SOLAR

W: RT-SOLAR.RU

БЕСПЕРЕБОЙНОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ В ЕДИНЫЙ ДЕНЬ ГОЛОСОВАНИЯ

ЕДИНЫЙ ДЕНЬ ГОЛОСОВАНИЯ

18·19·20

СЕНТЯБРЯ 2026

Игорь Ляпунов

Генеральный директор ГК «Солар»

«Три дня мы фактически находились в состоянии непрерывного киберпротивостояния. Это была проверка на прочность всей системы — от отдельных сервисов до ключевой телекоммуникационной инфраструктуры страны. Но ни один из этих ударов не привёл к нарушению работы защищаемых систем.»

ИСТОРИЯ УСПЕХА

ЦЕНТР ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ SOLAR JSOC

Масштаб угроз

Что обрушилось на инфраструктуру выборов за три дня

Контекст: мощность и количество атак превысили показатели предыдущего Единого дня голосования и президентских выборов 2024 года. Атаки вели профессиональные группировки, применявшие ИИ-инструменты для автоматизации части процессов.

- источники трафика — IP-пространства более 30 стран
- цели: ЕСИА, «Госуслуги», ДЭГ, ресурсы ЦИК, инфраструктура «Ростелекома»
- после отражения основных атак удары перенесли на сторонние системообразующие организации

DDoS-волны по ключевым целям



Данные по четырём ключевым целям; всего за три дня отражено более 3 тыс. волн DDoS-атак.

Читать пресс-релиз

Данные о проекте

Круглосуточная киберзащита дистанционного электронного голосования и ресурсов ЦИК

ГК «Солар» совместно с «Ростелекомом» выступила провайдером киберзащиты федеральных систем голосования. Подготовка стартовала в мае 2026 г., активная фаза — 18–20 сентября 2026 г.

О JSOC: первый коммерческий SOC в России, работает с 300+ заказчиков

- входит в топ-5 коммерческих SOC Европы
- 14+ лет опыта на рынке оказания ИБ-услуг
- №1 в списке исследователей по рейтингу ФСТЭК России
- имеет 6 центров SOC на территории России, расположенных во всех часовых поясах страны

О Solar AURA: центр мониторинга внешних цифровых угроз — выявляет и блокирует поддельные ресурсы, имитирующие сайты ЦИК и сервисы голосования

Единый штаб: защита велась в общем штабе по кибербезопасности под руководством и во взаимодействии с ФСБ России, НКЦКИ, ФСТЭК России и ГРЧЦ

Узнать подробнее

3 000+

волн DDoS-атак отражено

1,7 Тбит/с

пиковая мощность DDoS-атаки

170 млн+

вредоносных воздействий на веб-сервисы заблокировано

900+

экспертов Solar JSOC из разных часовых поясов

сотни

поддельных ресурсов выявлено и заблокировано

0

атак, приведших к недоступности или снижению производительности

SOLAR

Цель

Обеспечить бесперебойное электронное голосование под массированными кибератаками и не допустить компрометации, подмены или раскрытия результатов до завершения официальной процедуры

Задача

- Обеспечить непрерывную работу ДЭГ, ресурсов ЦИК и инфраструктуры электронного правительства под массированными атаками
- Не допустить компрометации систем, подмены или раскрытия результатов голосования
- Защитить веб-сервисы vybory.gov.ru, izbirkom.ru и сайт ЦИК
- Выявить и остановить попытки проникновения во внутреннюю инфраструктуру
- Пресечь деятельность поддельных сайтов, имитирующих ресурсы ЦИК и ДЭГ
- Скоординировать действия всех участников защиты

Решение

- С мая 2026 г. — многоуровневая оценка защищённости ДЭГ и создание оперативного штаба
- Solar JSOC: круглосуточный мониторинг аномалий в поведении систем и пользователей, блокировка атак и оперативное реагирование силами 900+ экспертов
- Эшелонированная фильтрация DDoS совместно с «Ростелекомом»: трансграничные маршрутизаторы, фильтры НСПА, магистральный комплекс защиты
- Solar AURA совместно с НКЦКИ — поиск и блокировка поддельных сайтов
- Единый штаб кибербезопасности при участии ФСБ, НКЦКИ, ФСТЭК и ГРЧЦ

Результат

- Ни одна атака не привела к недоступности или снижению производительности защищаемых систем
- Заблокировано 170 млн+ воздействий; предотвращено развитие инцидента со сканированием и подбором учётных данных к коммутаторам магистральной сети
- Заблокированы сотни поддельных ресурсов
- Расследование подтвердило отсутствие взлома инфраструктуры ЦИК — данные выборного процесса защищены



SOLAR

W rt-solar.ru
E solar@rt-solar.ru