РАСШИРЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ ДОМЕННЫХ ИМЕН

ПОМОГИТЕ ЗАЩИТИТЬ ИНФОРМАЦИЮ, КОТОРУЮ ВЫ ПЕРЕСЫЛАЕТЕ ЧЕРЕЗ ИНТЕРНЕТ

Протокол DNSSEC (расширения безопасности системы доменных имен) позволяет владельцам использовать метод **цифровой подписи** информации, которую они вносят в систему доменных имен (DNS). Это обеспечивает защиту потребителей, так как данные DNS, которые подверглись искажению, случайно или со злым умыслом, до них не доходят.

ХРОНОЛОГИЯ

Когда DNS создавалась, вопрос безопасности не был главным. Злоумышленники могли **компрометировать ваши DNS-сообщения** и **перенаправлять ваши сообщения на другой адрес** в интернете вместо того, на который вы их отправляли.

Техническое сообщество DNS выработало окончательное решение этой проблемы – DNSSEC. DNSSEC укрепляет процедуры проверки подлинности данных в DNS при помощи цифровых подписей, основанных на **криптографии открытого ключа.**

DNSSEC В ДЕЙСТВИИ

Для правильной работы протокола DNSSEC должны быть задействованы обе его стороны.

Владельцы доменов, которые отвечают за публикацию информации в DNS, должны **проследить за тем, чтобы их данные DNS были подписаны DNSSEC.**

Сетевые операторы должны **включить DNSSEC-валидацию на тех своих резолверах, которые обрабатывают запросы к DNS.**

ПРЕИМУЩЕСТВА РАЗВЕРТЫВАНИЯ DNSSEC

Помогает защитить интернет, конечных пользователей, компании, организации и органы государственной власти.

Снижает уязвимость к атакам.

Способствует инновациям. DNSSEC позволяет проверять и защищать данные DNS что в свою очередь создает доверие к данным в приложениях за пределами DNS.

ПРЕДЛОЖИТЕ ВАШИМ СЕТЕВЫМ ОПЕРАТОРАМ ВКЛЮЧИТЬ DNSSEC

ICANN

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ О DNSSEC ДОСТУПНА ПО АДРЕСАМ:

http://go.icann.org/OCTOpublications
http://go.icann.org/DNSSEC

Подготовлено отделом по связям с общественностью ICANN | май 2020 года