

Нужна помощь?



tld-ops@lists.dns-oarc.net

TLD-OPS — это созданное национальными доменами верхнего уровня в своих интересах сообщество для реагирования на инциденты, которое объединяет лиц, отвечающих за общую безопасность и стабильность своих ссTLD.

Цель сообщества TLD-OPS состоит в том, чтобы позволить операторам национальных доменов верхнего уровня (ссTLD) по всему миру совместно наращивать возможности реагирования на инциденты. Мы поставили перед собой задачу дополнительного повышения уровня безопасности и стабильности служб ссTLD (DNS и регистрация) во всем мире и инфраструктуры интернета в целом. Сообщество TLD-OPS открыто для всех ссTLD, независимо от членства в Организации поддержки национальных доменов (ccNSO).

Хранилище контактных данных

Средоточием сообщества TLD-OPS является лист рассылки TLD-OPS, который служит хранилищем контактных данных ссTLD. Его подписчики регулярно получают автоматически рассылаемые сообщения электронной почты с обзором всех подписанных на этот лист рассылки ссTLD и их контактными данными для реагирования на инциденты (контактные лица, номера телефонов и адреса электронной почты). Это позволяет им (а) использовать свой почтовый ящик для удобного и быстрого поиска контактных данных других ссTLD и (б) хранить контактные данные локально на своем устройстве (в локальном почтовом ящике), что позволяет находить контактные данные в ситуациях, когда отсутствует подключение к интернету. Таким образом, подписчики повышают свою доступность в случае необходимости реагирования на инциденты, а это позволяет быстрее обнаруживать и устранять угрозы благодаря помощи со стороны коллег.

Предупреждения безопасности

В состав сообщества TLD-OPS входит 61% всех ссTLD в мире, что также делает его превосходным форумом для распространения предупреждений безопасности, например, для сообщений о вредоносном ПО, использующем пространство имен ссTLD. Поэтому мы рекомендуем всем подписчикам отправлять такие предупреждения через лист рассылки. Для инициализации указанного процесса мы сотрудничаем с отделом безопасности ICANN, который оформляет типовые предупреждения безопасности для отправки подписчикам на лист рассылки TLD-OPS.

Управление

Лист рассылки TLD-OPS был создан национальными доменами верхнего уровня для внутреннего использования в 2014/2015 годах [1]. Он целиком находится под управлением сообщества ссTLD через Постоянный комитет TLD-OPS, в состав которого входят представители ссTLD из всех пяти географических регионов (Африка, Азиатско-Тихоокеанский регион, Европа, Северная Америка, Латинская Америка и Карибский бассейн) и представители Консультативного комитета по безопасности и стабильности (SSAC), Администрации адресного пространства интернета (IANA) и отдела безопасности ICANN. Постоянный комитет курирует повседневное функционирование листа рассылки и дальнейшее развитие «экосистемы TLD-OPS». Секретариат ccNSO обеспечивает административную поддержку. Сервер рассылки находится в Центре

175 членов*

147 ссTLD ASCII

От .ad (Андорра) до .zm (Замбия)

28 IDN ссTLD

От .中国 (Китай) до .فلسطين (Палестина)

Управление

Управление на 100% силами ссTLD при поддержке со стороны ICANN и DNS-OARC

Подписка

По электронной почте, отправка копии на адрес вашего контактного лица по административным вопросам IANA

Использование

Обеспечение простоты поиска вашими коллегами контактных данных лиц, отвечающих в вашем ссTLD за реагирование на инциденты, а также получение и распространение важных предупреждений безопасности

* По состоянию на 14 апреля 2016 года. Текущий список членов представлен на главной странице TLD-OPS.

Стать подписчиком не составит труда!

Стать подписчиком на лист TLD-OPS чрезвычайно просто, так как это лист рассылки электронной почты. Однако данный лист доступен только людям, отвечающим за общую безопасность и стабильность ccTLD, личность которых подтверждена соответствующим контактным лицом по административным вопросам IANA.

Чтобы подписаться на этот лист, попросите свое контактное лицо по административным вопросам IANA отправить в секретариат ccNSO электронное письмо, в котором указаны имена, адреса электронной почты и номера телефонов контактных лиц вашего ccTLD по вопросам безопасности и стабильности. Воспользуйтесь расположенным справа шаблоном подписки, который также можно скопировать с главной страницы сообщества TLD-OPS.

Важная информация: электронное письмо с запросом на оформление подписки должно быть отправлено с действующего адреса электронной почты контактного лица по административным вопросам, который зарегистрирован в базе данных IANA. Если это невозможно, необходимо скопировать этот адрес электронной почты в свое письмо с запросом на оформление подписки. В противном случае мы не сможем включить вас в число подписчиков. Сведения о вашем контактном лице по административным вопросам имеются в базе данных IANA: <https://www.iana.org/domains/root/db>.

Личное доверие

В основе листа рассылки TLD-OPS лежит личное доверие. Это означает, что подписчики могут указывать только свои личные контактные данные: адрес электронной почты и номер телефона. Основная причина такого подхода в том, что модель на основе личного доверия способствует повышению уровня доверия в сообществе ccTLD, например, благодаря тому, что люди начинают узнавать друг друга по именам. Адреса электронной почты, привязанные к должностям, запрещено использовать в этом листе рассылки.

Модель поручительства, которая обычно применяется в сообществе лиц, реагирующих на инциденты, непригодна для листа рассылки TLD-OPS. Причина этого в том, что сообщество ccTLD — многочисленная группа, а это означает, что будет трудно добавить в число подписчиков относительно малоизвестных людей.

Правила взаимодействия

Обмен информацией через лист рассылки с целью получения контактных данных ccTLD для реагирования на инциденты

Шаблон подписки

Воспользуйтесь указанным ниже форматом, чтобы подписаться на лист TLD-OPS. Эта форма также представлена для копирования на главной странице сообщества TLD-OPS.

-- Начало сообщения --

От кого: контактное лицо ccTLD по административным вопросам IANA или уполномоченный представитель

Кому: секретариат ccNSO <ccnsosecretariat@icann.org>

Копия: адрес контактного лица ccTLD по административным вопросам IANA

Тема: просьба о включении в число подписчиков на лист рассылки TLD-OPS

Уважаемый секретариат ccNSO,

Прошу включить указанных ниже лиц в число подписчиков на лист рассылки TLD-OPS. Настоящим подтверждаю, что они отвечают за общую безопасность и стабильность моего ccTLD, а я являюсь контактным лицом по административным вопросам IANA моего ccTLD или действую от его имени как уполномоченный представитель.

С уважением,

контактное лицо по административным вопросам IANA <ccTLD>

== КОНТАКТНЫЕ ДАННЫЕ ДЛЯ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ==

Контактное лицо №1 (основное):

Имя: <1-е имя> <1-я фамилия>

Адрес электронной почты: <1-й адрес электронной почты>

Номер мобильного телефона: +<код страны> <номер>

Контактное лицо №2 (дополнительное):

Имя: <2-е имя> <2-я фамилия>

Адрес электронной почты: <2-й адрес электронной почты>

Номер мобильного телефона: +<код страны> <номер>

Контактное лицо №3:

Имя: <3-е имя> <3-я фамилия>

Адрес электронной почты: <3-й адрес электронной почты>

Номер мобильного телефона: +<код страны> <номер>

-- Конец сообщения --

носит конфиденциальный характер и не должен выходить за рамки сообщества TLD-OPS.

Сведения о фактических инцидентах в системе безопасности должны выделяться с использованием цветов протокола Traffic Light (TLP) [2]: красный (информация только для конечного получателя), желтый (ограниченное распространение), зеленый (распространение в масштабе сообщества) или белый (неограниченное распространение). Сообщество TLD-OPS соблюдает определения TLP, которые были даны US-CERT [3].

Подписчики на лист рассылки не должны распространять автоматически созданные сообщения. В листе рассылки TLD-OPS не используется шифрование, чтобы подписчиком мог стать любой ccTLD. ■

Ссылки

[1] Итоговый отчет Рабочей группы SECIR: <http://ccnso.icann.org/workin/ggroups/secir.htm>

[2] Протокол Traffic Light: http://en.wikipedia.org/wiki/Traffic_Light_Protocol

[3] Определение TLP US-CERT: <https://www.us-cert.gov/tlp>

Описание

Брошюра Постоянного комитета TLD-OPS. Редакция 2.3, 14 апреля 2016 года.