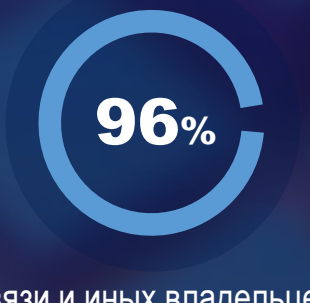
НАЦИОНАЛЬНАЯ СИСТЕМА ДОМЕННЫХ ИМЕН

- **10 млрд** среднее количество запросов в сутки
- **180 тыс.** запросов в секунду
- **1 млн** уникальных пользователей (уникальных IP-адресов)

ПОДКЛЮЧЕНИЕ К МОНИТОРИНГУ

Операторов связи и иных владельцев автономных систем подключены к мониторингу ЦМУ ССОП

СВЕДЕНИЯ ПО ИНФРАСТРУКТУРЕ



операторов связи и иных владельцев автономных систем предоставили информацию по инфраструктуре сетей связи

Статистика

Автоматизированная система обеспечения безопасности российского сегмента сети «Интернет» (АСБИ)

СПЕКТР ФОРУМ 25-26.10 2022
spectr-forum.com

ПОКРЫТИЕ ОБОРУДОВАНИЕМ ТСПУ РОССИЙСКОЙ ФЕДЕРАЦИИ

СТАТИСТИКА ТРАФИКА, ПРОХОДЯЩЕГО ЧЕРЕЗ ТСПУ

АКТИВНОЕ РЕАГИРОВАНИЕ НА УГРОЗЫ УСТОЙЧИВОСТИ И БЕЗОПАСНОСТИ

В 2022 году успели помочь в отражении DDoS-атак

65

ОРГАНИЗАЦИЯМ

в том числе Почта России, Министерство Культуры, РЖД

В рамках противодействия угрозам безопасности ограничено

67

СЕРВИСОВ

включая средства обхода блокировок

Итоги учений 2022

СПЕКТР ФОРУМ 25-26.10 2022
spectr-forum.com

ТРЕБУЕТСЯ ОБЕСПЕЧИТЬ:

НАДЕЖНОСТЬ ФУНКЦИОНИРОВАНИЯ РЕСУРСОВ

- Независимость от зарубежных библиотек
- Приоритетное использование TLS-сертификатов, выпущенных российскими удостоверяющими центрами, в том числе с использованием российской криптографии
- Создание распределенной иерархической системы российских удостоверяющих центров

ПРОТИВОДЕЙСТВИЕ DDOS-АТАКАМ

- Создание на базе ТСПУ национальной системы противодействия DDoS-атакам
- Улучшение координации операторов связи, владельцев ресурсов и организаций по кибербезопасности

ПОВЫШЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ

- Ограничение возможности сканирования ресурсов и систем из-за рубежа
- Создание доверенного сервиса по проведению аудита безопасности
- Создание информационной системы о страновой принадлежности сетей связи
- Внедрение механизмов проверки корректности маршрутизации с использованием PAHP, в том числе на основе открытых ключей (RPKI)

Публичный портал ЦМУ ССОП

СПЕКТР ФОРУМ 25-26.10 2022
spectr-forum.com

2022 год

Looking Glass

Просмотр маршрутной информации, накопленной системой мониторинга маршрутов трафика в сети «Интернет» ИС «ЦМУ ССОП»

Доступность сервисов

Анализ доступности ресурсов средствами мониторинга ЦМУ ССОП.
Прием информации от пользователей сети «Интернет»

Публикации

Общедоступная информация
(отчеты по результатам деятельности ЦМУ ССОП)

2023 год

Оценка безопасности почтовых серверов

Оценка безопасности web-серверов

Развитие ЦМУ ССОП

- РАЗВИТИЕ УЖЕ СОЗДАННЫХ ПОДСИСТЕМ В СОСТАВЕ ИС «ЦМУ ССОП»
- СОЗДАНИЕ НАЦИОНАЛЬНОЙ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ DDoS-АТАКАМ
- ВВОД В ЭКСПЛУАТАЦИЮ СИСТЕМЫ АНТИФРОД
- СОЗДАНИЕ СИСТЕМЫ МОНИТОРИНГА КАЧЕСТВА УСЛУГ СВЯЗИ

СПЕКТР ФОРУМ 25-26.10 2022
spectr-forum.com

Благодарю за внимание!

Хуторцев Сергей Сергеевич
Директор ЦМУ ССОП
ФГУП «ГРЧЦ»

СПЕКТР ФОРУМ 25-26.10 2022
spectr-forum.com