ПРОЕКТ, май 2023 года

Информационное сообщение: соблюдение обязательств в отношении злоупотреблений DNS, предусмотренных Соглашением об аккредитации регистраторов и Соглашением об администрировании доменов верхнего уровня

Данная рекомендация содержит указания по интерпретации и соблюдению [СРОК] поправок к Соглашению об аккредитации регистраторов (RAA) и базовому соглашению об администрировании доменов верхнего уровня (gTLD) (RA), касающихся обязательств по смягчению последствий злоупотреблений в системе доменных имен (DNS) (Поправки по злоупотреблениям DNS).

Если Поправки по злоупотреблениям DNS не содержат особых изменений, все обязательства RAA и RA, действовавшие до принятия этих Поправок, остаются в силе.

Все термины, написанные с заглавной буквы, которые не определены в настоящем информационном сообщении, имеют те значения, которые даны им в RAA и RA.

Регистраторы и регистратуры, использующие методы, изложенные в настоящих рекомендациях, скорее всего, выполнят обязательства, изложенные в Поправках по злоупотреблениям DNS, однако следование одному или нескольким из этих методов не приведет к автоматическому признанию того, что регистратор или оператор регистратуры выполнил свои обязательства. Приведенные ниже примеры носят исключительно иллюстративный характер и не ограничивают возможные меры по смягчению последствий. Во всех случаях, когда Отдел по контролю исполнения договорных обязательств ICANN инициирует расследование, регистраторы и операторы регистратур должны предоставить доказательства, подтверждающие соблюдение соответствующих требований RAA и RA.

Для справки

Корпорация ICANN заключает с регистратурами договоры на управление gTLD в рамках RA. RA определяет обязанности оператора регистратуры, которые включают ведение авторитативной базы данных всех зарегистрированных доменных имен в gTLD и публикацию зоны DNS для gTLD.

Кроме того, ICANN заключает с каждым регистратором соглашение RAA, которое позволяет регистратору предлагать регистрационные услуги доменных имен в gTLD. В RAA изложены обязанности регистратора, такие как проверка информации о владельце домена (владельце зарегистрированного имени) и ведение точных записей. Роли и обязанности регистраторов и регистратур различны и отражены в их соответствующих соглашениях: RAA и RA.

ICANN обладает полномочиями по обеспечению соблюдения правил, связанных с услугами регистрации доменных имен и доменными именами и изложенных в RAA и RA. Данное Информационное сообщение посвящено доменным именам (зарегистрированным именам) в gTLD, которые используются в качестве средств или механизмов для злоупотребления DNS. Требования Поправок по злоупотреблениям DNS в RAA и RA основаны на действиях, которые регистраторы и операторы регистратур, соответственно, могут предпринять для минимизации масштабов и интенсивности ущерба и виктимизации, вызванных злоупотреблением DNS. Эти требования также учитывают, что регистраторы и операторы регистратур представляют собой лишь часть экосистемы DNS, состоящей из множества участников[1]. В зависимости от конкретных обстоятельств случая злоупотребления DNS наиболее подходящий участник для обнаружения, оценки, проверки и пресечения злоупотреблений может быть различным, и иногда им может быть не только регистратор или оператор регистратуры.

Злоупотребление DNS

Для целей RAA, RA и настоящего руководства под *злоупотреблением DNS* понимается вредоносное ПО, ботнеты, фишинг, фарминг и спам (когда спам используется в качестве механизма доставки для любого из четырех других типов злоупотреблений DNS), как эти термины определены в разделе 2.1 отчета Консультативного комитета по безопасности и стабильности об основанном на функциональной совместимости подходе к решению проблемы злоупотреблений в DNS (SAC 115[2]):

[1] Дополнительная информация приведена в отчете группы специальных интересов по злоупотреблениям DNS в FIRST, в котором также содержатся рекомендации для групп быстрого реагирования на инциденты относительно организаций, с которыми можно продуктивно связаться на различных этапах реагирования на инциденты для определения различных методов злоупотребления DNS. Кроме того, Организация по вопросам интернет-политики и юрисдикции (https://www.internetjurisdiction.net/) предоставила дополнительные инструкции по таким формам злоупотребления DNS в своем документе «Операционные подходы, нормы, критерии и механизмы».

[2] Консультативный комитет по безопасности и стабильности ICANN, SAC 115, раздел 2.1, стр. 12–13, 19 марта 2021 года

Вредоносное ПО — это вредоносные программы, устанавливаемые и/или исполняемые на устройстве без согласия пользователя, которые нарушают работу устройства, собирают конфиденциальные данные и/или получают доступ к частным компьютерным системам. К вредоносному ПО относятся вирусы, шпионские программы, программы-вымогатели и другое нежелательное программное обеспечение.

Ботнеты — это группы подключенных к интернету компьютеров, которые заражены вредоносным ПО и находятся под управлением удаленного злоумышленника.

Фишинг происходит, когда злоумышленник обманом заставляет жертву раскрыть конфиденциальные личные, корпоративные или финансовые данные (например, номера счетов, идентификаторы входа, пароли), отправляя мошеннические или внешне похожие на подлинные электронные письма или заманивая конечных пользователей на подложные сайты. Некоторые фишинговые кампании направлены на то, чтобы убедить пользователя установить вредоносное ПО.

Фарминг — это перенаправление ничего не подозревающих пользователей на мошеннические сайты или услуги, как правило, за счет перехвата или т. н. отравления кэша DNS. Перехват DNS может произойти, когда злоумышленники с помощью вредоносного ПО перенаправляет своих жертв на собственный сайт вместо изначально запрошенного. Отравление кэша DNS приводит к тому, что DNS-сервер (или резолвер) в ответ на запрос отправляет ложный интернет-протокол-адрес,содержащий вредоносное ПО. Фишинг отличается от фарминга тем, что последний подразумевает изменение записей DNS, в то время как первый обманным путем заставляет пользователей ввести персональные данные.

Спам — это нежелательная массовая рассылка электронных писем лицам, не дававшим согласия на их получение, когда сообщение отправлено в составе большой группы сообщений, имеющих одинаковое по сути содержание. Спам считается злоупотреблением DNS только в том случае, если он используется в качестве механизма доставки хотя бы одного из других видов злоупотреблений DNS, описанных выше.

Обязанности регистратора

Раздел 3.18 RAA

До вступления в силу поправок по злоупотреблениям в DNS раздел 3.18 обязывал регистраторов вести и публиковать контактную информацию для получения сообщений о злоупотреблениях, включая противоправную деятельность.
В этом положении также изложены требования, касающиеся расследования и реагирования на сообщения о злоупотреблениях, связанных с Зарегистрированными именами, спонсируемыми регистратором, и соответствующие записи, которые регистратор должен вести.
Требования раздела 3.18 PAA изменены следующим образом:

Требования, связанные с публикацией и сохранением контактов для сообщений о злоупотреблениях (RAA 3.18.1)

Куда сообщить о злоупотреблениях[3]
Для облегчения подачи сообщений от любой стороны о злоупотреблениях и/или противоправной деятельности регистратор должен опубликовать адрес электронной почты или веб-форму, легко доступную на главной странице веб-сайта регистратора[4]. Веб-формы не должны требовать ввода логина для отправки сообщений о злоупотреблениях.

Соответствующей требованиям будет считаться главная страница регистратора, на которой размещена ссылка на страницу «Сообщить о нарушении» или «Связаться с нами» (на которой четко указана контактная информация для сообщений о нарушении) и которая позволяет легко отправлять сообщения с указанной страницы.

Подтверждение получения сообщения о злоупотреблении
Кроме того, регистратор должен предоставить лицу, сообщившему о злоупотреблении, подтверждение того, что сообщение было получено. Это подтверждение получения может быть отправлено лицу, сообщившему о злоупотреблении, или выведено на экран по завершении отправки регистратору. Подтверждение о получении должно содержать достаточно информации для того,

[3] Во избежание двусмысленного толкования, требования, относящиеся к публикации адреса электронной почты и номера телефона контактного лица регистратора по жалобам на злоупотребления через Службу каталогов регистрационных данных (RDDS), остаются без изменений.

[4] Этот сайт должен располагаться по тому же унифицированному адресу ресурса (URL), который регистратор отображает в качестве значения поля «Registrar URL» в своей RDDS, предоставляемой ICANN и оператору регистратуры для публикации в RDDS оператора регистратуры.

чтобы заявитель мог доказать, что он подал сообщение о злоупотреблении. Как минимум, в подтверждении получения должны быть указаны регистратор, зарегистрированное имя (имена) и дата подачи сообщения.

Контакты для правоохранительных агентств
Требования, связанные с контактами, предназначенными для получения сообщений от правоохранительных агентств (LEA) и другим органов, находящихся в юрисдикции регистратора, ранее описанные в разделе 3.18.2 RAA, теперь приведены в разделе 3.18.3 RAA; эти требования остаются неизменными.

Требования, касающиеся принятия мер для смягчения последствий при получении сообщений о злоупотреблении DNS (RAA 3.18.2)

Раздел 3.18.2 RAA, измененный в соответствии с поправками по злоупотреблению DNS, теперь гласит:

> *Если Регистратор располагает действительными доказательствами того, что Зарегистрированное имя, спонсируемое Регистратором, используется для злоупотребления DNS, Регистратор должен незамедлительно предпринять соответствующие действия по смягчению последствий, которые разумно необходимы для прекращения, или иным образом запретить использование Зарегистрированного имени для злоупотреблений DNS. Действия могут быть различными в зависимости от обстоятельств, с учетом причины и серьезности ущерба от злоупотребления DNS, а также возможности сопутствующего ущерба*.

Действенные доказательства
Доказательства должны быть *действенными*. Это означает, что информация, которая легко доступна регистратору, должна быть достаточной для того, чтобы регистратор мог обоснованно определить, используется ли Зарегистрированное имя для одной или нескольких форм злоупотребления DNS. Регистраторам рекомендуется осуществлять проактивный мониторинг спонсируемых ими Зарегистрированных имен с целью выявления потенциальных злоупотреблений DNS. Оценка регистратором действенных доказательств зависит от обстоятельств каждого конкретного дела.

Получение действенных доказательств от внешней стороны
Палата сторон, связанных договорными обязательствами (CPH), опубликовала руководство, призванное помочь в представлении регистраторам полных и действенных сообщений о злоупотреблениях (Руководство CPH). В Руководстве CPH описаны доказательства, которые позволяют считать сообщение о злоупотреблении действенным. Например, скриншот, демонстрирующий попытку фишинга, с указанием того, против чего направлен фишинг (например, против

финансового учреждения), а также полный URL-адрес, на котором находится злоумышленник (например, пример[.]tld/страница[.]html)[5]. Сообщающим о злоупотреблениях рекомендуется ознакомиться с Руководством CPH и следовать ему, а также предоставлять в своих сообщениях как можно больше информации, чтобы регистратор мог провести расследование возможного злоупотребления DNS.

В тех случаях, когда регистратор получает сообщение о злоупотреблении, не содержащее всей необходимой информации для того, чтобы считать его доказательством злоупотребления DNS, регистратор должен провести расследование в соответствии с разделом 3.18 RAA. В некоторых случаях регистратор может иметь доступ к информации, которая не была предоставлена лицом, сообщившим о злоупотреблении, но является необходимой или полезной для определения того, что Зарегистрированное имя используется для злоупотребления DNS. В таких случаях регистратор должен рассмотреть информацию, к которой он может получить разумный доступ и которая имеет отношение к расследованию (например, DNS-серверы, информация об учетной записи и ее активности, а также содержимое, по крайней мере, основной веб-страницы или конкретного URL-адреса в сообщении о нарушении, если оно было предоставлено).

После получения действенных доказательств необходимо предпринять незамедлительные действия

После получения действенных доказательств регистратор должен *незамедлительно* предпринять *соответствующие действия*, которые разумно необходимы для прекращения или иного нарушения работы Зарегистрированного имени в целях злоупотреблений DNS. Для определения оперативных и надлежащих мер по смягчению последствий регистратор рассматривает конкретные обстоятельства дела, которые могут включать сопоставление масштаба и интенсивности ущерба, причиненного злоупотреблением DNS, с возможностью сопутствующего побочного ущерба.

Сопутствующий ущерб особенно важен в тех случаях, когда легитимное или неопасное доменное имя используется в качестве вектора злоупотреблений DNS без ведома или согласия владельца домена. Это часто называют «скомпрометированным доменом» и иногда является следствием махинаций с системы управления контентом сайта. В таких компромиссных ситуациях прямое приостановление регистрации домена регистратором или оператором регистратуры может оказаться неприемлемым средством защиты, так как приостановка прекращает доступ ко всему легитимному контенту, а также делает

[5] Этот URL показан в формате, известном как «безопасный формат URL». Безопасный URL-адрес читается человеком, но не реагирует на нажатие. Поэтому, если вы или получатель сообщения о нарушении по ошибке нажмете на URL-адрес, он не направит вас или получателя на потенциально вредоносный сайт.

недоступными все связанные с доменом почтовые и другие сервисы[6].
Это происходит и в том случае, если злоупотребление DNS связано с доменом третьего уровня или поддоменом. Регистраторы и регистратуры могут действовать только на уровне доменов второго уровня. Поэтому, если они приостановят работу домена второго уровня, будут приостановлены и все домены третьего уровня, а не только тот, который связан со злоупотреблением DNS.
В таких ситуациях регистратор может решить направить уведомление владельцу домена, оператору сайта и/или веб-хосту.

Что делает действие оперативным
Как уже отмечалось выше, соответствующие меры по смягчению последствий или пресечению случаев злоупотребления DNS будут зависеть от конкретных обстоятельств. Соответственно, время, необходимое для проведения расследования и принятия мер, также будет разным, что не позволяет установить фиксированный срок, в течение которого то или иное действие будет считаться «оперативным». Вместо этого регистраторы должны демонстрировать постоянное внимание к обвинениям в использовании спонсируемых имен для злоупотреблений DNS. Внимательность должна быть соизмерима с потенциальным ущербом, который наносит жертвам злоупотребление DNS.

Соответственно, в ответ на запрос ICANN по соблюдению договорных обязательств регистраторы должны будут объяснить, насколько оперативными были их действия с учетом конкретных обстоятельств. Затем отдел ICANN по контролю исполнения договорных обязательств рассмотрит объяснение и соответствующие обстоятельства, чтобы принять решение в каждом конкретном случае о том, были ли действия разумно оперативными. Сроки, приведенные в примерах, включенных в настоящее информационное сообщение, не являются контрактными требованиями, а лишь иллюстрируют их. Если регистратору требуется больше времени на расследование и принятие мер в случае, аналогичном приведенному в примере, это не обязательно будет свидетельствовать о несоответствии требованиям. Напротив, другие обстоятельства могут потребовать от регистратора более оперативных действий, например, случаи злоупотребления DNS, которые могут привести к неминуемому ущербу конечным пользователям. Предполагается, что регистратор проведет расследование и примет меры в кратчайшие сроки после того, как предпримет разумную попытку подтвердить факт злоупотребления DNS.

[6] Более подробную информацию о сопутствующем ущербе и соображениях пропорциональности при действиях на уровне DNS можно найти в публикации Организации по вопросам интернет-политики и юрисдикции «Пакет инструментов: Действия на уровне DNS для борьбы со злоупотреблениями».

Подводя итог: примеры соответствия регистратора требованиям
Приведенные ниже примеры иллюстрируют разумные и оперативные действия, предпринятые для предотвращения использования Зарегистрированного имени для злоупотреблений DNS (первый сценарий) и для пресечения злоупотреблений DNS в отношении Зарегистрированного имени (второй сценарий). Эти сценарии содержат конкретные фактические обстоятельства. При различных обстоятельствах отдельные регистраторы могут предпринимать различные действия и в различные сроки, чтобы остановить или иным образом пресечь отдельные случаи злоупотребления DNS. Во всех случаях регистраторы должны быть способны продемонстрировать, что любой подход отвечает соответствующим требованиям раздела 3.18 RAA.

Сценарий 1: Регистратор получает полный и действенный отчет о злоупотреблениях, в котором утверждается, что Зарегистрированное имя, спонсируемое регистратором, используется для фишинга. В отчете приведены данные о том, что по электронной почте или в SMS-сообщениях рассылается URL-адрес, содержащий Зарегистрированное имя, спонсируемое регистратором, который представляет себя как крупный банк и предлагающий получателям разблокировать их счета. Регистратор начинает расследование, рассматривая всю соответствующую информацию, содержащуюся в сообщении о злоупотреблении. В результате проведенного регистратором расследования выяснилось, что Зарегистрированное имя не имеет общедоступного веб-сайта и отображает только прямой URL-адрес с экраном входа в систему крупного банка. Этот же URL-адрес отправляется по электронной почте или SMS. Регистратор также считает, что клиент является новым и Зарегистрированное имя было зарегистрировано за пять дней до этого.

Надлежащие действия по смягчению последствий: Регистратор обоснованно делает вывод, что Зарегистрированное имя используется для злоупотребления DNS, и прекращает злоупотребление DNS, приостанавливая действие Зарегистрированного имени, применяя состояние домена clientHold протокола EPP[7]. Расследование и принятие мер по устранению последствий происходят в течение двух рабочих дней с момента получения сообщения о злоупотреблении. Регистратор также может принять решение о наложении блокировки на смену регистратора Зарегистрированного имени, чтобы предотвратить попытки владельца домена обойти меры по смягчению последствий и возобновить использование доменного имени для злоупотреблений DNS, при условии, что регистратор соблюдает применимые требования Политики смены регистратора ICANN.

Сценарий 2: Регистратор получает полный и действенный отчет о злоупотреблениях, в котором утверждается, что Зарегистрированное имя,

[7] Щелкните здесь для получения дополнительной информации от ICANN по статусам доменов EPP.

спонсируемое регистратором (autobrand.tld), используется для фишинга. Сообщение о злоупотреблении содержит доказательства использования конкретного URL-адреса для фишинга. Регистратор проводит расследование, рассматривая всю соответствующую информацию, содержащуюся в сообщении о злоупотреблении, а также информацию, легко и разумно доступную регистратору.

Расследование подтвердило, что URL-адрес, указанный в сообщении о злоупотреблении, используется для фишинга. В ходе расследования также выяснилось, что URL-адрес принадлежит поддомену (city.autobrand.tld) и, судя по всему, используется одним из франчайзи. Регистратор признает, что Зарегистрированное имя autobrand.tld было зарегистрировано три года назад и имеет надежный набор контента для франшизы автомобильного дилерства. Регистратор может подтвердить, что Зарегистрированное имя используется для корпоративной электронной почты Autobrand и поддоменов для нескольких франчайзи.

Надлежащие действия по смягчению последствий: Регистратор обоснованно заключает, что Зарегистрированное имя используется для злоупотребления DNS, но что это, скорее всего, является результатом компрометации домена и что владелец домена не использует Зарегистрированное имя для злоупотребления DNS сознательно. Регистратор оценивает потенциальный побочный ущерб, который может повлечь за собой приостановка действия доменного имени, и обоснованно приходит к выводу, что в данный момент это не является целесообразным действием по смягчению последствий. Вместо этого регистратор нарушает действие злоупотребления DNS, уведомляя Autobrand, владельца домена autobrand.tld, с требованием устранить фишинговое содержимое к определенной дате, разумно определенной регистратором. Расследование и принятие мер по смягчению последствий происходят в течение трех рабочих дней с момента получения сообщения о злоупотреблении.

Требования, связанные с ведением и предоставлением ICANN записей

Требования, касающиеся документирования и предоставления записей, связанных с получением и реагированием на сообщения о злоупотреблениях, которые ранее были описаны в разделе 3.18.3 RAA, теперь включены в раздел 3.18.4 RAA; эти требования остались без изменений. Эти требования также относятся к реагированию на сообщения о злоупотреблениях DNS в соответствии с разделом 3.18.2.

Обязанности оператора регистратуры

Раздел 4, Спецификация 6 RA

Раздел 4 Спецификации 6 RA требует публикации и предоставления в ICANN контактных данных для обработки запросов, связанных со злонамеренным поведением в домене верхнего уровня (TLD). Он также включает требования, связанные с удалением «осиротевших» связующих записей, если они используются в связи со злонамеренным поведением. Требования в данной Спецификации изменены следующим образом:

Требования, связанные с публикацией и сохранением контактов для сообщений о злоупотреблениях (базовое RA, раздел 4.1 спецификации 6)

Куда сообщить о злоупотреблениях
Для облегчения подачи сообщений от любой стороны о злонамеренном поведении в TLD, включая злоупотребления DNS, оператор регистратуры должен опубликовать адрес электронной почты или веб-форму, почтовый адрес и основное контактное лицо для обработки таких сообщений.

Соответствующей требованиям будет считаться главная страница оператора регистратуры, на которой имеется ссылка на страницу «Сообщить о нарушении» или «Связаться с нами» (на которой четко указана контактная информация для сообщений о нарушении), где можно беспрепятственно отправлять сообщения.

Подтверждение получения сообщения о злоупотреблении
После получения сообщения оператор регистратуры должен предоставить лицу, сообщившему о злоупотреблении, подтверждение того, что сообщение получено. Это подтверждение получения может быть отправлено лицу, сообщившему о злоупотреблении, или выведено на экран по завершении отправки оператору регистратуры. Подтверждение о получении должно содержать достаточно информации для того, чтобы заявитель мог подтвердить отправку сообщения о злоупотреблении. Как минимум, в подтверждении получения должны быть указаны оператор регистратуры, зарегистрированное имя (имена) и дата подачи сообщения.

Требования, касающиеся принятия мер для смягчения последствий при получении сообщений о злоупотреблении DNS (базовое RA, раздел 4.2 спецификации 6)

Раздел 4.2 спецификации 6, измененный в соответствии с поправками по злоупотреблению DNS, теперь гласит:

> *Если оператор регистратуры обоснованно определяет, основываясь на действенных доказательствах, что зарегистрированное доменное имя в TLD используется для злоупотребления DNS, оператор регистратуры должен незамедлительно предпринять соответствующие действия, которые разумно необходимо для того, чтобы способствовать прекращению или иному пресечению использования доменного имени для злоупотребления DNS. Такие действия, как минимум, должны включать следующее: (i) передача доменов, используемых для злоупотребления DNS, вместе с соответствующими доказательствами регистратору-спонсору; или (ii) принятие прямых мер со стороны Оператора регистратуры, если Оператор регистратуры сочтет это целесообразным. Действия могут варьироваться в зависимости от обстоятельств каждого случая, принимая во внимание серьезность ущерба от злоупотребления DNS и возможность сопутствующего ущерба.*

Действенные доказательства

Доказательства должны быть *действенными*. Это означает, что информация, которая легко доступна оператору регистратуры, должна быть достаточной для того, чтобы он мог обоснованно определить, используется ли Зарегистрированное имя для одной или нескольких форм злоупотребления DNS. Операторы регистратур могут получить действенное доказательство путем анализа информации, к которой они могут получить разумный и независимый доступ, будь то в связи с сообщением о злоупотреблении или в рамках собственных усилий в соответствии со Спецификацией 11(3)(b) Соглашения об администрировании доменов верхнего уровня путем проведения технического анализа с целью выявления доменов, используемых для злоупотребления DNS. Действенные доказательства также могут быть представлены оператору регистратуры внешней стороной, например правоохранительными органами, доверенными или признанными источниками соответствующего оператора регистратуры или любой другой стороной или источником. Сообщающим о злоупотреблениях рекомендуется предоставлять как можно больше информации, чтобы обеспечить оператора регистратуры достаточными сведениями для проведения расследования возможных злоупотреблений DNS. Во избежание двусмысленного толкования, сообщение о злоупотреблении, признанное оператором регистратуры неполным, может быть признано правомерным, если оператор регистратуры имеет доступ к достаточной информации для обоснованного проведения расследования с целью определения того, используется ли Зарегистрированное имя для злоупотребления DNS.

После получения действенных доказательств необходимо предпринять незамедлительные действия

После получения соответствующих доказательств оператор регистратуры должен незамедлительно предпринять соответствующие меры по смягчению последствий, которые разумно необходимы для того, чтобы способствовать прекращению использования доменного имени в целях злоупотребления DNS или иным образом помешать этому. Для определения соответствующих действий оператор регистратуры рассматривает конкретные обстоятельства дела, которые могут включать сопоставление масштабов вреда и виктимизации, причиненных злоупотреблением DNS, с возможностью сопутствующего ущерба. Важность сопутствующего ущерба в ситуации со скомпрометированными доменами, описанная выше для регистраторов, в равной степени относится и к регистратурам.

Оператор регистратуры также рассматривает вопрос о том, является ли он, спонсирующий регистратор и/или другая сторона наилучшим образом подготовленными сторонами для анализа и принятия соответствующих пропорциональных мер по смягчению последствий. Например, если одно Зарегистрированное имя используется для злоупотреблений DNS, то регистратор может рассмотреть и устранить злоупотребления DNS вместе со своим клиентом. Аналогичным образом, в случае взлома систем владелец зарегистрированного имени или хостинг-провайдер, имеющий административный доступ к затронутым системам, может лучше справиться с проблемами, и оператор регистратуры должен в первую очередь направить их регистратору, поскольку приостановка домена путем применения clientHold или serverHold может нанести побочный ущерб неопасному или легитимному содержимому. С другой стороны, оператор регистратуры может иметь наилучшие возможности для борьбы с крупномасштабными угрозами, охватывающими многих владельцев зарегистрированных имен или регистраторов, например, алгоритмами генерации доменов, используемыми для распространения ботнетов.

Оперативно предпринятые действия по смягчению последствий должны быть разумно необходимыми для достижения одного из следующих результатов: *способствовать прекращению* или *пресечению использования* Зарегистрированного имени для злоупотреблений DNS. Как минимум, оператор регистратуры должен принять следующие меры:

1) *Сообщить* о зарегистрированном имени (именах) и *предоставить* соответствующие доказательства спонсирующему регистратору (регистраторам); или
2) *Предпринять прямые действия* в отношении Зарегистрированного имени (имен), если оператор регистратуры сочтет такие прямые действия целесообразными.

Что делает действие оперативным

Как уже отмечалось выше для регистраторов, соответствующие действия по смягчению последствий или пресечению случаев злоупотребления DNS будут зависеть от конкретных обстоятельств.
Соответственно, время, необходимое для проведения расследования и принятия соответствующих мер, также будет разным, что не позволяет установить фиксированный срок, в течение которого то или иное действие будет считаться «оперативным». Вместо этого операторы регистратур должны демонстрировать постоянное внимание к обвинениям в использовании спонсируемых имен для злоупотреблений DNS. Внимательность должна быть соизмерима с потенциальным ущербом, который наносит жертвам злоупотребление DNS.

Соответственно, в ответ на запрос ICANN по соблюдению договорных обязательств оператор регистратуры должен будет объяснить, насколько оперативными были его действия с учетом конкретных обстоятельств. Затем отдел ICANN по контролю исполнения договорных обязательств рассмотрит объяснение и соответствующие обстоятельства, чтобы принять решение в каждом конкретном случае о том, были ли действия оперативными. Сроки, приведенные в примерах, включенных в настоящее информационное сообщение, не являются контрактными требованиями, а лишь иллюстрируют их. Если оператору регистратуры требуется больше времени на рассмотрение конкретного дела, это не обязательно свидетельствует о несоблюдении требований. И наоборот, другие обстоятельства могут потребовать от оператора регистратуры более оперативных действий, например случаи масштабных угроз, способных нанести неминуемый ущерб большому количеству конечных пользователей. Предполагается, что оператор регистратуры проведет расследование и примет меры в кратчайшие сроки после того, как предпримет разумную попытку подтвердить факт злоупотребления DNS.

Приведенные ниже примеры иллюстрируют разумные действия по предотвращению злоупотреблений DNS (второй сценарий) и по пресечению злоупотреблений DNS в отношении Зарегистрированного имени (первый и третий сценарии). Эти сценарии содержат конкретные фактические обстоятельства.
При различных обстоятельствах отдельные операторы регистратур могут предпринимать различные действия с разной продолжительностью, чтобы способствовать прекращению или иному пресечению отдельных случаев злоупотребления DNS. Во всех случаях операторы регистратур должны быть способны продемонстрировать, что любой подход отвечает соответствующим требованиям раздела 4.2 спецификации 6 RA.

Раздел 3(b), Спецификация 11 RA

В данный раздел были внесены изменения, в результате которых вместо термина «угрозы безопасности» было введено определение злоупотребления DNS, приведенное в поправках к разделу 4 спецификации 6.

Подводя итог: примеры соответствия операторов регистратур требованиям

Сценарий 1: Оператор регистратуры получил от кредитного союза (Example Credit Union) через веб-форму уведомление о том, что кто-то зарегистрировал домен <loginexamplecreditunion[.]TLD> шесть дней назад, и кредитный союз утверждает, что домен занимается фишингом. Кредитный союз приводит скриншот, на котором изображена веб-страница домена, собирающая учетные данные для входа в систему.

Надлежащие действия по смягчению последствий: После выполнения внутренних процедур отчет обрабатывается и рассматривается оператором регистратуры в течение двух рабочих дней. По завершении расследования оператор регистратуры обоснованно установил, что Зарегистрированное имя используется для злоупотребления DNS. Поэтому оператор регистратуры нарушает осуществление злоупотребления DNS, уведомляя и предоставляя всю необходимую информацию регистратору-спонсору. Оператор регистратуры включает ограниченное по времени требование к регистратору провести расследование и принять разумно необходимые меры по прекращению или иному пресечению злоупотребления DNS. К указанному сроку оператор регистратуры может подтвердить, что регистратор приостановил действие Зарегистрированного имени, применив статус домена clientHold.

Сценарий 2: К оператору регистратуры обратились правоохранительные органы и предоставили доказательства того, что ряд доменов участвует или будет участвовать в алгоритме генерации доменов, связанном с ботнетом. В ботнете задействуются некоторые существующие Зарегистрированные имена, но преимущественно домены, которые еще не зарегистрированы.

Надлежащие действия по смягчению последствий: В течение шести часов после завершения расследования и обоснованного подтверждения факта злоупотребления DNS оператор регистратуры вносит вклад в прекращение злоупотребления DNS, предпринимая действия, указанные правоохранительными органами или согласованные с ними. В этом случае оператор регистратуры согласился с тем, что для соответствующих Зарегистрированных имен по запросу правоохранительных органов регистратура будет делегировать их на другой DNS-сервер (серверы) (например, перенаправлять DNS-серверы имен или переводить их в синкхол). По запросу правоохранительных органов оператор регистратуры

также непосредственно создает домены для тех ранее незарегистрированных доменов, которые связаны с ботнетом. Отметим, что для создания домена оператором регистратуры обычно требуется разрешение в рамках разрешения ICANN на отступление от требования по мерам безопасности (SRW).)[8]. Кроме того, оператор регистратуры должен своевременно обратиться с просьбой о предоставлении разрешения на отступление от требования. При этом отмечается, что SRW также может применяться как можно скорее, насколько это практически возможно, и корпорация ICANN может ответить ретроактивным разрешением на отступление от требования, если это необходимо, чтобы не задерживать поддержку работы правоохранительных органов[9].

Сценарий 3: В ходе технического анализа на предмет выявления злоупотреблений DNS в соответствии со спецификацией 11(3)(b) оператор регистратуры обнаруживает, что подстраница домена используется для распространения вредоносных программ, в то время как остальная часть сайта на домене выглядит как легитимный или доброкачественный контент. Доменное имя зарегистрировано уже три года.

Надлежащее действие по смягчению последствий: В течение трех часов с момента установления факта использования зарегистрированного имени для злоупотребления DNS и его компрометации оператор регистратуры вносит свой вклад в пресечение процесса злоупотребления DNS путем уведомления и предоставления всей необходимой информации спонсирующему регистратору, а также направления регистратору запроса о принятии им мер по предоставлению отчета в течение определенного времени. Затем регистратор уведомляет об этом непосредственно владельца домена, который решает проблему путем обновления своей системы управления контентом для удаления вредоносного ПО.

Расследование корпорации ICANN на предмет соответствия новому разделу 3.18.2 RAA и разделу 4.2 спецификации 6 RA

Что представляет собой полный, обоснованный и соответствующий требованиям ответ? Отдел ICANN по контролю исполнения договорных обязательств будет обеспечивать соблюдение требований, изложенных в настоящем информационном сообщении, путем рассмотрения внешних жалоб, проактивного мониторинга и аудиторских проверок. Когда Отдел ICANN по

[8] Информация о разрешениях на отступление от требований приведена на этой странице.
[9] Более подробную информацию о том, как регистратуры могут сотрудничать с правоохранительными органами и ICANN для решения проблемы алгоритмов генерации доменов, см. в документе «Концепция алгоритмов генерации доменов, связанных с вредоносным ПО и ботнетами», опубликованный Рабочей группой по обеспечению общественной безопасности Правительственного консультативного комитета и Группой заинтересованных сторон регистратур gTLD.

контролю исполнения договорных обязательств получает жалобу, он рассматривает все доказательства, представленные заявителем, а также всю имеющуюся соответствующую информацию, чтобы определить, нужно ли возбуждать дело о соблюдении требований в отношении соответствующего регистратора или оператора регистратуры. В случае отсутствия достаточных доказательств в поддержку заявления о злоупотреблении DNS, отдел ICANN по контролю исполнения договорных обязательств закрывает дело как недействительное. Среди прочего, в ходе этой проверки будет рассматриваться вопрос о том, достаточно ли информации, легко доступной спонсирующему регистратору напрямую или через посредника, или оператору регистратуры (в зависимости от ситуации) для обоснованного определения того, что зарегистрированное имя используется для одной или нескольких форм злоупотребления DNS. В ходе проверки будет также рассмотрен вопрос о том, имелась ли какая-либо дополнительная информация от подателя заявления в ответ на запросы регистратора или оператора регистратуры о предоставлении дополнительной информации или доказательств.

Кроме того, если это применимо и имеет отношение к конкретному случаю, отдел ICANN по контролю исполнения договорных обязательств предпримет следующие действия: (1) просмотр соответствующих общедоступных данных, отображаемых в Службе каталогов регистрационных данных, например дату создания, статус(ы) EPP или информацию о DNS-серверах; и (2) выполнение поиска по DNS, чтобы определить, разрешаются ли сообщенные Зарегистрированные имена в DNS. Отдел ICANN по контролю исполнения договорных обязательств может также провести собственное расследование и изучить дополнительную релевантную информацию о конкретном Зарегистрированном имени, предположительно вовлеченном в злоупотребление DNS.

При возбуждении дела о соответствии требованиям в отношении регистратора или оператору регистратуры в соответствии с разделом 3.18.2 RAA или разделом 4.2 Спецификации 6 RA, соответственно, отдел ICANN по контролю исполнения договорных обязательств предоставит подробный список всей информации и записей, необходимых для оценки соответствия требованиям в отношении заявленных Зарегистрированных имен и форм предполагаемого злоупотребления DNS. В ответ на возбуждение дела о нарушении требований регистратор и оператор регистратуры должны будут, как минимум, выполнить следующие действия:

- Объяснить, как и почему регистратор или оператор регистратуры пришел к выводу, что полученные доказательства не могут быть использованы, если это применимо. Например, регистратор может объяснить, что, изучив информацию и записи, предоставленные сообщившей стороной, и проведя расследование, регистратор не смог подтвердить, что злоупотребление DNS имело место в отношении упомянутого Зарегистрированного имени (имен). Отдел ICANN по контролю исполнения договорных обязательств

может попросить регистратора или оператора регистратуры разъяснить любые явные несоответствия между предоставленным объяснением и любой информацией и данными, полученными отделом ICANN по контролю исполнения договорных обязательств в процессе проверки жалобы.

- Предоставить подробное объяснение, подкрепленное соответствующими записями, конкретных предпринятых мер по смягчению последствий, когда они были предприняты и как предпринятые действия были сочтены оперативными и разумно необходимыми для прекращения или срыва или содействия прекращению или срыву, применительно к конкретным обстоятельствам дела (включая любые применимые объяснения, касающиеся непропорциональности действий на уровне DNS и сопутствующего ущерба). Требования к регистратору о предоставлении этой информации будут по-прежнему применяться в тех случаях, когда регистратор решает делегировать расследование отчета о злоупотреблении DNS реселлеру. В таких случаях регистратор сохраняет обязанность продемонстрировать соблюдение раздела 3.18 RAA[10], объяснив свои действия, а также действия любых других делегированных сторон, таких как реселлеры, и предоставив соответствующие записи.

Политика ICANN и контрактные требования применяются в рамках законов и нормативных актов, применимых к каждому регистратору и оператору регистратуры. Во избежание двусмысленного толкования, ни от регистраторов, ни от операторов регистратур не требуется и не предполагается предпринимать какие-либо действия, противоречащие действующим законам и нормативным актам.

Информация о том, когда, как и куда можно подать жалобу в отдел ICANN по контролю исполнения договорных обязательств, приведена здесь.

[10] См. раздел 3.12 RAA.