№15
Май 2021

MSK IX

Интернет изнутри

Информационная безопасность

Тенденции и проблематика корпоративной безопасности

с. 4

Содержание:

Журнал
«Интернет изнутри»

info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №15, дата выхода:
Май 2021 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ПИ № ФС77-71202 от 27.09.2017

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Редакционная коллегия:
Воронина Елена
Платонов Алексей

Продакшн:
Гончаров А.В.

Дизайн и вёрстка:
Дмитрий Ивлянов

Арт-директор:
Новикова Ольга

Дизайнер:
Сдобнова Юлия

Корректор:
Рябова Наталья

Обложка разработана с использованием ресурсов сайта Freepik.com

Целостность, конфиденциальность, доступность

Главный редактор:
Андрей Робачевский

Дорогой читатель!

Цифровой мир все крепче переплетается с физической реальностью. Достоинства этой эволюции трудно переоценить, а перспективы поражают воображение. Доступность необходимой информации, вычислительные мощности и всемирная связность позволяют нам решать все более сложные задачи, более эффективно и с минимальными затратами. Разумеется, все это предполагает, что целостность, конфиденциальность и доступность этих ресурсов – триада информационной безопасности – не могут быть скомпрометированы. Однако чем больше мы зависим от цифрового мира — тем более значительны последствия нарушений его функционирования, чем более связанны наши системы — тем необъятнее наша «поверхность атаки», чем более доступны данные – тем труднее обеспечить требования конфиденциальности. Другими словами, информационная безопасность чрезвычайно важна, но ее обеспечение далеко не тривиальная задача.

Наши постоянные читатели наверное помнят, что мы уже не раз касались этой темы – мы посвятили безопасности один из первых номеров (№2), а также затронули эти вопросы в №4 о критической инфраструктуре, а также в №10, обсуждая проблемы и решения защиты данных. Но тема поистине необъятна, поэтому мы решили вернуться к ней опять.

Мы открываем журнал статьей Константина Чумаченко «Безопасность веб-приложений в корпоративной среде: возможности и риски», в которой он обсуждает тенденции и проблематику корпоративной безопасности и безопасности интернет-инфраструктуры, которая является неотъемлемой частью корпоративной среды. Эта критическая зависимость от глобальной инфраструктуры несет в себе колоссальные преимущества, но также приводит к размытию границ корпоративной сети и связанным с этим рискам.

Ярким примером этого является DNS. Муслим Меджлумов в статье «Использование DoH в корпоративных сетях» приводит практические рекомендации по применению этой относительно новой технологии (DNS через протокол HTTPS) системы разрешения имен.

Защищенность онлайн-транзакций существенным образом зависит от цифровых сертификатов, поддерживаемых т.н. системой WebPKI. Возможность отзыва скомпрометированных сертификатов является критической функцией. Но является ли сегодняшняя практика отзыва эффективной? Джефф Хьюстон в своей статье «Отзыв сертификатов» приходит к неутешительному выводу, что в вопросах интернет-безопасности мы безосновательно полагаемся на неповоротливую систему защиты, чье время реакции в нынешнем наносекундном мире измеряется в лучшем случае неделями.

Аутентификация — еще один важный элемент информационной безопасности. Об использовании биометрии, ее возможностях и проблемах с вами поделится Наталья Коннова в статье «Биометрия в информационной безопасности. Настоящее и перспективы биометрической аутентификации».

Не оставили мы без внимания и наши стандартные темы. Как всегда, Павел Храмцов приглашает вас в свою рубрику «Новости науки и техники», а в новостях доменной индустрии вы узнаете, как обеспечивается безопасность российского доменного пространства.

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках? Пишите нам по адресу info@internetinside.ru.

Безопасность веб-приложений в корпоративной среде: возможности и риски

Константин Чумаченко, NGENIX

Бурная и отчасти вынужденная цифровизация нашей жизни привела к росту числа используемых в организациях веб-приложений и создала новые угрозы информационной безопасности. Как держать риски ИБ под контролем и могут ли облачные платформы в этом помочь?

Кризис ускоряет изменения

В последние годы трудно найти отрасль экономики, в которой не использовались бы веб-приложения, а за время пандемии их роль в профессиональной и бытовой среде многократно возросла. Даже компании, чья деятельность напрямую не связана с товарами, услугами и финансовыми транзакциями, перестроили работу с прицелом на онлайн, обновили веб-сайты и обзавелись мобильными приложениям. Вероятно, скоро не останется ни одной области человеческой деятельности, которая не имела бы веб-интерфейса. Стремительная цифровизация заставляет компании и учреждения заново открывать для себя IT, пересматривать подходы к организации процессов и обновлять инструментарий для их автоматизации. Новой нормой стало расположение большей части корпоративных систем вне офиса. Новой инфраструктурой для создания и масштабирования веб-приложений стали облачные платформы. Фраза “The Network is the Computer”, сказанная в середине 80-х сотрудником Sun Microsystems Джоном Кейджем, идеально описывает сегодняшнюю реальность, в которой компании могут предоставлять и использовать десятки внешних веб-приложений и не иметь ни собственного дата-центра, ни даже сервера в офисе.

С начала коммерциализации Интернета компании столкнулись с потребностью быстро создавать и улучшать цифровые сервисы. В условиях глобальной конкурентной среды гонка за новыми функциями и дефицит разработчиков оставляют мало времени и ресурсов, чтобы системно заниматься устранением уязвимостей и обеспечением сохранности данных. Во многих компаниях ИБ (информационная безопасность) конфликтует с бизнесом за ресурсы и воспринимается как препятствие для развития. Поэтому зачастую безопасности уделяется недостаточно внимания, а реакция на угрозы следует, когда жертва злоумышленников уже оказывается в новостях.

Удобство или безопасность?

Размытие границ между Интернетом и корпоративной сетью увеличивает зависимость внутреннего IT-хозяйства компаний от внешнего мира, а вместе с этим повышает риски кибербезопасности. Чтобы вести деятельность в глобальном масштабе Интернета, компаниям приходится пересматривать стратегии безопасности и экстренно наращивать компетенции в сфере ИБ. Каждое преимущество может иметь обратную сторону, поэтому главная цель любой ИБ-стратегии – определить разумный баланс между удобством и безопасностью. Существенное влияние на него оказывают два фактора – удаленная работа и проникновение в корпоративную среду публичных веб-приложений.

Удаленная работа

От глубоких изменений в рабочих отношениях не скрыться, даже если вы работаете не в IT-компании. Удаленная работа, которая до пандемии воспринималась передовыми руководителями как средство привлечения квалифицированных сотрудников, в период локдаунов для многих компаний стала единственным способом продолжить деятельность. Масштабный тест-драйв доказал способность распределенных команд делать сложные проекты – от съемок сериалов до проектирования космических кораблей. Это означает, что спрос на платформы для совместной работы и средства коммуникаций для организаций будет нарастать, как и головная боль ИБ-подразделений.

Если раньше возможности «удаленки» сводились к доступу к корпоративной почте, то сегодня сотрудникам требуется обеспечить доступ к приложениям (интранету, CRM, хелпдеску и пр.) из любого места, где есть подключение к Интернету. Ситуация усложняется многообразием используемых сотрудниками устройств и необходимостью поддерживать достаточно высокий уровень «цифровой гигиены» при их использовании.

Публичные веб-приложения в корпоративной среде

Сервисная модель использования ПО (SaaS, Software-as-a-Service) позволяет компаниям-потребителям экономить на разработке, поддержке и эксплуатации приложений, а провайдерам подобных услуг – осваивать глобальные рынки. Неслучайно рыночная оценка одной из самых известных компаний в SaaS-сегменте Salesforce CRM составляет более 200 млрд долларов. Компании из самых разных секторов экономики – от Visa до Starbucks – становятся сервисными платформами и предоставляют партнерам и заказчикам возможность взаи-

модействия с их собственными системами через веб. Широкое распространение получила интеграция веб-платформ с использованием интерфейсов программирования приложений (API, Application Programming Interface). Такие интерфейсы базируются на протоколе HTTP и позволяют обмениваться данными и встраивать необходимые функции веб-платформы в систему заказчика. Публичные веб-приложения осуществляют критичные транзакции и аккумулируют конфиденциальные данные. Потенциальный ущерб от потерь данных и прерываний работы таких сервисов велик, и ставки непрерывно растут.

Идентифицируем риски

Широкое использование публичных веб-приложений и удаленная работа повышают продуктивность сотрудников, но осложняют защиту информации в компаниях. Цели, описываемые классической триадой «конфиденциальность — целостность — доступность», накладываются на приоритеты бизнеса, которому важны удобство инструментов, возможность быстрого наращивания ресурсов при росте нагрузок и контроль бюджетов. В достижении этих целей важно соблюсти баланс. С одной стороны, обеспечение ИБ не должно сводиться к чисто формальному набору мероприятий, проводимых в параллельном для бизнеса мире. С другой стороны, оно не должно подрывать эффективность компании и блокировать работу сотрудников. Важно учесть реальные потребности пользователей: в организациях с драконовскими запретами большая часть задач решается с помощью «теневого IT» — внешних облачных дисков, публичных емейлов и пр.

Обеспечение ИБ для веб-приложений следует традиционной схеме, первый шаг которой – идентифицировать угрозы, определить проблемы безопасности и уязвимости. Универсальный рецепт для этого вряд ли возможен, поэтому я бы хотел выделить следующие риски:

- минимизация уязвимостей на этапе разработки и интеграции ПО;
- контроль прав доступа к системам;
- учет рисков воздействий на интернет-инфраструктуру.

Безопасность ПО на уровне дизайна

Современная веб-разработка, как правило, не начинается с нуля, а представляет собой интеграцию готовых фреймворков, библиотек и микросервисов. Важно понимать исходный состав ингредиентов на протяжении всего жизненного цикла разработки веб-приложения и принимать меры, чтобы уменьшить вероятность появления уязвимостей. Правильный подход на этапе дизайна ПО позволит снизить цену защиты в будущем.

Как системно подойти к учету рисков при создании веб-приложения? Основой любой системы информационной безопасности является модель угроз. Она формализует предметы беспокойства – то есть критичные функции приложения, потенциальные источники и способы реализации угроз – и помогает оценить возможный ущерб, а также выбрать меры по его предотвращению.

Отправной точкой для знакомства с основными угрозами и рисками ИБ веб-приложений считается список OWASP Top Ten, публикуемый некоммерческой организацией OWASP Foundation. В основе списка лежат данные независимых исследований и отраслевых опросов о распространенности, сложности обнаружения и простоте эксплуатации уязвимостей веб-приложений. Список OWASP не является исчерпывающим, а отражает только наиболее актуальные угрозы на момент составления рейтинга. Документ обновляется каждые 3-4 года, последний апдейт был опубликован в 2017 году.

- Топ-10 угроз безопасности веб-приложений OWASP (https://owasp.org/www-project-top-ten/)
- Внедрение вредоносного кода (Injection)
- Недостатки аутентификации (Broken Authentication)
- Незащищённость конфиденциальных данных (Sensitive Data Exposure)
- Внешние сущности XML (XXE) (XML External Entities)
- Недостатки контроля доступа (Broken Access Control)
- Некорректная настройка параметров безопасности (Security Misconfigurations)
- Межсайтовое выполнение сценариев (XSS) (Cross Site Scripting)
- Небезопасная десериализация (Insecure Deserialization)
- Использование компонентов с известными уязвимостями (Using Components with Known Vulnerabilities)
- Недостатки журналирования и мониторинга (Insufficient Logging and Monitoring)

В числе других проектов OWASP Foundation – поддержание руководств по тестированию веб- и мобильных приложений The Web Security Testing Guide (WSTG) и Mobile Security Testing Guide (MSTG), которые содержат рекомендации по составлению модели угроз и выявлению уязвимостей приложений на этапах дизайна и эксплуатации.

Управление доступом: от защиты периметра к нулевому доверию

Традиционный подход к управлению доступом пользователей базируется на понятии периметра информационной системы и предлагает считать доверенными все действия пользователей, прошедших авторизацию и допущенных в некий внутренний контур. Классический пример – свободный доступ к интранету организации со всех офисных компьютеров. Такой подход может работать для однородных групп пользователей в «плоской» информационной среде. В текущей реальности приложения могут сочетать собственный код и функции внешних платформ, поддерживать сложную систему прав доступа и использовать серверные ресурсы в разных частях света. К примеру, маркетплейс может предусматривать десятки пользовательских ролей для собственного персонала, мерчантов и подрядчиков, поддерживать авторизацию покупателей с профилями в Google, Facebook, VK, взаимодействовать по API с внешними платежными шлюзами, использовать рекомендательный движок собственной разработки. При этом он может арендовать вычислительные ресурсы у облачных провайдеров, а скрипты и картинки доставлять с помощью CDN. В «сложносочинённых» IT-средах сложность реализации подхода, основанного на защите периметра, делает его практически неприменимым.

Концепция «нулевого доверия» (Zero Trust), предложенная аналитиками Forrester Research более 10 лет назад, сегодня предлагает альтернативный подход к организации доступа к приложениям. В этой концепции привилегии пользователя не определяются его местоположением, а непрерывно находятся под сомнением и проверяются путем аутентификации и авторизации каждой пользовательской сессии. Внедрение архитектуры Zero Trust делает ненужным использование VPN и позволяет сотрудникам использовать внешние веб-приложения на облачных платформах без потерь производительности. Сервисы доступа к приложениям на основе Identity-aware-Proxy, наряду со средствами многофакторной аутентификации, поддерживают Google, Akamai и другие облачные вендоры.

Так ли надежна интернет-инфраструктура?

Глобализация IT-операций заставляет компании задумываться о надежности Интернета. Бесперебойная работа веб-приложения невозможна, если опорная интернет-инфраструктура испытывает недостаток ресурсов или если нарушено функционирование сетевых служб и протоколов. В качестве ключевых рисков в отношении интернет-инфраструктуры можно выделить DDoS-атаки (Distributed Denial of Service) и нарушения маршрутизации пользовательских запросов.

Широкая экспозиция веб-приложений в публичной сети влечет угрозу стать объектом DDoS-атак. Слабо защищенные компьютеры и другие интернет-устройства становятся мишенью распространителей вирусов и других злоумышленников. Объединившись в ботнет, такие устройства представляют собой сотни тысяч «заряженных ружей», способных сработать по сигналу и направить зловредный трафик на атакуемое приложение. В результате переполняются каналы связи, заканчиваются ресурсы серверов и приложение оказывается недоступным. Детектирование и блокировка DDoS-атак осложняется распределенным характером источников трафика, каждый из которых по отдельности может выглядеть как легитимный пользователь. Ежегодно регистрируются десятки тысяч DDoS-атак, а крупнейшие известные DDoS-атаки превышают терабитные значения.

Поддержка собственной системы защиты от DDoS-атак требует больших инвестиций в оборудование, софт и компетенции команды ИБ. К счастью, защита от DDoS широко доступна как сервис облачных провайдеров и ISP – об этих возможностях ниже.

Среди протоколов и систем, отвечающих за маршрутизацию пользовательских запросов к веб-приложению, наиболее значимые угрозы связаны с DNS и BGP.

Доступ практически к любому веб-сайту начинается с DNS-запроса. Система DNS (Domain Name System) отвечает за преобразование доменных имен в IP-адреса путем обращений к иерархической системе серверов, хранящих доменные записи.

После 30 лет существования многие представляют себе DNS как идеально отлаженную систему, все уязвимости которой давно ликвидированы.

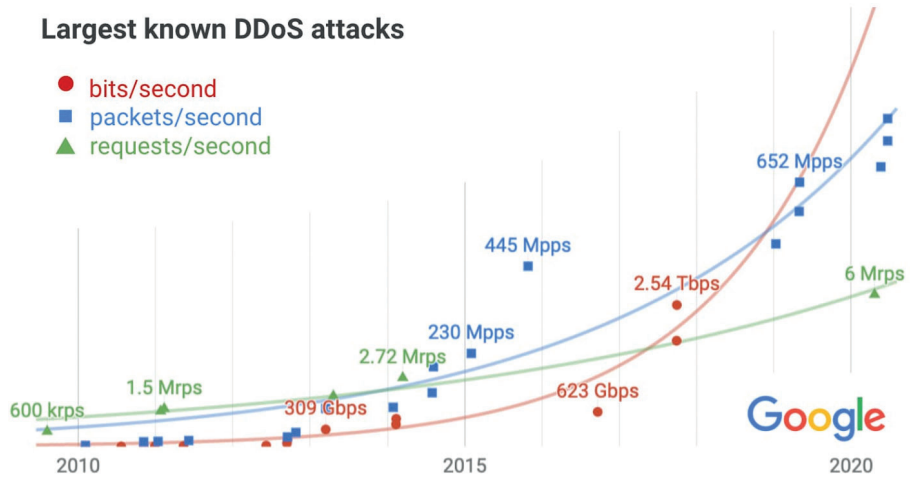
Реальная сложность настройки DNS может стать сюрпризом для администратора веб-приложения. Берт Хубер, автор популярного свободного ПО PowerDNS, отмечает, что текущий стандарт системы описывается в 185 документах RFC, и сравнивает его с верблюдом, перегруженным функциями и расширениями. В обычной практике администраторами настраивается малая часть этих функций - и важные моменты приватности и защищенности обмена с DNS-серверами часто остаются без внимания.

Неудивительно, что неправильная конфигурация является основной причиной инцидентов ИБ, связанных с DNS. Перехват управления авторитативным сервером зоны или резолвером, а также подмена содержимого ответов DNS-серверов в результате атаки типа Man-in-the-Middle позволяют злоумышленникам перенаправить пользовательские запросы на зловредный веб-ресурс, чтобы впоследствии внедрить вредоносное ПО или похитить пользовательские данные. Усугубляет ситуацию то, что корпоративные межсетевые экраны, как правило, не блокируют DNS-трафик, и сама система DNS может стать мишенью для DDoS-атак или каналом утечки чувствительной информации из сети компании.

Протокол BGP, применяемый для обмена маршрутной информацией между автономными интернет-сетями (AS, Autonomous Systems), редко попадает в сферу внимания администраторов веб-приложений, но часто является причиной их недоступности. Уже многие годы уязвимости BGP являются предметом дискуссий сетевых инженеров. Каждая из примерно 70 тысяч организаций, управляющих собственной AS, может передать средствами BGP своим «соседям» ложную информацию о готовности маршрутизировать трафик на интернет-сеть, которая в реальности недоступна. Если соседние AS доверятся этим анонсам, трафик пользователей отправится в «черную дыру».

Подобные инциденты обычно случаются из-за ошибок сетевых администраторов – информация о сбоях маршрутизации регулярно попадает в новостные заголовки. Более опасны атаки, целенаправленно использующие анонс чужих сетей (BGP prefix hijacking). Используя протокол BGP, в 2018 году злоумышленники смогли перенаправить трафик DNS-сервиса Amazon Route 53

Рисунок 1. Крупнейшие известные DDoS-атаки.



[Источник:https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks]

на свой DNS-сервер, который отдавал для сайта MyEtherWallet.com IP-адрес сервера атакующих. Подобная операция позволила хакерам получить доступ к кошелькам пользователей с криптовалютой без непосредственной компрометации веб-приложения.

Чем помогут облака?

Как видим, спектр задач, связанных с информационной безопасностью веб-приложений, весьма широк. Где IT-службам взять ресурсы и компетенции для их решения и могут ли в этом помочь облачные сервисы?

От безопасных облаков к облачной безопасности

Колоссальный объем инноваций в автоматизации рабочих процессов, реализованных за последнее десятилетие, был бы невозможен без облачных сервисов, ставших инфраструктурой и платформами для быстрого запуска и масштабирования приложений. По данным агентства Eurostat, 36% предприятий Европы использовали облачные вычисления в 2020 году, в основном для размещения своих систем электронной почты и хранения файлов в электронном формате. 55% из этих организаций также использовали передовые облачные сервисы, относящиеся к финансовым и бухгалтерским программным приложениям, CRM- и ERP-системам или использованию вычислительных мощностей для запуска бизнес-приложений. Потенциал облачных сервисов только начинает раскрываться, и пока стоимость разработки ПО растет быстрее биткоина, миграция в облако будет только ускоряться.

Могут ли облака быть безопасными, а безопасность – облачной? Основные сомнения в ходе миграции в облако связаны с передачей конфиденциальных данных и с сомнениями в защищенности самого облака. Согласно результатам недавнего опроса 2020 Enterprise Cloud Trends Report, 45% IT-руководителей, использующих облачные сервисы, считают проекты ИБ наивысшим приоритетом. Доля тех, кто готов перенести в облако защиту от кибератак, пока еще относительно невелика, но быстро растет.

Плюсы перевешивают риски

С точки зрения безопасности для большинства компаний облака сегодня гораздо надежнее, чем сеть предприятия. Вендоры облачных решений ставят безопасность на первое место и вкладывают огромные ресурсы в механизмы защиты, исследования возникающих угроз и новые разработки. Поставщики облачной безопасности обладают уникальным опытом и квалификациями, быстрее и эффективнее реагируют на входящие угрозы. Поэтому облачные решения в области безопасности дают даже небольшим компаниям возможность обеспечивать защиту самыми передовыми инструментами.

Хорошим примером эффективности является облачная защита от DDoS-атак. Решения по фильтрации DDoS-трафика, разворачиваемые на территории заказчика, имеют заведомо ограниченную емкость. Крупную атаку сложно отразить собственными силами, намного эффективнее бороться с ней с помощью облака, которое будет отражать нелегитимный трафик на дальних подступах к атакуемому веб-ресурсу. Распределенные платформы Edge Cloud – следующий этап в эволюции CDN – позволяют сочетать ускорение и защиту веб-ресурсов, обрабатывая и фильтруя запросы к приложению в непосредственной близости от пользователей.

Другая проблема, которую решает облачная безопасность, – дороговизна содержания собственной инфраструктуры («железо», ПО, лицензии) и содержания собственного Центра по обеспечению безопасности (SOC, Security Operations Center). С помощью облака компании могут избежать затрат на покупку, установку, обслуживание и модернизацию оборудования и программного обеспечения. Пользователи услуги также могут легко масштабировать или изменять свою защиту для отражения угроз нового типа или решения организационных задач – это изначально заложено в возможности облачной платформы.

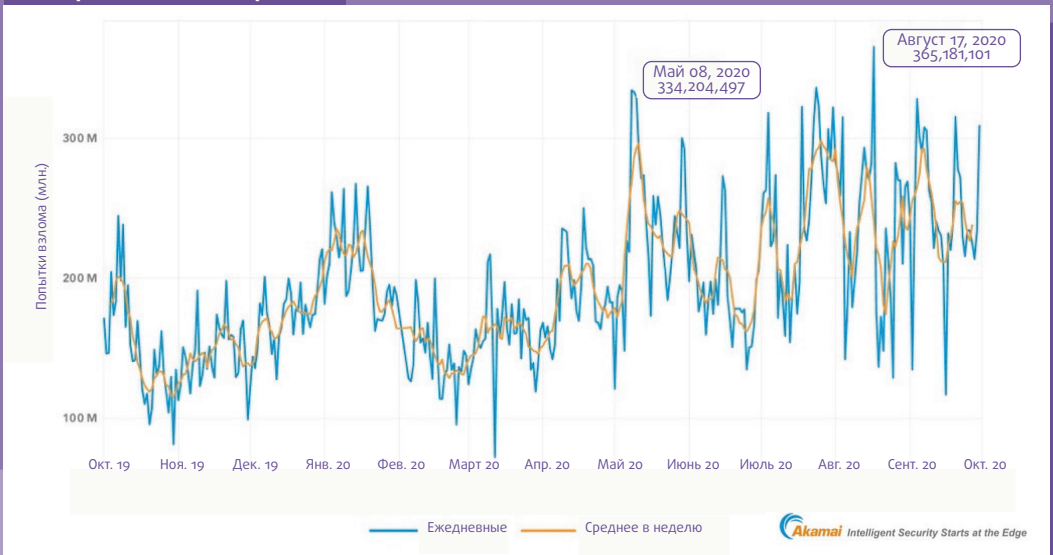
Любую систему киберзащиты должны сопровождать квалифицированные специалисты в области ИБ. Их опыт, умение и скорость реакции в конечном счете определяют эффективность защиты. Эти компетенции весьма недёшевы. К тому же, кибербезопасность – обширная тема, и нет такого эксперта, который бы детально разбирался в каждом аспекте, а рекрутировать и содержать штат разнопрофильных профессионалов имеет смысл только для очень крупных бизнесов.

Как выбрать облачного провайдера и убедиться в безопасности его решений? Простейший рецепт – ориентироваться на опыт и масштаб деятельности. Важно убедиться, что ваши требования являются для него типовыми, а предлагаемые вами задачи были не раз успешно решены с другими клиентами. В IT нет монополий на инновации, и этому критерию могут соответствовать как универсальные, так и нишевые игроки. Также стоит оценить, способен ли ваш провайдер инвестировать достаточные средства в защищенность облака и поддерживать высокий уровень экспертизы в ИБ. В этом вам может помочь «второе мнение» независимых организаций, например, сертификат на соответствие стандарту безопасности данных индустрии платёжных карт PCI DSS. И наконец, нельзя пренебрегать формальной стороной – поинтересуйтесь декларируемой политикой конфиденциальности и уровнем ответственности – в первую очередь финансовой, – которую готов взять на себя провайдер.

Доверие как сознательный выбор

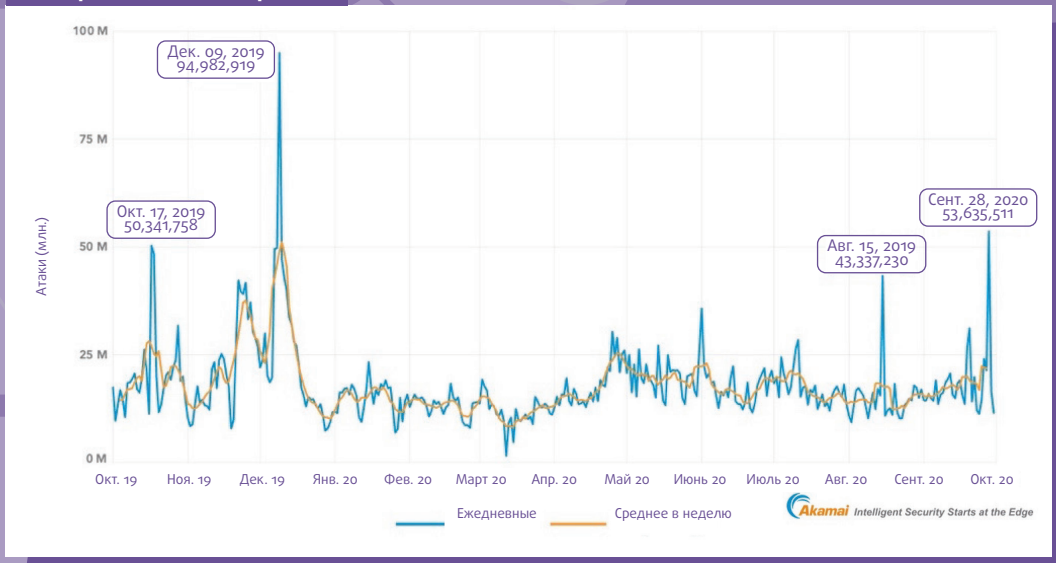
В цифровую эпоху деятельность многих предприятий зависит от бесперебойного обмена информацией. Закон больших чисел работает против нас: с ростом проникновения веб-приложений в корпоративные среды, распространением удаленной работы и окончательным уходом в прошлое концепции «безопасного периметра» уровень угроз ИБ будет нарастать. Как прагматичный IT-руководитель может решить эти проблемы? Можно выбрать консервативный подход – ограничить использование внешних сервисов и устройств, а развитие IT вести по принципу «натурального хозяйства». Можно принимать всё, что предлагает обширный рынок SaaS-стартапов, и в один прекрасный день обнаружить свои данные в публичном доступе. Разумный путь где-то посередине. Технологии быстро меняются, время универсальных экспертов уходит. Новыми актуальными навыками CIO и CTO будут кругозор и эрудиция в области готовых решений. Умение оценивать свои возможности, проектировать процессы и системы на базе проверенных компонент, правильно выбирать партнеров для аутсорсинга сегодня не менее важно для IT-руководителя, чем технические знания.

Ежедневные попытки взлома учетных данных октябрь 2019 – сентябрь 2020



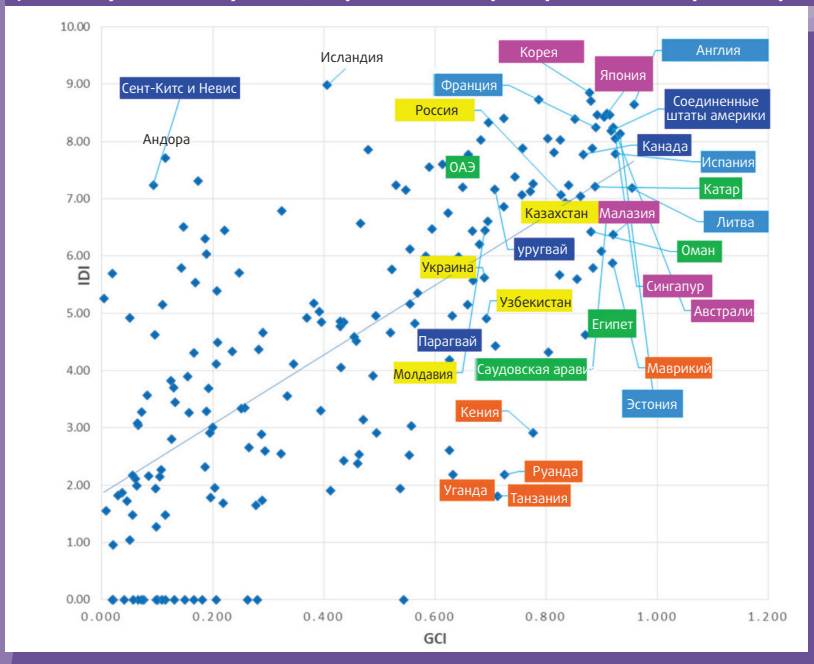
Источник:
Отчет Akamai «2021 State of the Internet / Security Research Report: Adapting to the Unpredictable»
https://www.akamai.com/us/en/resources/our-thinking/state-ofthe-internet-report/

Ежедневные атаки на веб-приложения октябрь 2019 – сентябрь 2020



Источник:
Отчет Akamai «2021 State of the Internet / Security Research Report: Adapting to the Unpredictable»
https://www.akamai.com/us/en/resources/our-thinking/state-ofthe-internet-report/

Позиционирование стран по индексу IDI (ICT Development Index, отражающий уровеньразвития ИТ в стране) и индексу GCI (Global Cybersecurity Index, отражающий приверженность стран вопросам кибербезопасности).



Источник МКЭ:
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Число DDoS-атак заметно увеличилось после введения карантина во многих странах

Источник:
https://www.netscout.com/whitepaper/cyber-security-after-pandemic

Процент входящих почтовых сообщений, которые являлись спамом

Источник:
Источник: https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/

Отзыв сертификатов

Джефф Хьюстон (Geoff Huston)

PKI (Public Key Infrastructure, Инфраструктура открытых ключей) – это система, предназначенная для поддержки электронно-цифровых подписей (ЭЦП) с открытым/закрытым ключом в системе со структурированнным транзитивным доверием. Смысл PKI в том, чтобы обеспечивать доверительные отношения между сторонами, которые, возможно, никогда не встречались и никогда не встретятся друг с другом. Обычно в PKI используются сертификаты X.509 с открытым ключом. Это цифровые объекты, содержащие проверяемое заявление о том, что издавший его удостоверяющий центр (УЦ) убедился — посредством процедур, описанных в его регламенте (Certificate Practice Statement, CPS), — что держатель данной конкретной пары «открытый/закрытый ключ» соответствует определенным критериям, перечисленным УЦ. Затем УЦ публикует сертификат, который связывает имя субъекта (например, личные данные для сертификатов идентичности или имя DNS для сертификатов доменных имен) с открытым ключом владельца, а затем добавляет к этому объекту электронно-цифровую подпись, сгенерированную с помощью закрытого ключа УЦ. Это действие, с одной стороны, проверяемо любой стороной, знающей открытый ключ УЦ, а с другой – не может быть впоследствии отозвано этим УЦ.

Сертификаты X.509 с открытым ключом используются для самых разных целей, так как поддерживают аутентичность, проверку подлинности и атрибуцию. Например, если человек подписывает электронный документ своим сертифицированным закрытым ключом, то затем любой, кто обратится к связанному сертификату идентичности, может проверить (это и есть проверяемость), что документ подписал именно тот самый человек (атрибуция) и что документ не менялся (аутентичность), подразумевая, что проверяющий доверяет практикам выпуска сертификатов в данном удостоверяющем центре.

В контексте Интернета мы наблюдаем рост популярности PKI в онлайне, поскольку веб-сайты публикуют свой контент с помощью протокола Transport Layer Security (TLS) (как видно по префиксу HTTPS в URL). Благодаря веб-PKI клиент может проверить аутентичность удаленного сервера, гарантировать, что транзакцию никто не подслушает, а содержимое транзакции никто не изменит, а также что сервер не может отказаться от проделанной транзакции. Очевидно, такой уровень доверия жизненно важен для Интернета, а следовательно, жизненно важен и фундамент этого доверия – система сертификации владельцев доменных имен. Сертификаты X.509 бывают самого разного вида, и их использование в том или ином контексте обычно определяется параметрами стандартного профиля. Стандартный профиль сертификатов X.509 для использования в Интернете закреплен в стандарте RFC 5280.

Доверие не вечно, поэтому не следует считать вечными и сертификаты. Сертификат X.509 с открытым ключом содержит два поля данных: notBefore и notAfter, - указывающих диапазон времени, в течение которого сертификат можно использовать. (Однако, полноты ради, нельзя не отметить, что на случай вечного доверия в RFC 5280 для поля notAfter предусмотрено значение «forever»!) В управлении сертификатами принято ставить в поле notBefore дату выдачи сертификата, а в поле notAfter – конец периода, предусмотренного контрактом или соглашением между УЦ, выдавшим сертификат, и субъектом. Если субъекту требуется продлить сертификацию после даты в поле notAfter, ему положено обратиться за новым сертификатом до истечения срока действия текущего. Раньше, до прихода Let's Encrypt (https://letsencrypt.org/) на рынок сертификатов SSl/TLS, типичный период действия сертификата составлял 1-2 года. Теперь Let's Encrypt прочно закрепился на рынке, а у его сертификатов период действия составляет 90 дней, поэтому средний по отрасли срок действия сертификата снизился.

В жизни всегда есть место неожиданностям, и сертификаты X.509 не исключение. Бывают ситуации, когда сертификаты нужно помечать как недействительные до наступления даты в поле notAfter. Причины бывают самые разные: от компрометации открытого ключа до выдачи сертификата по ошибке. Или, может быть, владелец сертификата перестал заниматься тем, для чего он ему требовался, или случилось что-то другое – вариантов масса.

Как же можно объявить сертификат недействительным (как еще говорят, отозвать или аннулировать его)? Для этого УЦ, выдавший сертификат, должен удалить его из своего репозитория, чтобы он стал недоступен для загрузки и использования проверяющими сторонами. Но ведь многие проверяющие стороны хранят копии сертификатов локально до истечения срока их действия. Как сообщить такой третьей стороне, что сертификат аннулирован и больше не может применяться для установки доверительных отношений? Например, как можно на практике поставить браузер в известность о том, что сертификат, используемый для установки сеанса TLS, отозван УЦ и сеанс нельзя открывать?

Перед тем как вдаваться в тонкости механизмов отзыва сертификатов, я хочу отметить еще один момент – отмену отзыва

(unrevocation). При отзыве сертификата УЦ создает запись метаданных о том, что сертификат непригоден для пользования, но не выпускает измененного сертификата, который бы зафиксировал факт отзыва. Поэтому в теории УЦ может впоследствии просто убрать метаданные об отзыве сертификата, а поскольку сам сертификат при этом не изменился, его снова можно разместить в репозитории. Статус опубликованного сертификата после удаления метаданных об отзыве станет совершенно тем же, каким он был до отзыва. Это и есть отмена отзыва сертификата. На практике, однако, это очень плохая идея, и УЦ не стоит так поступать. Гораздо лучше обозначить восстановление доверия выпуском нового сертификата с новым серийным номером для того же субъекта. Новый сертификат может использовать ту же пару «открытый/закрытый ключ» или другую, и это решение должен принимать субъект, а не УЦ. А причина того, почему УЦ не следует пытаться срезать углы, отменяя отзыв сертификатов, заключается в том, что УЦ не имеет никакого контроля над обращением сторон с метаданными об отзыве. Вполне возможно (и даже разумно) для проверяющей стороны считать отзыв сертификатов необратимым и просто удалять аннулированные сертификаты из своего локального доверительного набора на все их оставшееся время действия. То есть проверяющая сторона может на практике расценивать отзыв сертификата как необратимое действие. А значит, УЦ ничего не может сделать, чтобы заставить такие проверяющие стороны восстановить состояние доверия к таким отозванным сертификатам, то есть по факту УЦ вынужден и сам расценивать отзыв сертификата как необратимое действие.

Списки отзыва сертификатов (CRL)

В инфраструктуре PKI удостоверяющие центры регулярно публикуют подписанные списки отзыва сертификатов (Certificate Revocation List или CRL). Такой CRL содержит список серийных номеров всех отозванных сертификатов с неистекшим сроком действия, выпущенных именно этим УЦ, с указанием времени отзыва для каждого. Также в CRL указываются дата выпуска самого CRL и ожидаемая дата публикации следующего для этого УЦ. CRL подписываются закрытым ключом удостоверяющего центра, который выпускает CRL. Стандартный профиль CRL для использования в Интернете закреплен в RFC 5280.

CRL задуман как полный документ, в том смысле, что на дату, указанную в нем, он содержит все отозванные сертификаты с неистекшим сроком действия для данного УЦ в данной области охвата (scope). Если областью охвата CRL является весь набор сертификатов, выпущенных этим УЦ, то получается следующее: если у сертификата не истек срок действия и он не значится в CRL, значит, этому сертификату можно доверять до момента выпуска следующего CRL.

Проверяющие стороны могут считать сам CRL действительным, если текущее время позднее, чем времмя выдачи CRL, и раньше следующего времени обновления CRL, при условии, что электронно-цифровая подпись CRL может быть проверена.

Попадание сертификата в CRL, по сути, ставит крест на его действительности, но эффект может наступить не сразу. Бывает, что проверяющие стороны держат у себя локальные копии CRL удостоверяющих центров до времени, обозначенного в поле CRL nextUpdate, а потому не заметят отзыв сертификата до момента публикации следующего CRL.

Чем больше непросроченных отозванных сертификатов, тем массивнее оказывается CRL. Для крупного удостоверяющего центра нагрузка, связанная с обработкой CRL, может оказаться существенной. Отправлять каждый раз полный список всех отозванных сертификатов может показаться немного чересчур, особенно если автор запроса всего-то хотел узнать статус отзыва какого-то конкретного сертификата. Кроме того, генерация CRL не является обязательным требованием к работе удостоверяющих центров. УЦ может по своему выбору публиковать CRL регулярно, либо публиковать CRL и дополнять их так называемыми дельта-CRL, или вообще не публиковать CRL! Поэтому, как правило, CRL не используются конечными клиентами при создании сеансов TLS.

Протокол OCSP

OCSP (Online Certificate Status Protocol) – это альтернатива использования CRL. Клиент генерирует запрос OCSP, содержащий серийный номер сертификата, и отправляет его в УЦ, выдавший этот сертификат. В ответ на запрос УЦ отправляет подписанный отчет о статусе сертификата, где указывает, действителен ли сертификат или отозван. Этот протокол описан в RFC 6960.

Запрос OCSP является объектом ASN.1, содержащим один или несколько серийных номеров сертификатов, которые отправитель просит УЦ проверить.

Ответ OCSP подписывается цифровой подписью УЦ, выпустившего сертификат, или назначенного УЦ респондера. Ответ содержит идентичность респондера, время ответа, ответы по каждому сертификату в запросе и необязательные дополнения. Коды ответов, используемые в OCSP, означают, что сертификат:

- либо годен, что по сути означает – сертификат с таким серийным номером, выданный этим УЦ, не отзывался. В RFC 6960 это объясняется так: «Этот статус не обязательно означает, что сертификат вообще выдавался или что время, в которое был сгенерирован ответ, находится в пределах интервала действия сертификата»;
- либо отозван, что означает – сертификат отозван, но его срок действия не истек; но также этот статус может означать, что данный УЦ не выдавал сертификата с таким серийным номером;
- либо неизвестен, что означает – данный УЦ не распознает указанный серийный номер.

Дополнения к ответу могут включать в себя случайный код (nonce), который криптографически связывает запрос с ответом для предотвращения атак на ответ. Также можно указать ссылку на CRL. Ответы OCSP могут также содержать четыре значения времени:

- thisUpdate – время генерации этой информации о статусе респондером;
- nextUpdate – время, когда будет доступна обновленная информация;
- producedAt – время подписания ответа респондером;
- revocationTime – время отзыва сертификата.

Благодаря наличию этих полей клиент может кэшировать ответ OCSP вплоть до наступления времени nextUpdate.

Ответы OCSP могут генерироваться заранее, при этом время генерации ответа указывается в поле producedAt.

Использование OCSP ставит ряд вопросов о конфиденциальности: раз клиент обращается в УЦ, значит, УЦ становится известно о том, какие клиенты используют этот сертификат и когда – для этого достаточно отследить источник запроса. Кроме того, возникают проблемы с быстродействием, так как генерация запроса OCSP и ожидание ответа требует времени. Запрос не обязан быть единичным, так как осторожный клиент проверит не только статус отзыва сертификата, используемого сервером, но и статус отзыва всех сертификатов этого УЦ, используемых клиентом для формирования цепочки проверки от якоря доверия до этого сертификата.

Одним из вариантов решения проблемы, связанной с проверкой статуса сертификатов по требованию, является упаковка ответа OCSP и самого сертификата в одно целое – эта структура называется OCSP stapling («подшивка» OCSP, описана в RFC 6961). Поскольку ответ OCSP уже подписан и датирован CA, а сервер знает, какой сертификат он передавал клиенту, он также знает, какие запросы OCSP клиент будет направлять для проверки того, не отозвал ли УЦ этот сертификат. Сервер с помощью «подшивки» OCSP прикрепляет ответ OCSP к материалу TLS, используемому при «рукопожатии», и может также прикрепить ответы OCSP для других сертификатов УЦ, которые образуют цепочку проверки этого сертификата клиентом.

Тестирование отзыва сертификатов на разных браузерах

Чтобы поэкспериментировать с тем, как различные браузеры обрабатывают отозванные сертификаты, я с помощью Let's Encrypt сгенерировал сертификат и затем отозвал его. Чтобы подтвердить, что сертификат отозван, я отправил запрос OCSP:

```
$ openssl ocsp -issuer lets-encrypt-x3-cross-signed.pem.txt -serial
0x03DEAA6ADA0286BB5D733188CDB1EBF3cc9B -url http://ocsp.int-x3.letsencrypt.org  -text
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 7EE66AE7729AB3FCF8A220646C16A12D6071085D
          Issuer Key Hash: A84A6A63047DDDBAE6D139B7A64565EFF3A8ECA1
          Serial Number: 03DEAA6ADA0286BB5D733188CDB1EBF3CC9B
    Request Extensions:
        OCSP Nonce:
            0410F996916B40E625BEAC68513525FA1593
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
    Produced At: Mar 10 23:39:00 2020 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 7EE66AE7729AB3FCF8A220646C16A12D6071085D
      Issuer Key Hash: A84A6A63047DDDBAE6D139B7A64565EFF3A8ECA1
      Serial Number: 03DEAA6ADA0286BB5D733188CDB1EBF3CC9B
    Cert Status: revoked
    Revocation Time: Mar 10 23:39:49 2020 GMT
    This Update: Mar 10 23:00:00 2020 GMT
    Next Update: Mar 17 23:00:00 2020 GMT

    Signature Algorithm: sha256WithRSAEncryption
         73:88:aa:a1:1d:ff:5f:5b:eb:30:9d:43:ca:76:b8:3e:70:9f:
         d7:d2:3f:6e:dd:dd:fb:69:0f:16:e4:b3:3c:f3:75:d3:6b:37:
         f4:fa:cc:10:15:8c:cf:59:e0:f4:2a:60:d9:4c:5e:b2:df:24:
         d9:a1:20:b2:7e:14:d8:d0:03:92:97:9e:be:b3:e5:4e:c9:6c:
         db:96:8c:ff:6c:c7:4f:cf:88:35:bb:52:90:4f:6e:b9:51:70:
         f1:51:93:9d:de:b0:91:44:69:12:47:15:b2:18:c3:0d:bd:d5:
         af:01:ff:c3:8d:c0:31:94:87:e0:0e:06:18:35:7a:a8:4a:dd:
         2a:e4:61:2a:6d:db:6e:9f:87:d4:9f:79:25:17:f5:7a:e3:4d:
         7b:44:95:56:d4:ff:b2:38:50:f6:58:7c:d3:97:0c:e6:ab:2c:
         f6:2b:9a:55:a8:63:c6:f4:b9:97:2b:21:a2:bf:38:0d:91:e6:
         af:64:22:b8:50:b4:e8:70:27:ee:60:0d:fd:96:6e:b2:54:f8:
         38:ed:14:31:ca:1e:3f:c3:7f:ae:f5:d3:ff:9b:75:bf:4d:12:
         e7:1b:9a:62:a8:d9:c0:a4:8f:48:33:b2:f5:ea:d0:e9:27:e3:
         4f:ed:c3:1a:80:3a:1b:94:27:7c:90:56:c3:b3:65:7a:6e:5f:
         94:a9:56:79
WARNING: no nonce in response
Response verify OK
0x03DEAA6ADA0286BB5D733188CDB1EBF3cc9B: revoked
        This Update: Mar 10 23:00:00 2020 GMT
        Next Update: Mar 17 23:00:00 2020 GMT
        Revocation Time: Mar 10 23:39:49 2020 GMT
```

Служба OCSP на сервере Let's Encrypt использует семидневные ответы OCSP. Для защиты ответа от повтора я запросил случайный код (nonce), но OCSP-сервер Let's Encrypt не использовал его в ответе.

Потом я протестировал поведенние различных браузеров и операционных систем при попытке подключения к сайту, использующему этот отозванный сертификат, и результаты свел в таблицу 1. Сервер не был настроен на «подшивку» OCSP, поэтому браузер клиента должен был обнаружить отзыв посредством OCSP. В приведенной ниже таблице ДА означает, что браузер обнаружил отзыв сертификата, а НЕТ – что браузер подключился к сайту и объявил подключение безопасным. В таблице я также указал номера версий платформы и браузера, использованных в этом маленьком эксперименте.

Таблица 1.
Опознание отозванных сертификатов браузерами

Платформа	Chrome	Firefox	Opera	Safari	Edge
Mac OS X 10.15.3	ДА 80.0.3987.132	ДА 73.0.1	ДА 67.0.3575.53	ДА 13.0.5	
iOS 13.3.1	ДА 80.0.3987.95	ДА 23.0	НЕТ 16.0.15	ДА 13.3.1	
Android 10	НЕТ 80.0.3987.132	НЕТ 68.6.0	НЕТ 56.1		
Windows 10	НЕТ 80.0.3987.132	ДА 74.0	НЕТ 67		ДА 44.18362

Вскрывшиеся в этом эксперименте различия в поведении браузеров обусловлены как различиями между сервисами разных платформ, так и выбором API-опций тем или иным приложением при взаимодействии с сервисами безопасности своей платформы. В наши дни подавляющее большинство людей в Интернете пользуется браузером Chrome на платформе Android. То есть получается, что большинство пользователей Интернета не проверяет сертификаты на действительность.

Стоит ли отзыв сертификатов свеч?

На первый взгляд – что за странный вопрос? Если закрытый ключ скомпрометирован, его нельзя использовать. С его помощью хакер может подменить сайт другим, а это недопустимо. Чтобы скомпрометированный ключ перестали принимать, необходимо распространить информацию о том, что данная пара ключей более недействительна, а это и достигается путем отзыва сертификата открытого ключа. По крайней мере, так думали авторы идеи сертификатов X.509 и их отзыва.

Но отзыв сертификатов используется не всегда – и даже не всегда полезен. Например, у DNSSEC, тоже использующей открытые/закрытые ключи, нет функции отзыва. Если закрытый ключ скомпрометирован, то решением будет переподписать зону свежим ключом и полагаться на то, что данные управления кэшем DNS TTL «вымоют» старые значения ключа из различных кэшей DNS. В DNS значения TTL обычно исчисляются часами или днями, а не месяцами

или даже годами, как у веб-сертификатов PKI. Это означает, что окно уязвимости вследствие компрометации ключа в DNSSEC гораздо короче, чем в веб-PKI. Возможно, потому отзыв сертификатов в веб-PKI и является гораздо большей проблемой, чем в DNSSEC.

Получается, что при использовании открытого/закрытого ключа есть сценарии, в которых механизмы отзыва не считаются нужными. А как насчет обычной схемы использования сертификатов в веб-PKI? Есть ли польза от отзыва сертификатов? Или это просто еще один способ увеличить риск, добавив в структуру новые точки потенциальной уязвимости?

Для работы CRL по запросу и OCSP требуется, чтобы были доступны сервисные точки управляющего центра. В случае CRL можно полагаться на локальное кэширование списков CRL, что в известной степени смягчает требования к доступности УЦ, но для OCSP по запросу вариантов нет. Сервер OCSP должен быть доступен, мало того – доступен на скорости, соразмерной жестким временным ограничениям на установку сеанса TLS в приложении.

Для OCSP такая ситуация возможна не всегда, поэтому нужно внимательно изучить, что произойдет, если это не так. Если ответа на запрос OCSP нет, то как должен поступить клиент? Можно продолжить установку связи (принцип soft-fail), сделав клиента уязвимым к потенциальным опасностям, от которых и должен был защищать его OCSP. А можно поосторожничать и отказать (hard-fail), что чревато необоснованными блокировками. Сервисная точка OCSP становится точкой потенциального отказа, а в мире, и так набитом ограничениями доступа и ненадежными соединениями, последнее, что нужно – это создавать новые точки, где соединение может разорваться. Кроме того, принцип hard-fail сопряжен еще и с риском превратить серверы OCSP в лишнюю уязвимость при DoS-атаках. Похоже, что многие клиентские приложения и сервисные библиотеки операционных систем при отсутствии ответа OCSP действуют по принципу soft-fail. Это тоже уязвимость: хакер, находящийся на пути между пользователем и УЦ, может увидеть незашифрованный запрос OCSP и просто заблокировать его. Тогда функция проверки сертификата на клиенте отработает по soft-fail и сочтет отозванный сертификат действительным. В результате клиент будет доверять отозванному сертификату.

Можем ли мы сделать OCSP надежнее и противостоять атакам, удаляющим OCSP? Если проблемой является перехват запросов или ответов OCSP, то, возможно, имеет смысл перейти на обязательную «подшивку» OCSP. Это предложение описано в давно устаревшем интернет-драфте 2013 года (draft-hallambaker-muststaple-00.txt), согласно которому сервер, сообщающий сертификат при открытии сеанса TLS, также обязан был прикрепить к сертификату текущую информацию OCSP в качестве расширения. Поскольку флаг must staple находится внутри подписанного сертификата, хакер не может удалить его во время настройки сеанса TLS. В этом предложении УЦ (или, возможно, оригинальный субъект) предписывает всем серверам, использующим данный сертификат, использовать также «подшивку» OCSP. Так удается справиться с угрозами удаления OCSP и нарушения конфиденциальности, не добавляя к рукопожатию TLS дополнительных задержек на проверку действительности сертификата, которые неизбежны при отдельном обмене данными между клиентом и сервером удостоверяющего центра OCSP. В результате окно уязвимости из-за компрометации сертификата сокращается с нескольких лет (с текущего момента до прекращения срока действия сертификата) до нескольких дней (срок действия ответа OCSP).

С отзывом сертификатов связаны и другие проблемы – в том смысле, что отзыв не пресекает атаки, использующие скомпрометированные ключи. Хакер может сгенерировать с тем же скомпрометированным закрытым ключом новые учетные данные, а по ним повторно сертифицировать скомпрометированную службу. К тому моменту, когда компрометация исходного ключа будет обнаружена, хакер будет использовать новые ключи и новый сертификат, и теперь первоначальному владельцу службы придется доказывать удостоверяющему центру, выдавшему новый сертификат, что последний необходимо отозвать. Ловкий взломщик может повторить процедуру ресертификации несколько раз, все больше затрудняя усилия по вычистке незаконно полученных сертификатов из PKI.

Возможно, проблему отзыва лучше всего решить, просто отказавшись от сертификатов с большим сроком действия. Еще девять лет Адам Лэнгли (Adam Langley) из Google заметил:

> Гораздо лучшим решением было бы ограничить срок действия сертификатов несколькими днями, а об отзыве просто забыть. Нет, менять закрытый ключ каждые несколько дней не надо, только сам сертификат. А сертификат относится к открытым данным, поэтому серверы могли бы просто загружать обновленные сертификаты по HTTP, периодически и автоматически (как при «подшивке» OCSP). Клиентам не нужно было бы возиться с проверками на отзыв (процедура очень сложная и долгая), УЦ не пришлось бы платить за большие серверные мощности с защитой от DDoS, а отзыв бы реально заработал. Если УЦ лег на шесть часов – ну и черт с ним. Проблема возникает только тогда, когда УЦ лежит несколько дней. А если сертификат нужно «отозвать», просто не возобновляйте его.
> https://www.imperialviolet.org/2011/03/18/revocation.html

Есть ли другие подходы к отзыву сертификатов?

Как всегда, эта проблема тоже решается методом «а давайте используем DNS». В сравнительно недавнем интернет-драфте (от 2017 года) предлагается сделать OCSP типом записей ресурсов DNS (draft-pala-odin-02.txt). Запрос OCSP закодируется в имя запроса DNS, объединяя в себе и запрос, и ответ. Например, на запрос типа OCSP RR с именем запроса 123456.ca1.example.com последует ответ с указанием статуса OCSP у сертификата с серийным номером 123456, выпущенного УЦ с именем точки публикации ca1.example.com. Скорее всего, для аккуратной реализации потребуется также подписывать зону DNS по DNSSEC, хотя, поскольку сама запись OCSP подписана УЦ, основной смысл подписания по DNSSEC будет заключаться в гарантии наличия и актуальности.

При этом методе DNS помогает справиться с уязвимостью сервисной точки OCSP в удостоверяющем центре, поскольку

эти данные кэшируются на рекурсивных резолверах DNS. Там, где такие запросы широко используются, кэширование DNS на резолверах невероятно повысит скорость запросов, даже с учетом проверки DNSSEC. Правда, если данных не будет в локальном кэше резолвера DNS, процедура будет гораздо медленнее обычного запроса и ответа OCP.

Mozilla возродила обсуждение подходов на базе CRL, разрешив проблему с объемом CRL. Ее метод – сжать эффективный размер CRL с помощью Bloom Filters, используя технику, которую назвали CRLite (https://blog.mozilla.org/security/ 2020/01/09/crlite-part-2-end-to-end-design/). Применение этого метода показало сокращение объемов данных CRL: список серийных номеров всех выданных и не отозванных сертификатов на 6,7 Гб ужался до каких-то 1,3 Мб. Mozilla предлагает использовать эту технику для больших CA и возвращаться к OCSP там, где данные CRL не настроены как фильтр. Таким образом авторы метода пытаются устранить дополнительные задержки в OCSP по запросу, не полагаясь на поддержку must staple OCSP на серверной стороне, которой может и не быть.

Итак, на чем мы остановились?

УЦ выдают долгоживущие сертификаты, а это значит, что компрометация пары ключей может вылиться в уязвимость, которая будет оставаться незакрытой годами. Мы хотели бы аннулировать сертификаты быстрее. Такая возможность предоставляется списками отзыва сертификатов (CRL), но они разбухают до крупных размеров, а потому доставка «просто на всякий случай» такой горы данных клиентам вызывает проблемы. Мы обратились к OCSP, чтобы можно было запросить статус отзыва отдельного сертификата, но из-за сомнений в надежности OCSP клиентские системы применяют подход soft-fail, из-за чего доверие к отозванным сертификатам сохраняется.

Доверие

Панацеи здесь не существует, и каждый из подходов к отзыву сертификатов представляет собой компромисс.

Долгосрочные сертификаты с большой стоимостью создания жизнеспособны, но только при наличии быстрого и надежного механизма их отзыва, а создать его пока не удалось. CRL и OCSP работают не мгновенно, но могут значительно сузить временное окно уязвимости после компрометации закрытого ключа, хотя есть проблемы с устойчивостью CRL и различных вариантов OCSP.

Можно последовать примеру Let's Encrypt и выдавать лишь краткосрочные сертификаты, генерируемые с помощью автоматизированных процедур. Поскольку такие сертификаты недолговечны, их отзыв не создает больших проблем, а в перспективе можно выдавать сертификаты и на еще более короткий срок. Если списки отзыва обновляются раз в неделю, то сертификаты с недельным сроком действия можно вообще не отзывать, поскольку наличие или отсутствие отзыва мало что изменит для проверяющих сторон.

Но если мы выберем путь краткосрочных сертификатов, зачем тогда нам вообще X.509? Может быть, проще использовать DANE, закодировать ключи в DNS и обеспечение необходимой аутентичности возложить на DNSSEC, а о времени жизни кэшированных открытых ключей пусть позаботится механизм DNS TTL? С помощью расширений цепочек DNSSEC можно реализовать безопасное рукопожатие (security association handshake), при котором сервер отправляет клиенту ответ со своим открытым ключом, подпись DNSSEC и связанные ответы проверки DNSSEC, не выполняя вообще никаких запросов в DNS. Таким образом можно, подобно «подшивке» OCSP, внедрить «подшивку» DANE и цепочек DNSSEC, полностью устранив задержку запроса DNS.

Эта история еще далека от завершения. Мы наблюдаем скоростные атаки, где весь процесс внедрения, обмана и кражи данных занимает всего несколько часов, а вовсе не дни или недели. А контрмеры, на которые мы полагаемся сегодня, включая журналы прозрачности сертификатов и нерегулярное использование OCSP, оставляют в защите учетных данных дыры, которые исчисляются днями вместо секунд.

Приходится сделать неутешительный вывод, что в вопросах интернет-безопасности мы безосновательно полагаемся на неповоротливую систему защиты, чье время реакции в нынешнем наносекундном мире измеряется в лучшем случае неделями.

Ссылки и дополнительная литература

1. RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", D. Cooper и др., май 2008 г.
2. https://tools.ietf.org/html/rfc5280
3. RFC 6960, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP", S. Santesson и др., июнь 2013 г.
4. https://tools.ietf.org/html/rfc6960
5. RFC6961, "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", Y. Pettersen, июнь 2013 г.
6. https://tools.ietf.org/html/rfc6961
7. "X.509v3 Extension: OCSP Stapling Required", Internet Draft, P. Hallam-Baker, апрель 2013 г.
8. https://tools.ietf.org/id/draft-hallambaker-muststaple-00.txt
9. "OCSP over DNS (ODIN)", Internet Draft, M. Pala, ноябрь 2017 г.
10. https://tools.ietf.org/id/draft-pala-odin-02.txt
11. "Revocation Doesn't Work", Adam Langley, март 2011 г.
12. https://www.imperialviolet.org/2011/03/18/revocation.html
13. "No, don't enable revocation checking", Adam Langley, апрель 2014 г.
14. https://www.imperialviolet.org/2014/04/19/revchecking.html
15. "OCSP Stapling: How CloudFlare Just Made SSL 30% Faster", Matthew Prince, октябрь 2012 г.
16. https://blog.cloudflare.com/ocsp-stapling-how-cloudflare-just-made-ssl-30/
17. "High-reliability OCSP stapling and why it matters", Nick Sullivan, июль 2017 г.
18. https://blog.cloudflare.com/high-reliability-ocsp-stapling/
19. "Revocation is Broken", Scott Helme, июль 2017 г.
20. https://scotthelme.co.uk/revocation-is-broken/
21. "The Problem with OCSP Stapling and Must Staple and why Certificate Revocation is still broken", Hanno Böck, май 2017 г.
22. https://blog.hboeck.de/archives/886-The-Problem-with-OCSP-Stapling-and-Must-Staple-andwhy-Certificate-Revocation-is-still-broken.html

Биометрия в информационной безопасности. Настоящее и перспективы биометрической аутентификации

Коннова Н. С., к.т.н., доцент МГТУ им. Н. Э. Баумана

В современном мире людям постоянно приходится подтверждать свою личность: для получения доступа к компьютеру, смартфону и различным интернет-ресурсам. Для удобства пользователей многие повседневные вещи, такие как поход в банк, оформление различных документов и оплата счетов перенесены в Интернет. Вместе с этим остро встала проблема защиты личных данных, а также предоставления авторизованного доступа. Приходя в банк, люди подтверждают свою личность при помощи паспорта, но как быть в случае с интернет-банкингом? На протяжении многих лет для получения доступа к интернет-ресурсам использовались пароли, идеология которых заключается в том, что их знают только полноправные владельцы, но, к сожалению, утрата анонимности пароля влечет за собой колоссальные последствия, ведь пароль от интернет-банка равнозначен ключу от сейфа и предоставляет злоумышленнику безграничный доступ к финансам полноправного пользователя. Таким образом, вопрос идентификации и аутентификации в Интернете становится одной из главных проблем нашего времени. С развитием информационных технологий стало появляться много способов подтверждения личности, в этой статье хотелось бы сконцентрировать внимание на одном из наиболее интересных и актуальных – на биометрической идентификации и аутентификации.

Что такое биометрия? В самом общем смысле биометрия – это наука, основанная на измерении и описании характеристик тела живых существ [1]. Например, рисунок отпечатков пальцев, «геометрия» лица или рисунок сетчатки глаза – это наиболее распространенные формы биометрических данных, но далеко не все. Исследователи утверждают, что у любого человека имеется множество уникальных параметров тела – то, как человек сидит или ходит, форма уха, расположение вен на руках и многое другое. Именно из-за уникальности этих данных биометрические признаки человека обрели такую популярность в вопросах, связанных с необходимостью подтверждения личности.

Биометрические данные можно условно разделить на три группы [2]:

- биологическая биометрия;
- морфологическая биометрия;
- поведенческая биометрия.

Все, что касается генетических особенностей человека (ДНК, кровь и др.), относят к биологической биометрии. Ее можно оценить при помощи образцов жидкостей. Морфологическая биометрия – наиболее популярная в прикладном применении, это внешние особенности человека: форма лица, отпечаток пальца и т.п. Поведенческая биометрия подразумевает некоторые шаблоны, которые прослеживаются в поведении человека: походка, манера речи или мимика.

Традиционные пароли всегда были слабым местом систем безопасности ввиду того, что их легко скомпрометировать. Биометрия, в свою очередь, является куда более мощным решением, поэтому она обретает все большую популярность. Наиболее распространенными примерами использования биометрии для обеспечения безопасности являются распознавание лиц и голосов, а также сканирование отпечатков пальцев.

В начале статьи мы говорили о том, что биометрия используется для идентификации и аутентификации, но в чем же разница между этими терминами? Идентификация – это процедура распознавания субъекта по его идентификатору, а аутентификация – процедура проверки подлинности [3]. Если переводить эти определения в термины биометрии, то биометрическая идентификация – это распознавание личности, то есть, предположим, существует база данных, хранящая образцы выбранного биометрического признака всех людей, которым требуется предоставить доступ к какому-либо ресурсу. При сравнении предоставленного признака со всеми, хранящимися в базе данных, система определяет, является ли человек, обращающийся к некой системе, тем, чьи признаки в ней хранятся, и кем именно. Биометрическая аутентификация – это непосредственно процесс сравнения предоставленного признака с хранящимся в базе данных, для определения того, имеет ли заявитель право на получение доступа к

системе [4]. Авторизацией же называют предоставление конкретному лицу или группе лиц прав на выполнение определённых действий.

Разобравшись с тем, что такое биометрические данные, можно предположить, что их использование является высоконадежным способом защиты информации от несанкционированного доступа. Это действительно так, но использование биометрии в качестве механизма аутентификации влечет за собой также и некоторые осложнения и последствия.

Первой проблемой здесь является ложноотрицательное срабатывание сканера [5]. Например, система, проверяющая подлинность пользователя по отпечатку пальца, может отказать в доступе из-за пореза на пальце, грязи, попавшей на сканер, или излишней влаги. В случаях, где биометрические данные являются одним из нескольких вариантов авторизации в системе, например, в смартфонах, где при неверном считывании отпечатка пальца пользователю предлагается ввести пароль, это не является проблемой.

В системах, где биометрические данные являются единственным способом подтверждения личности, подобное приведет к тому, что полноправный пользователь не сможет пройти проверку личности.

Вторая проблема – это тот факт, что о развитии технологий знают не только законопослушные граждане, но и злоумышленники. Уже несколько лет существуют, к примеру, технологии, позволяющие на видеозаписи заменять лицо одного человека на другого, что может позволить хакерам обмануть сканер лица. Достаточно иметь фотографию потенциальной жертвы, чтобы предоставить сканеру динамический видеоклон человека. Если говорить о сканировании отпечатков пальцев, то здесь тоже не все гладко: их можно подделать с помощью латексной формы, перчатки или даже фотографии ладони с высоким разрешением. Данную проблему пытаются решить разработкой все новых методов и видов биометрической аутентификации.

Самая серьезная проблема – это компрометация биометрических данных. Если злоумышленники украдут пароль, то его можно сменить за пару минут. Восстановление украденной кредитной карты или токена займет больше времени, но все же не будет большой проблемой для владельца. Но что произойдет, если у человека украдут его биометрию? Мы говорили о том, что биометрические данные принадлежат человеку с самого рождения и они уникальны. Поэтому при краже таких данных происходит настоящая кража личности. Человек не может позвонить куда-либо и заказать себе новое лицо или отпечатки пальцев просто потому, что злоумышленники каким-либо образом получили доступ к их полноценным копиям. И это является серьезным риском использования биометрии.

В настоящее время существуют два класса методов биометрической аутентификации: основанные на статических методах и основанные на динамических методах. Рассмотрим самые актуальные решения обоих классов.

Статические методы биометрической аутентификации

Статические методы основаны на биометрических характеристиках человека, которые присутствуют у него от рождения. Рассмотрим некоторые из них подробно.

Аутентификация по геометрии лица отличается наиболее сложной технической реализацией. Метод основан на построении трёхмерной модели человеческого лица, для этого выделяются контуры различных элементов и характеристические точки лица пользователя, вычисляется расстояние между ними. Для определения уникального шаблона необходимо от 12 до 40 характерных элементов. Уникальный шаблон должен учитывать множество вариаций изображения [7]. Он состоит в том, что на объект (лицо) проецируется сетка. Далее камера делает снимки со скоростью десятки кадров в секунду, и полученные изображения обрабатываются специальной программой. Луч, падающий на искривленную поверхность, изгибается – чем больше кривизна поверхности, тем сильнее изгиб луча. Изначально при этом применялся источник видимого света, подаваемого через «жалюзи». Затем видимый свет был заменен на инфракрасный, который может работать в условиях низкой освещённости или даже в полной темноте. По полученным снимкам восстанавливается 3D-модель лица, на которой выделяются и удаляются ненужные помехи (прическа, борода, усы и очки). Затем производится анализ модели — выделяются антропометрические особенности, которые в итоге и записываются в уникальный код, заносящийся в базу данных. Время захвата и обработки изображения составляет 1-2 секунды для лучших моделей.

Полные данные об FRR (False Rejection Rate, ошибка первого рода) и FAR (False Acceptance Rate, ошибка второго рода) для алгоритмов этого класса на сайтах производителей открыто не приведены. Но для лучших моделей фирмы Bioscript (3D EnrolCam, 3D FastPass) (см. рис. 1), работающих по методу проецирования шаблона, при FAR = 0,0047% FRR составляет 0,103%. Следует заметить, что величины ошибок первого и второго рода взаимосвязаны, и попытки снизить одну из них неизбежно приводят к росту второй. В области ИБ наиболее критической считается ошибка второго рода (допуск к ресурсу нелегитимного пользователя), поэтому ее стремятся минимизировать, накладывая на ошибку первого рода (недопуск к ресурсу легитимного пользователя) при этом разумные ограничения. Считается, что статистическая надежность описанного метода сравнима с надежностью метода аутентификации по отпечаткам пальцев [8].

Рисунок 1.
Bioscript 3D EnrolCam [7].

В качестве преимуществ метода можно выделить отсутствие необходимости контактировать со сканирующим устройством и низкую чувствительность к внешним факторам как на самом человеке (появление очков, бороды, из-

менение прически), так и в его окружении (освещенность, поворот головы). Также отмечается высокий уровень надежности, сравнимый с метом аутентификации по отпечаткам пальцев.

Основной недостаток метода – высокая стоимость оборудования. Имеющиеся в продаже комплексы превосходят по цене даже сканеры радужной оболочки глаза. Кроме того, изменения мимики лица и помехи на лице ухудшают статистическую надежность метода. Метод еще недостаточно хорошо разработан, особенно в сравнении с давно применяющейся дактилоскопией, что затрудняет его широкое применение.

Аутентификация по рисунку вен. В основе метода – инфракрасная (ИК) камера, делающая снимки внешней или внутренней стороны ладони. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК-излучение. В результате степень отражения уменьшается, и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку.

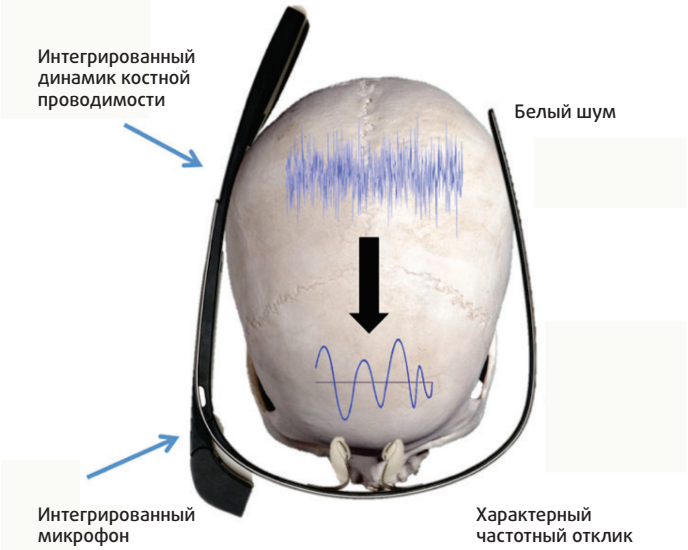
Значение FRR и FAR приведено для сканера Palm Vein (см. рис. 2). Согласно данным разработчика, при FAR 0,0008% FRR составляет 0,01%. Более точные данные не раскрывает ни одна фирма-производитель [9].

Основные преимущества метода – отсутствие необходимости контактировать со сканирующим устройством и высокая достоверность: статистические показатели метода сравнимы с показаниями радужной оболочки. Следует отметить и скрытость характеристики. В отличие от всех вышеприведённых примеров биометрии, эту характеристику очень затруднительно получить от человека «на улице» в преступных целях, например, сфотографировав его фотоаппаратом.

Недостатки метода связаны с чувствительностью сканера и возможными изменениями вен человека. Недопустима засветка сканера солнечными лучами и лучами галогеновых ламп. Некоторые возрастные заболевания, например, артрит сильно ухудшают показатели точности. Метод пока менее изучен в сравнении с другими статическими методами биометрии.

Рисунок 2. Пример устройств со сканером Palm Vein [8].

Рисунок 3. Интеграция SkullConduct в Google Glass [10].



Аутентификация по структуре черепа. Команда исследователей Университета Штутгарта провела интересный эксперимент, пропустив идентичные звуковые волны через черепа десяти разных людей. Полученные результаты [10] легли в основу создания устройства SkullConduct. Как оказалось, черепа у всех людей индивидуальны, поэтому звуковые волны, проходя через них, имеют разные характеристики, что может быть в дальнейшем использовано в качестве новой формы идентификации и аутентификации. Ее эффективность достигает 97%. Гарнитура SkullConduct, состоящая из двух проводящих пластин, крепится на верхней части скул рядом с ушами. В настоящее время SkullConduct проходит испытания: исследователи работают над повышением его эффективности.

Основные преимущества метода – скрытость характеристики и возможность интеграции системы в носимую электронику (см. рис. 3). Главные же недостатки заключаются в необходимости контакта с человеком и шумом, издаваемым при использовании.

Динамические методы биометрической аутентификации

Неизменяемость и открытость биометрических характеристик, используемых в статических методах, допускают подделку биометрического ключа. Вследствие этого ряд преимуществ имеет использование динамических методов биометрической аутентификации.

Аутентификация по характеристикам сердца. В сентябре 2017 года стало известно о новом способе биометрической аутентификации – по сердцу. Такую разработку придумали в Университете Баффало. Ее суть заключается в использовании так называемого низкоуровневого допплеровского радара, который позволяет каждые 8 секунд определять форму, размер и ЭКГ сердца человека. Если в течение этого времени сердце пользователя,

Рисунок 4. Использование смартфона в роли сканера [11].

информация о котором загружена в систему, не будет обнаружено, компьютер будет заблокирован.

Авторы проекта утверждают [11], что сканер безвреден для человеческого организма, поскольку его излучение составляет всего 5 мВт, что соответствует менее 1% излучения от современных смартфонов. Кроме того, в прототипе устройства сам смартфон выступает в роли сканера сердечной активности (см. рис. 4).

Преимущества данного метода – это не просто отсутствие необходимости контактировать со сканирующим устройством, а возможность работы на расстоянии до 30 м. Это делает его потенциально востребованным и удобным способом для безошибочной проверки личности в местах массового скопления людей. Кроме того, система отличается низким энергопотреблением, что позволит эффективно использовать ее не только в стационарных компьютерах, но и в мобильных устройствах.

В качестве основного недостатка выступает возможность изменений формы и ритма работы сердца при некоторых заболеваниях.

В дальнейшем появились различные вариации авторизационных методов, использующих параметры и их комбинации работы сердечно-сосудистой системы пользователя: по микровибрациям сердца, по сердечному ритму и др.

Аутентификация по движениям губ. Технологию аутентификации личности по губам разработали и запатентовали в Баптистском университете Гонконга в 2015 году. В основе ее – распознавание характерных движений губ с учетом текстуры и мимики, например, во время произношения пароля. Ученые утверждают [12], что подделать такого рода биометрический след практически невозможно.

Идентификация по губам может применяться для повышения эффективности систем безопасности и служить дополнением к таким методам получения доступа, как распознавание лиц, сканирование сетчатки глаза, дактилоскопии. Пилотное применение технологии планируют внедрить для обслуживания в банкоматах и для контроля доступа в общественные места.

Преимуществом технологии является возможность выступать дополнением к уже существующему сканеру лица, значительно усложняя задачу по изготовлению копии. Недостатком является необходимость продолжительного сканирования различных эмоций для создания точного образа.

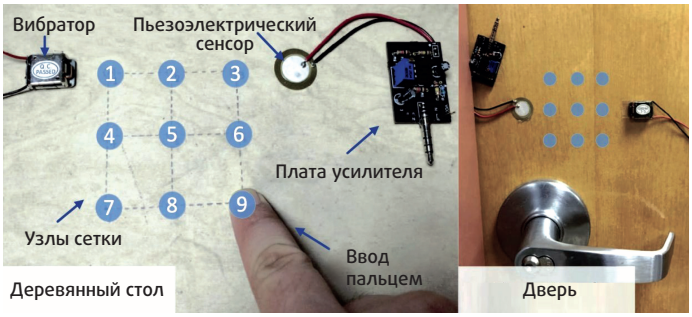
Аутентификация по микровибрациям пальцев. Инженеры Рутгерского университета в Нью-Брансуике предложили осенью 2017 года еще один интересный динамический метод авторизации людей – по микровибрациям пальцев. Исследователи исходят из того, что для каждого пользователя они будут уникальными, и соответственно, таким образом может получиться индивидуальная сигнатура, подделать которую будет как минимум очень сложно.

Система, получившая название VibWrite, работает достаточно просто: к твердой поверхности – будь то дерево, метал, пластик или стекло – крепится недорогой вибродвигатель и датчик; когда человек касается пальцем поверхности, в вибрации двигателя вносятся помехи, которые считываются как уникальные сигнатуры (см. рис. 5).

При этом уникальными они будут для каждого пальца, а их кратковременность обеспечивает повышенную надежность авторизации, особенно по сравнению со вводом кода, графическими ключами, а также, как уверяют разработчики технологии, с традиционными биометрическими средствами [13].

Преимущество исследуемой технологии в малой стоимости производства самого сканера и в возможности комбинации со сканерами отпечатков пальцев. Недостаток технологии – в малой изученности: тестирование производилось в закрытых помещениях. Как она будет функционировать на улице в сложных погодных условиях, пока не ясно. Испытания «в поле» еще впереди.

Рисунок 5. Установка VibWrite [13].



Стандарт биометрии для авторизации на сайтах

Стандарт под названием Web Authentication (WebAuthn), разработанный Консорциумом Всемирной Паутины (W3C), определяет программный интерфейс (API), который позволит сайтам в сети Интернет или веб-сервисам использовать приложения, аппаратные токены или биометрические данные для авторизации пользователей вместо паролей или в качестве второго этапа двухфакторной аутентификации. Так, WebAuthn предлагает использовать для аутентификации на сайтах и в приложениях аппаратные ключи, отпечатки пальцев, распознавание лиц, сканы радужной оболочки глаза и прочую биометрию. WebAuth является частью проекта FIDO2 (см. рис. 6).

Функционал уже доступен в Mozilla Firefox и в течение нескольких следующих месяцев появится в Microsoft Edge и Google Chrome. О поддержке WebAuthn также заявили разработчики Opera. Кроме того, к соответствующей рабочей группе недавно присоединилась команда разработчиков движка Webkit (используется в Apple Safari и App Store).

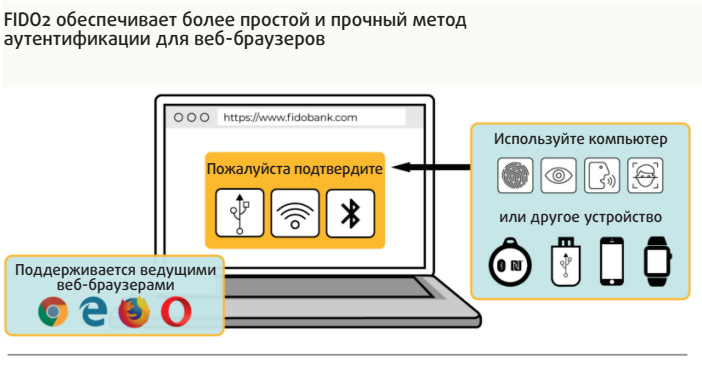
Разработчики, желающие реализовать поддержку WebAuthn, должны реализовать поддержку JavaScript API. Пользователям для авторизации на сайтах или в сервисах с поддержкой нового стандарта придется использовать соответствующие устройства или приложения. В связи с этим Google и Microsoft представят в этом году так называемые аутентификаторы FIDO2. Все устройства под управлением Windows 10 получат их через функцию Windows Hello, а большинство версий Android – через Android Fingerprint API [14].

Заключение

С распространением систем авторизации, основанных на биометрических методах, растет и число способов для их обхода. Наиболее перспективными из исследованных технологий представляются те, которые дополняют уже существующие комплексы возможностью последовательного или параллельного использования. Так, безопасность современных систем по распознаванию лица может быть улучшена возможностью учета мимики и тепловых карт. Дактилоскопические системы могут считывать микровибрации пальца и костную проводимость. Таким образом, задача подделки биометрических характеристик будет сильно усложнена, без потери скорости работы и удобства использования системы.

Итак, подводя итог, можно сказать, что, безусловно, биометрическая аутентификация весьма надежна и удобна. Нет необходимости носить с собой какой-либо ключ или карту, тем более не нужно держать в голове множество разных паролей – все, что нужно, всегда с собой. Но используя подобные технологии, нужно всегда задумываться о рисках и последствиях, ведь абсолютной защиты не существует, и любая система, так или иначе, уязвима.

Рисунок 6. Схема-описание стандарта FIDO 2.0 [14].



Список литературы

1. Блог компании ИНТЕМС [Электронный ресурс]. URL: https://securitytyrussia.com/blog/biometriya.html#33 (дата обращения 25.03.2021)
2. Kaspersky Resource Center [Электронный ресурс]. URL: https://www.kaspersky.com/resource-center/definitions/biometrics (дата обращения 25.03.2021)
3. IT-уроки [Электронный ресурс]. URL: http://it-uroki.ru/uroki/bezopasnost/identifikaciya-autentifikaciya-avtorizaciya.html (дата обращения 25.03.2021)
4. Биометрия в информационной безопасности [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/biometriya-v-informatsionnoy-bezopasnosti/viewer (дата обращения 25.03.2021)
5. Protectimus Solutions [Электронный ресурс]. URL: https://www.protectimus.com/blog/biometric-authentication-pros-and-cons/ (дата обращения 25.03.2021)
6. Search Security [Электронный ресурс]. URL: https://searchsecurity.techtarget.com/definition/biometric-authentication (дата обращения 25.03.2021)
7. Брагина Е. К., Соколов С. С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития // Вестник АГТУ. 2016. №1 (61). URL: https://cyberleninka.ru/article/n/sovremennye-metody-biometricheskoy-autentifikatsii-obzor-analiz-i-opredelenie-perspektiv-razvitiya (дата обращения: 27.03.2021)
8. Ворона В. А., Костенко В. О. Биометрические технологии идентификации в системах контроля и управления доступом // Computational nanotechnology. 2016. №3. URL: https://cyberleninka.ru/article/n/biometricheskie-tehnologii-identifikatsii-v-sistemah-kontrolya-i-upravleniya-dostupom (дата обращения: 27.03.2021)
9. «Forget your PIN, Barclays just needs your veins» [Электронный ресурс].URL: https://www.telegraph.co.uk/finance/newsbysector/banksandfinance/11076624/Forget-your-PIN-Barclays-just-needs-your-veins.html (дата обращения: 27.03.2021)
10. «SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull» [Научная статья]. URL: http://simpleskin.org/papers/SOB2016.pdf (дата обращения: 23.02.2021)
11. Lei Wang, et all. Unlock with your heart: heartbeat-based authentication on commercial mobile phones // Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., Vol. 2, No. 3, Article 140. Sept. 2018. URL: https://samsonsjarkal.github.io/KeSun/files/ubicomp18Heartbeat.pdf (дата обращения: 27.03.2021)
12. «В Гонконге нашли новый способ идентификации – по губам» [Электронный ресурс]. URL: https://digital.report/pretsedent-v-gonkonge-nashli-novyiy-sposob-identifikatsii-po-gubam/ (дата обращения: 27.03.2021)
13. Jian Liu, Chen Wang, Yingying Chen, Nitesh Saxena. VibWrite: Towards Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration // CCS'17, Oct. 30–Nov. 3, 2017, Dallas, TX, USA. ACM. DOI: http://dx.doi.org/10.1145/3133956.3133964 URL: http://www.winlab.rutgers.edu/~yychen/papers/vibwrite.pdf (дата обращения: 27.03.2021)
14. «Новый стандарт позволит использовать биометрию для авторизации на сайтах» [Электронный ресурс]. URL: https://www.securitylab.ru/news/492552.php (дата обращения: 27.03.2021)

Использование DoH в корпоративных сетях

Муслим Меджлумов, BI.ZONE

DNS является базовым инфраструктурным сервисом, без которого невозможно себе представить работу любой корпоративной сети. Широкая распространенность DNS и необходимость выпускать трафик данного протокола за пределы корпоративного периметра привели к тому, что он активно используется злоумышленниками в своих целях. Поэтому для специалистов по информационной безопасности важно обеспечить контроль коммуникаций по протоколу DNS, чтобы иметь возможность выявлять:

- резолвинг известных доменов, используемых для Command and Control (C2) серверов злоумышленников;
- резолвинг фишинговых доменов или доменов, используемых для распространения вредоносного программного обеспечения (ВПО);
- работу DGA (Domain Generation Algorithm);
- эксфильтрацию данных (DNS-туннели, DNS-FTP);
- аномалии в DNS (новые домены, нетипичный всплеск обращений к домену с одного или множества хостов внутри сети и т.д.).

Введение

В случае работы DNS поверх UDP или TCP для анализа трафика возможно использование следующих методов.

Пассивные:

- сбор логов с корпоративного рекурсивного DNS-резолвера и последующий анализ в одном из инструментов LM (Log Management) или SIEM (Security Information and Event Management);
- передача копии (SPAN/PortMirroring) трафика в систему обнаружения вторжений IPS/IDS.

Активные:

- Next-Generation Firewall[1];
- рекурсивный DNS-сервер с функциональностью безопасности (далее Secure DNS).

В 2018 году был принят новый стандарт DNS Queries over HTTPS (DoH, https://datatracker.ietf.org/doc/rfc8484/), который определяет возможность передачи DNS-запросов поверх HTTPS, тем самым обеспечивая их конфиденциальность. С тех пор поддержка DoH появилась:

- у облачных DNS-провайдеров (например, CloudFlare, Google Public DNS, BlahDNS и др.);
- в DNS-серверах BIND, Unbound, PowerDNS;
- в браузерах (Firefox, Chrome, Microsoft Edge на основе Chromium, Opera);
- в ОС (Windows 10, MacOS 11 Big Sur);
- в мобильных ОС (Apple iOS 14).

Изначально в основе идеи DoH стоит возможность анонимизации пользовательской активности, чтобы операторы связи, правоохранительные органы или иные государственные службы не могли анализировать DNS-трафик граждан, при этом сотрудники организаций также могут настроить свои браузеры для работы с DoH-серверами и оставаться неподконтрольными для служб информационной безопасности. Злоумышленники также понимают, что DoH позволяет им обходить пассивные инструменты мониторинга DNS и часть активных, поэтому начали использовать его в качестве канала коммуникации для ВПО (например, https://blog.netlab.360.com/ an-analysis-of-godlua-backdoor-en/). В итоге, из перечисленных выше методов анализа DNS-трафика в случае с DoH работать в полной мере будет только в Secure DNS, который поддерживает DoH и соответственно терминирует сессию и самостоятельно обрабатывает DNS-запросы.

Далее будет представлен подход, который мы реализовали в ООО «БИЗон» и который позволяет обеспечить работоспособность и безопасность DoH в корпоративной среде.

Ввиду того, что внутри предприятия, как и за его пределами, использовались решения, не предоставляющие функционал DoH, было принято решение в качестве отправной точки взять кеширующий/рекурсивный DNS-резолвер с открытым кодом Unbound https://nlnetlabs.nl/projects/unbound/about/ и реализовать недостающий нам функционал, тем самым получить свою реализацию Secure DNS. Старт реализации необходимого нам функционала был в начале 2020 года; на тот момент DoH в основной ветке еще не был реализован. По результатам проекта был реализован протокол DoH, защита от несанкционированного использования рекурсивного DoH-резолвера в публичных сетях. Помимо функционала, реализующего DoH, были добавлены функции фильтрации доменов на основе известных вредоносных доменов, категорий ограниченного контента, информации о репутации, защиты от эксфильтрации трафика.

Предварительные мероприятия

При внедрении DoH на предприятии необходимо произвести ряд мероприятий, связанных с исключением использования DoH-резолверов, неподконтрольных службе информационной безопасности предприятия, а именно:

1. Ограничить доступ из внутреннего периметра сети предприятия к внешним DoH-резолверам. Для этого на периметровых устройствах сетевой безопасности необходимо создать правила, блокирующие доступ к публичным DoH-резолверам на L4-устройствах, список которых можно почерпнуть по следующей ссылке (https://raw. githubusercontent.com/oneoffdallas/dohservers/master/list.txt).

[1] Класс решений, который, в отличие от классического L3/L4 пакетного фильтра, умеет за счет встроенного DPI детектировать и фильтровать по приложениям, осуществлять сигнатурный поиск по известным сетевым угрозам (IDS/IPS), имеет функционал URL-прокси, потоковый антивирус и т.п.

На UTM/NGFW- устройствах необходимо включить блокировку DoH-приложений.

2. В случае предоставления сотрудникам предприятия доступа к веб-ресурсам, расположенным в сети Интернет, обеспечить его через HTTP-proxy-серверы. На последних необходимо создать правила фильтрации на основе URI и/или HTTP-заголовка Content-Type.

Давайте рассмотрим вариант фильтрации на примере ACL популярного HTTP-proxy с открытым кодом squid.

```
acl dns-query-url urlpath_regex ^/dns-query\??
acl dns-req-message req_header Content-Type
    ^application/dns-(?:message|json)}$
acl doh_request any-of dns-query-url dns-req-message
acl doh_reply rep_header Content-Type ^application/
    dns-(?:message|json)$
```

Вышеописанные действия позволят предотвратить скрытые действия злоумышленников через публичные DoH-резолверы.

Для получения доступа к легитимным внешним сервисам Secure DNS, предоставляющий функционал DoH-резолвера, необходимо добавить в исключающие правила на устройствах фильтрации.

Использование нескольких рекурсивных резолверов для внутренних и внешних преобразований

Для использования DoH на предприятии в разных сегментах сети (внутренний и внешний) развернут сервис Secure DNS, который будет обслуживать мобильных и удаленных пользователей предприятия. Secure DNS будет предоставлять функции DoH-резолвера, а также фильтрацию на основе категорий ограниченного контента, защиту от эксфильтрации трафика, фильтрацию на основе регулярных выражений доменов, фильтрацию доменов и IP-адресов на основе известных вредоносных доменов, информации о репутации, проверки расширений безопасности DNS (Aggressive Use of DNSSEC-Validated Cache[2], Query Name Minimisation[3] и т.д.).

На DNS-серверах предприятия, обслуживающих зону example.com (здесь и далее этот домен используется лишь в качестве примера), как внутренних, так и внешних, регистрируется домен doh.example.com. Для зарегистрированного доменного имени doh.example.com создается пара ключей для взаимодействия через TLS, сертификат подписывается общеизвестными удостоверяющими центрами (список УЦ можно получить из хранилище SSL-сертификатов операционной системы либо из настроек веб-браузеров). Выпущенные сертификаты размещаются на экземплярах Secure DNS. После этого Secure DNS может принимать запросы на резволвинг от клиентов через протокол DoH.

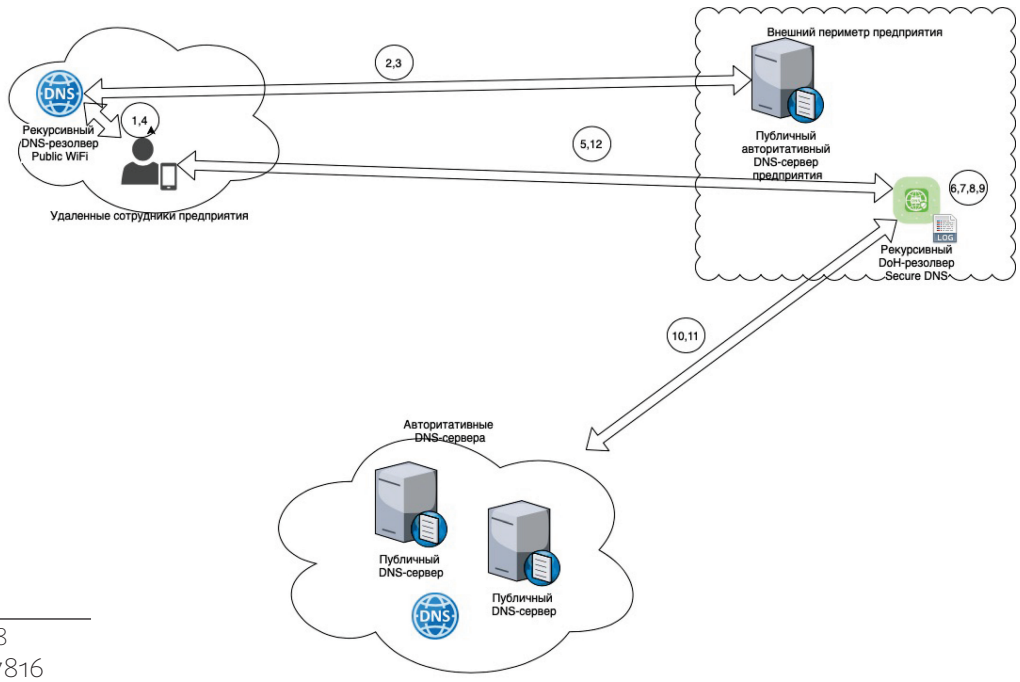
Через корпоративные политики производится конфигурирование устройств с использованием доменного имени Secure DNS с указанием уникального идентификатора организации - токена безопасности (например, https://doh.example.com/7300211b-aaoc-457f-9ce7-1ffa2a1dc956). Использование токена позволяет прикрыть Secure DNS от несанкционированного использования кем-либо из сети Интернет.

После проведенных мероприятий пользователи, находясь в локальной сети предприятия, могут использовать внутренний Secure DNS для получения как локальных имен, так и глобальных имен, полученных от авторитативных DNS-серверов, расположенных за пределами сети предприятия.

Мобильные или удаленные сотрудники, находясь за пределами сети предприятия, используя небезопасные подключения к сети (открытые точки доступа Wi-Fi, сети операторов мобильной связи, домашний Интернет), будут использовать корпоративный DoH-резолвер (Secure DNS), расположенный в DMZ предприятия, а не назначенные через DHCP DNS-резолверы, предоставленные к использованию небезопасной сетью. Это позволить уменьшить вероятность утечек приватных доменных имен предприятия.

В дополнение ко всему вышеописанному сервис Secure DNS предоставляет возможность мониторинга и регистрации всего проходящего через него DNS-трафика. Токен, передаваемый через URI и сопоставляемый с таким же значением в настройках Secure DNS, позволяет корректно идентифицировать запросы пользователей и корректно журналировать все запросы к DoH-резолверу.

Рис. 1. Вариант использования Secure DNS пользователями (мобильными и удаленными сотрудниками), использующими небезопасные подключения к сети.



[2] https://tools.ietf.org/html/rfc8198
[3] https://tools.ietf.org/html/rfc7816

Рассмотрим вариант использования Secure DNS пользователями (мобильными и удаленными сотрудниками), использующими небезопасные подключения к сети (рис 1.)

Удаленный сотрудник пользуется публичным Wi-Fi в кафе без подключения к VPN предприятия и начинает использовать ресурсы, расположенные в Интернете. При подключении к публичной Wi-Fi-сети устройство сотрудника через протокол DHCP получает настройки DNS-резолверов, работающих через традиционный транспорт 53 UDP/TCP. На устройстве пользователя в настройках DoH указан Secure DNS с корректными токеном организации.

Пользователь открывает веб-браузер и подключается к веб-ресурсу. Веб-браузер, имея настройки DoH и не имея в своем кэше информации о домене doh.example.com, пытается с помощью системного DNS-резолвера получить информацию об IP-адресе домена doh.example.com, отправляя запрос к DNS-серверу публичной Wi-Fi-сети (1). DNS-сервер публичной Wi-Fi-сети, не имея в своем кэше информации о домене doh.example.com, отправляет запрос к авторитативному DNS-серверу, отвечающему за DNS-зону example.com (2). В описании данного процесса пропущены шаги, связанные с поиском авторитативного DNS-сервера (example.com). На шаге (3, 4) авторитативный DNS возвращает информацию о публичных IP-адресах Secure DNS. Только описанные шаги 1-4 используют традиционный транспорт UDP/TCP по 53 порту, весь остальной поиск и резолвинг имен будет производиться по защищённому протоколу.

DoH-резолвер веб-браузера, имея информацию об IP-адресах, начинает взаимодействовать с рекурсивным DoH-резолвером предприятия (5).

В процессе взаимодействия веб-браузера и рекурсивного Secure DNS (рассмотрим только такой запрос, который удовлетворяет всем политикам, принятым на предприятии, и информации о домене нет в кэше):

- проверяется корректность токена безопасности в запросе (6);
- проверяются политики предприятия на резолвинг домена (фильтрации доменов на основе известных вредоносных доменов, категорий ограниченного контента, информации о репутации, детектирование от эксфильтрации трафика, DGA и т.п.) (7);
- проверяется наличие информации о домене в кэше экземпляра рекурсивного резолвера (8).
- В процессе обработки запроса происходит обогащение событий и журналирование таких событий (9).

После произведенных проверок, связанных с политиками, принятыми на предприятии, Secure DNS производит рекурсивный поиск информации о домене (9), отправляя запросы к авторитативным DNS-серверам, расположенным в сети Интернет (10). Secure DNS, получив ответы (11), прогоняет тесты с применением функционала Aggressive Use of DNSSEC-Validated Cache[4], Query Name Minimisation[5] и т.п., отправляет информацию о запрошенном доменном имени веб-браузеру удаленного сотрудника (12).

Мы рассмотрели положительный сценарий, когда запрос доменного имени удовлетворяет всем политикам, принятым на предприятии. В случае нарушения политик, принятых на предприятии, Secure DNS может прекратить процесс резолвинга, вернуть ошибку или вернуть IP-адрес страницы заглушки с пояснением причины блокировки инициатору запроса (веб-браузеру).

Далее рассмотрим варианты использования Secure DNS мобильными и стационарными пользователями, использующими подключения к локальной сети предприятия (рис. 2)

Мобильный сотрудник, вернувшись на площадку предприятия, подключается в локальную проводную или беспроводную сеть предприятия и начинает использовать ресурсы предприятия, расположенные как в локальной сети, так в сети Интернет. При подключении Wi-Fi-сети предприятия устройство сотрудника через протокол DHCP получает настройки DNS-резолверов, работающих через традиционный транспорт 53 UDP/TCP, также расположенный на кэширующем рекурсивном резолвере Secure DNS.

Совмещение DoH и традиционного рекурсивного резолвера позволяет кэшировть информацию как о приватных, так и о глобальных доменных именах.

Пользователь открывает веб-браузер и подключается к веб-ресурсу. Веб-браузер, имея настройки DoH и не имея в своем кэше информации о домене doh.example.com, пытается с помощью системного DNS-резолвера получить информацию об IP-адресе домена doh.example.com, отправляя запрос через традиционный транспорт (DNS over UDP) к Secure DNS (1). Secure DNS локальной сети, не имея в своем кэше информации о домене doh.example.com, отправляет запрос к приватному авторитативному DNS-серверу (размещенному внутри периметра сети предприятия), отвечающему за DNS-зону example.com. Так как Secure DNS сконфигурирован на пересылку всех запросов к зоне example.com на конкретные приватные IP-адреса внутри локальной сети, политики безопасности к таким запросам применяться не будут. Запросы будут перенаправлены на приватные авторитативные DNS-серверы корпоративного домена example.com (2). Запросы также будут зафиксированы в журнале (9). На шаге (3) авторитативный DNS возвращает информацию о приватных IP-адресах DoH-резолверов на кеширующий DNS-сервер (Secure DNS). Secure DNS возвращает инициатору запроса информацию о приватных IP-адресах в домене doh.example.com.

DoH-резолвер веб-браузера, имея информацию об IP-адресах, начинает взаимодействовать с локальным Secure DNS (5).

Далее процесс (6-12) идентичен описанному ранее.

Мы рассмотрели процессы, которые происходят во время работы протокола DNS, но не затронули процесс конфигурирования DoH-клиентов.

Опишем процесс настройки корпоративной политики Chrome Enterprise.

[4] https://tools.ietf.org/html/rfc8198
[5] https://tools.ietf.org/html/rfc7816

Настройки политик использования DNS-over-HTTPS в Chrome Enterprise

Опишем имеющиеся параметры конфигурации политики.

При настройке политики будет необходимо сконфигурировать пару параметров, такие как DnsOverHttpsMode и DnsOverHttpsTemplates.

Для управления политиками необходимо выбрать один из предложенных вариантов для параметра DnsOverHttpsMode:

off: отключите DNS-over-HTTPS (Disable DNS-over-HTTPS) - Chrome никогда не отправляет DoH-запросы на DNS-серверы.

automatic: включен DNS-over-HTTPS с небезопасным откатом. Если доступен DNS-сервер, поддерживающий DoH, Chrome сначала отправляет запрос DNS-over-HTTPS. Если получена ошибка или сервер, поддерживающий DoH, недоступен, Chrome вместо этого просто отправляет DNS-запрос на сервер, используя системный резолвер. Данная опция может быть полезна при использовании мобильных устройств в сетях с применением Captive Portal (публичные Wi-Fi-сети).

secure: включен DNS-over-HTTPS без небезопасного отката - Chrome отправляет запросы DoH только на DNS-серверы.

значение по умолчанию – включен DNS-over-HTTPS с небезопасным откатом.

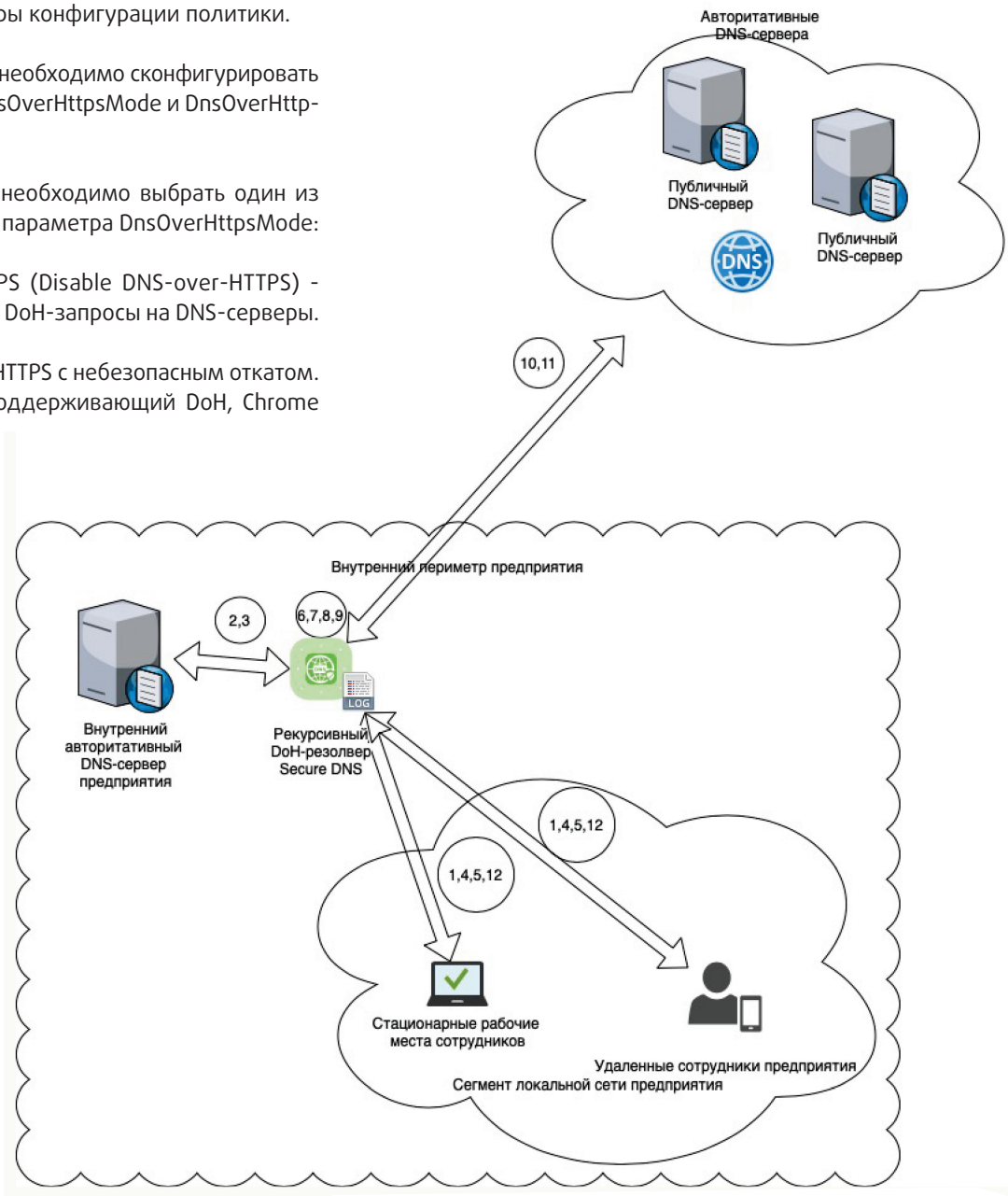
Включая DoH на предприятии, необходимо добавить в список шаблонов URI резолверов DoH (Secure DNS). Иначе будут использоваться публичные рекурсивные DNS-резолверы Google.

Например, при использовании Secure DNS в параметре DnsOverHttpsTemplates указать URI https://doh.example.com/7300211b-aa0c-457f-9ce7-1ffa2a1dc956.

Данные параметры можно поменять через групповые политики MS AD или через скрипт, вносящий изменения в ветки реестра:

- Software\Policies\Google\Chrome\DnsOverHttpsMode тип данных: строка
- Software\Policies\Google\Chrome\DnsOverHttpsTemplates тип данных: строка

Рис. 2. Варианты использования Secure DNS мобильными и стационарными пользователями, использующими подключения к локальной сети предприятия.



В итоге

DNS over HTTPS обеспечивает преимущества конфиденциальности для конечных пользователей, но может создавать проблемы для предприятий, желающих добиться защиты и видимости при работе DNS. Предприятия могут внедрить DoH в свои службы DNS для получения как преимуществ DoH, так и передовых методов защиты DNS. Однако предприятия, которые разрешают использование DoH без стратегического и тщательного подхода, в конечном итоге могут лишиться видимости DNS-трафика на средствах сетевого мониторинга, не дав им возможности обнаруживать вредоносную активность внутри сети и позволяя злоумышленникам и вредоносным программам обходить назначенные корпоративные DNS-резолверы. Часть разработок, которые были нами реализованы в собственных целях и описаны в статье, мы планируем опубликовать в корпоративном аккаунте на github.

IPv4-адресок продать не желаете?

Дэвид Стром (David Strom)

Если ваша компания хочет продать принадлежащий ей блок адресов IPv4 – или, наоборот, купить дополнительные адреса, – возможно, сейчас самое время для этого. Как хорошо известно читателям, количество доступных адресов IPv4 неуклонно сокращается: дошло до того, что многие региональные интернет-регистраторы (RIR) больше их не выдают. Быть может, имеет смысл обратить свой взгляд на вторичный рынок. Для тех, кто впервые слышит о таком, в этой статье я постараюсь помочь вам понять, что это вообще такое и как вести на нем бизнес.

Для продавцов адресные блоки – это и потенциальный источник дохода, и способ найти старому активу какое-то применение. Если вы когда-то поглощали другие компании, особенно те, у которых остались активы еще со времен зарождения Интернета, то, возможно, у вас уже есть блок-другой, который пылится без дела или используется не на полную мощность. Почему бы и не продать ненужный блок, точно так же, как компании продают или сдают в аренду ненужную им самим недвижимость? «У многих компаний имеются в собственности миллионы неиспользуемых IP-адресов, – говорит Винсентас Гриниус (Vincentas Grinius) из компании Heficed, занимающейся лизингом адресного пространства. – За них держатся, видя в них резерв для будущего развития или стратегический актив». Возможно, сейчас как раз пришла пора продавать, потому что цены вышли на плато, как сказали мне уже несколько брокеров (само собой, у них тут прямой интерес), да и сама практика становится более общепринятой.

А если вы покупаете, тоже хорошо – сейчас удачный момент, чтобы продлить жизнь вашему корпоративному IPv4-оборудованию еще на несколько лет. Особенно если вы не торопились переходить на IPv6 или вам это трудно.

До недавних времен репутация у вторичного рынка адресов была, скажем так, не лучшей. Для многих из нас купить б/у адресный блок – все равно что по дешевке купить старую машину. Как сказал мне Гриниус, в прошлом к б/у адресам относились «примерно так же, как к журналу «Хастлер»: что-то такое, чем стыдно владеть». Но с тех пор ситуация немного легализовалась: если продолжить аналогию с авторынком, появились аналоги «Автотеки» или «пробива» машины по базам ГИБДД на предмет ДТП, расчета ремонтов в страховых и так далее, в результате чего доверия между покупателем, брокером и продавцом стало больше.

Вторичный рынок адресов сейчас процветает, как и конкуренция на нем: число брокеров идет на десятки, и есть как минимум три лизинговых фирмы (IPv4 Market Group, Prefix Broker и Heficed), активно занимающихся помощью в подборе покупателей и продавцов.

У меня самого еще с 1993 года был блок адресов класса C, поэтому, когда редактор IPJ попросил меня написать статью о вторичном рынке IPv4, я решил заодно этот блок и продать.

Но, перед тем как погрузиться в специфику работы брокеров и вторичного рынка, сначала предпримем небольшой экскурс в историю и вспомним, как исчерпывалось адресное пространство IPv4 и как RIR распределяют адреса. Параллельно я буду рассказывать, как продавал свои адреса и что узнал в процессе – надеюсь, это поможет вам определиться с тем, стоит ли покупать адреса на «вторичке», продавать их или сдавать в аренду.

Справочная литература по смене владельцев адресов

Возможно, наилучшим источником информации об исчерпании адресов IPv4, связанных с ним мифах (таких, как «поменять роутеры у заказчиков просто» или «у провайдеров еще целая гора IPv4-адресов») и инструментах перехода на IPv6 являются старые номера самого IPJ, включая статьи Джеффа Хьюстона (Geoff Huston) из APNIC (Asia Pacific Network Information Centre). Приведу небольшой список самых полезных материалов – как из IPJ, так и из других источников. Сразу скажу, что во время подготовки материала я общался с Хьюстоном и использовал некоторые из его замечаний в этом обзоре.

- Статья в июньском номере IPJ за 2003 г.[1] содержит обзор раннего этапа развития IPv6. Здесь же Хьюстон развенчивает некоторые ранние мифы, например то, что IPv6 якобы от природы отличается лучшим уровнем безопасности, качества обслуживания (QoS) и поддержки мобильности. В одном месте Хьюстон заметил: «Если текущие политики будут применяться и дальше, то адресное пространство IPv4 будет доступно еще на протяжении многих лет». И оказался прав – хотя, возможно, не в том смысле, который первоначально вкладывал в свои слова. Недавно он написал мне по электронной почте: «В те времена все ожидали, что переход на IPv6 завершится еще до того, как закончатся адреса IPv4».
- Четыре года спустя, в сентябрьском номере IPJ за 2007 год[2], Хьюстон напрямую говорит о ситуации с исчерпанием адресного пространства IPv4 и демонстрирует модели, согласно которым пул адресов должен был полностью израсходоваться к 2011 году (что и произошло). На тот момент исчерпание адресного пространства было практически неизбежно. В этой статье Хьюстон пишет, что у IPv6 не самые оптимистичные бизнес-перспективы и что работать с NAT (Network Address

Translation) под IPv4 гораздо легче – то же самое верно и сегодня.

- Спецвыпуск IPJ за март 2011 г., посвященный переходу на IPv6[3], содержит комментарий о т.н. Всемирном дне IPv6, состоявшемся в 2011 году, и историю исчерпания адресов IPv4. В этом номере Хьюстон пишет, что «Запас адресов [IPv4] неизбежно будет исчерпан». К тому времени APNIC исчерпал свой пул адресов IPv4. «Большинство игроков в Интернете не уверены в том, что им делать дальше [касательно перехода на v6]: от крупнейших провайдеров до конечных пользователей», – продолжает он. Рекомендую весь этот номер к ознакомлению, так как он содержит массу полезной информации о переходе на IPv6.
- Декабрьская (2019 г.) презентация Хьюстона об IPv6 также достойна прочтения[4]. В ней он обсуждает тогдашние ценовые тренды при продаже блоков и предсказывает, что к тому времени, когда адреса IPv4 совсем закончатся, мы перерастем IPv6: «Он не был нужен нам тогда, когда впервые появился, не нужен и сейчас». Недавно Хьюстон писал мне в электронном письме, что «с момента первоначального исчерпания адресов прошло девять лет, и что мы видим? На IPv6 до сих пор приходится меньше четверти Интернета, а IPv4 так и остался основным. Изменить всю архитектуру Интернета оказалось легче, чем полностью перейти на новый протокол IP».
- В декабрьском номере IPJ за 2001 год приведен неплохой исторический обзор развития RIR.[5] Здесь освещены бесклассовая междоменная маршрутизация (CIDR), подсети и суперсети.
- Документ White Paper за авторством Eric Bais[6] содержит массу практических рекомендаций о передаче адресов с точки зрения брокера в регионе Réseaux IP Européens (RIPE), занимающегося и продажей блоков, и сдачей их в аренду.

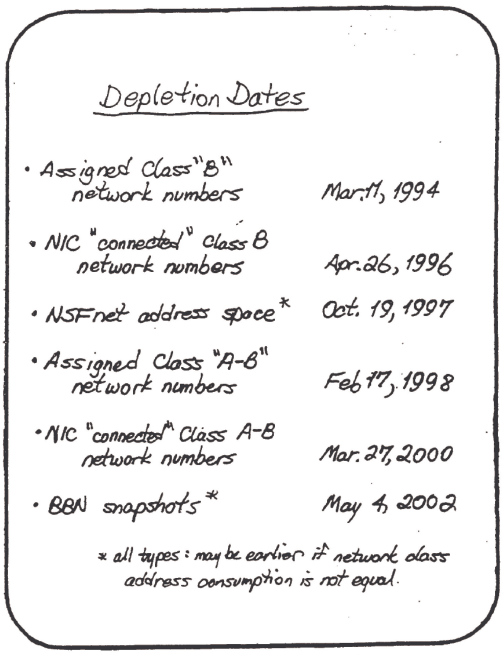
Исторический обзор

Впервые я писал об исчерпании адресного пространства IPv4 еще в начале девяностых, когда я был главным редактором журнала Network Computing. К сожалению, та статья более не доступна в Интернете. Я помню ее очень хорошо, потому что мой отец, который в технологиях не слишком разбирался, в шутку предложил мне тогда бросить работу и пойти торговать адресами. Шутка оказалась в каком-то смысле пророческой...

Тогда, на заре коммерческого Интернета, диапазоны IP-адресов выдавал Джон Постел (Jon Postel). Делал он это сам, вручную и, как правило, сразу же, как получал запрос по электронной почте: так я и стал обладателем своего блока /24. Понятное дело, что этот «метод» вышел из употребления, когда Интернет стал бурно развиваться. Одним из первых, кто забил тревогу, был Фрэнк Соленски (Frank Solensky), который еще в 1990 году опубликовал свои предсказания о том, когда что закончится, на 18-м совещании Internet Engineering Task Force (IETF).[7] Ксерокопию рукописной заметки Соленски я привел на рис. 1.

Основная проблема «золотой середины» в том, что для среднестатистической компании, которая хочет выйти в Интернет, 250 адресов в блоке класса C мало, а 65 тысяч адресов в блоке класса B слишком много. Для решения этой проблемы предлагалась масса технических подходов, включая бесклассовую адресацию (RFC 1918[8]), NAT, прекращение выдачи статических IP-адресов пользователям на диалапе и доработку протоколов маршрутизации. Но настоящим решением стала разработка IPv6, с тем чтобы увеличить общий объем адресного пространства. В начале 1990-х годов крупные блоки диапазонов A и B уже выдавались с большой оглядкой, особенно с учетом того, что Постел к тому моменту и там успел много чего раздать.

Рис. 1. Рукописная заметка Соленски с прогнозами дат исчерпания адресов.



Даты исчерпания	
Назначенные сетевые номера класса B	11 марта 1994 г.
«Подключенные» к NIC сетевые номера класса B	26 апреля 1996 г.
Адресное пространство NSFnet*	19 октября 1997 г.
Назначенные сетевые номера класса A-B	17 февраля 1998 г.
«Подключенные» к NIC сетевые номера класса A-B	27 марта 2000 г.
Снапшоты BBN*	4 мая 2002 г.

* для всех типов: возможно и раньше, если расход адресов неравномерен по сетевым классам

Пока адреса IPv4 постепенно заканчивались, были созданы три RIR согласно RFC 1366[9]. Потом эта система была модифицирована в 1993 году согласно RFC 1466[10], а еще через несколько лет окончательно оформилась в RFC 2050[11]. Теперь их пять:

- African Network Information Centre (AFRINIC) обслуживает Африку.
- Asia Pacific Network Information Centre (APNIC) обслуживает часть Азиатско-Тихоокеанского региона.
- American Registry for Internet Numbers (ARIN) обслуживает Северную Америку и часть Карибского бассейна.
- Latin America and Caribbean Network Information Centre (LACNIC) обслуживает Латинскую Америку и еще одну часть Карибского бассейна.
- Réseaux IP Européens Network Coordination Centre (RIPE NCC) обслуживает Европу, Ближний Восток и часть Центральной Азии.

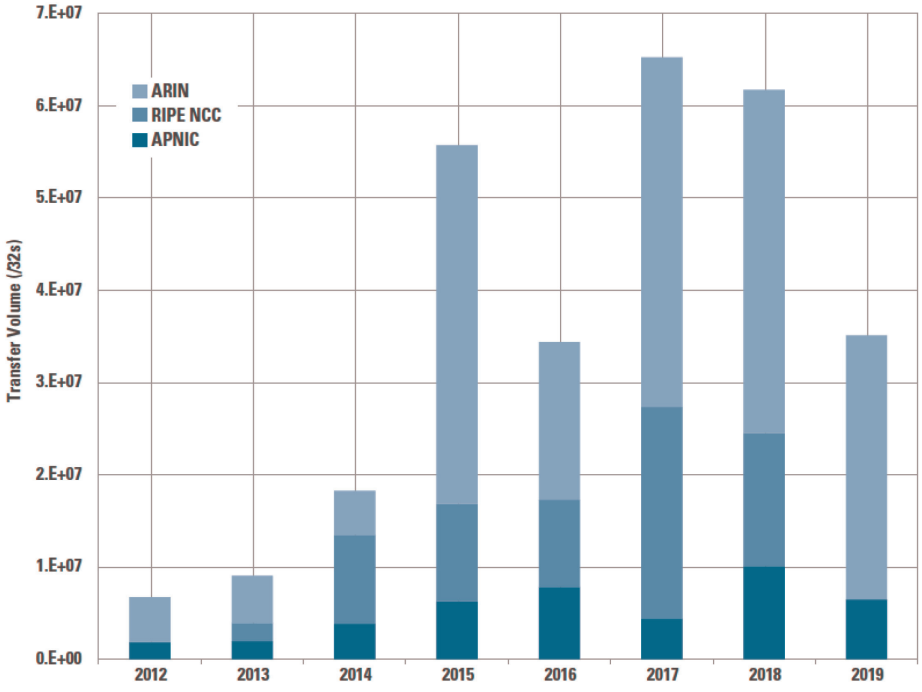
К февралю 2011 года оставшиеся общие блоки адресов IPv4 полностью распределили по RIR. В опубликованной в IPJ статье цитировались слова Рауля Эчеберриа (Raúl Echeberría), президента Number Resource Organization (NRO), головной над пятью RIR: «Это лишь вопрос времени, когда RIR и ISP придется начать отказывать в запросах на адресное пространство IPv4»[3]. Сегодня практически каждый блок адресов уже кем-то занят. Больше всего свободных блоков осталось в AFRINIC, несколько мелких блоков еще есть в APNIC. RIPE выдала последний блок адресов /22 в ноябре 2019 года[12].

Появление вторичного рынка адресов и надзор со стороны RIR

Возможно, вторичный рынок адресов родился в 2011 году, когда Microsoft купила адресное пространство Nortel – более 600 тысяч отдельных IPv4-адресов – за 7,5 миллиона долларов. (Строго говоря, это заявление не совсем верно, но, судя по всему, главным активом Nortel был именно адресный пул.) С тех пор миллионы адресов меняли владельцев[13] каждый год, как видно на рис. 2.

В течение последнего десятилетия RIR играли все большую роль в таких переходах. В списке дополнительной литературы я привожу прямые ссылки на актуальные политики передачи адресов для каждого регистратора[14]. Имейте в виду, что у некоторых RIR уровень точности и прозрачности этого процесса выше, чем у других, а также более высоки требования к доказательству владения адресным блоком.

Рис. 2. Статистика смены владельцев адресов на 2020 год, собранная Джеффом Хьюстоном. Количество передаваемых блоков /32.



Но эта система была далека от совершенства: вопросы о том, кто является владельцем блока, не всегда удавалось разрешить в рамках одного регистратора, записи об организациях безнадежно устаревали, иногда указывая на компании, давно прекратившие работу, а спамеры могли загадить блок адресов так, что его продажа становилась проблематичной. Не говоря уже о том, что многие блоки адресов (как, например, мой) были старше RIR и относились к т.н. legacy-ресурсам. Для RIR разобраться со всем этим – та еще задача, особенно в случае, когда компания-владелец адреса давно прекратила существование, и чтобы проследить судьбу блока от Постела до текущего владельца, может потребоваться прямо-таки следствие. И кто же будет следователем? Не самый простой вопрос, как мы увидим.

Частью проблемы является сама служба WHOIS, которая является главным инструментом выяснения вопросов о владельцах доменов и блоков. WHOIS далека от совершенства. Начнем с того, что она дает разные ответы в зависимости от того, какие данные опрашиваются, какой RIR отвечает за блок, предоставил ли владелец блока точную и актуальную информацию или, наоборот, намеренно скрыл эти детали.

Мало того, есть еще один аспект: интернет-сообщество внесло изменения в отображение информации из запросов WHOIS. Такие изменения были необходимы и по соображениям конфиденциальности (вследствие изменений законодательства в разных странах), и для защиты от спамеров, злоупотребление WHOIS с чьей стороны заставило законных предпринимателей скрывать свои данные. Если хотите сравнить страницы WHOIS у разных RIR, я включил их в раздел ссылок[15].

Если бы вы захотели получить информацию о моем собственном блоке /24 до того, как я начал писать эту статью, вы бы увидели следующее:

```
Organization: David Strom, Inc (DAVIDS-3)
RegDate: 1993-05-21
Updated: 1996-04-18
```

Адрес моей организации DAVIDS-3 – это адрес корпорации, зарегистрированной в штате Нью-Йорк и более не существующей. Указанное контактное лицо – инженер провайдера, у которого я регистрировал блок. Провайдер тоже давно закрылся. Так что передо мной встает нетривиальная задача: доказать, что нью-йоркская корпорация David Strom Inc. – это та же самая David Strom Inc., которая сейчас работает в штате Миссури. Я не был уверен, чем могу подтвердить «передачу активов», о которой ARIN рано или поздно спросила бы, – разве что найти авиабилет времен моего переезда.

Так и началось мое путешествие к продаже блока: нужно было внести в мою информацию исправления и подготовить актив к перепродаже. Я потратил массу времени на изучение материалов с сайта ARIN, несколько раз звонил к ним на горячую линию за разъяснениями и заплатил 300 долларов сбора, чтобы начать процедуру. Персонал ARIN отвечает на электронную почту в течение 48 часов, а если переписка затягивается, как у меня, это существенно удлиняет весь процесс.

На сцене появляется брокер

Так мы и подошли в нашем историческом обзоре к современности (скажем, после 2012 года) и появлению рынка брокеров блоков IP. Их задачей было облегчение процедуры передачи адресов и повышение уровня доверия между всеми сторонами. Как я уже говорил, сейчас на рынке работает немало брокеров. Работают все они (для продавца или арендодателя) примерно одинаково, включая следующие основные этапы:

1. Вам нужно зарегистрировать свою компанию у брокера – для этого требуется всего лишь ответить на несколько простых вопросов и создать логин для дальнейшего взаимодействия посредством веб-форм, форумов и электронной почты.
2. Теперь, если вы продавец, вы и брокер подписываете взаимное соглашение о неразглашении и затем выставляете блок на торги. У некоторых брокеров имеется целый ряд методов продажи, включая открытые и закрытые аукционы, а также возможность «купить сейчас». Если вы покупаете, вы теперь можете просматривать блоки, доступные на открытых аукционах, и делать ставки. Тем, кто хоть раз что-то продавал или покупал на интернет-аукционе, эта процедура хорошо знакома.
3. Выбрав покупателя для конкретного блока, вы требуете у него оплату и помещаете ее на счет эскроу, а затем закрываете аукцион.
4. Поддержка брокера организует передачу адресов в соответствующем RIR (или нескольких). Если вы покупаете, вы теперь уплачиваете сбор за передачу непосредственно в RIR. У каждого RIR эти сборы рассчитываются по-разному: например, в RIPE это бесплатно, а в других RIR сумма за крупный блок может доходить до нескольких тысяч долларов. (См. рис. 3.)
5. Наконец сделка оформлена. Контроль над блоком переходит к новому владельцу, а деньги со счета эскроу (за вычетом комиссии брокера) перечисляются продавцу или арендодателю. И вот теперь начинается интересное. Комиссии брокеров непрозрачны: чтобы выяснить, сколько это стоит, требуется зайти достаточно далеко, и брокеры намеренно построили процесс таким образом, чтобы нельзя было заранее сравнить комиссии и выбрать, где подешевле. И даже несмотря на это, в услугах брокеров есть смысл, потому что, как пишет автор цитируемого документа Prefix Broker[6], «нет ничего неприятнее, чем пытаться получить деньги в стране, в которой у вас нет представителя и о чьей правовой системе вы ничего не знаете».

Еще одна важная деталь касается сдачи блоков в аренду: отношения между арендодателем и арендатором гораздо более продолжительные и тесные, чем между продавцом и покупателем, потому что в конечном счете за репутацию тех, кто пользуется вашим IP-адресом, все равно отвечаете вы. Иными словами, сдача адресного пространства внаем несет в себе определенный риск для владельца: как и при аренде квартир, за имущество отвечает владелец, он же арендодатель. Если жильцы устроят в квартире притон, пострадает ваша репутация. Поэтому при аренде необходим более высокий уровень доверия к брокеру.

У трех из пяти RIR на сайтах есть списки брокеров, причем каждый ведет их на свой манер, с указанием разной контактной информации и разным количеством брокеров:

- У APNIC в списке 22 брокера[16] с указанием контактных лиц, их телефонов и скайп-контактов.
- В списке RIPE уже 76 брокеров[17], а в качестве контактной информации приведены ссылки на их сайты.
- У ARIN в списке 29 брокеров[18] с указанием контактных лиц, их телефонов и даты регистрации брокера в ARIN.

Все три RIR всячески подчеркивают, что эти списки носят не рекомендательный, а чисто информационный характер. Например, RIPE заявляет, что включила в список тех брокеров, кто согласился вести свой бизнес честно, но после включения в список их никто не проверял. Так что этот факт стоит иметь в виду: как говорится, в Интернете никто не знает, что ты собака.

Рис. 3. Суммы сборов за передачу адресов в каждом из RIR.

RIR	Сумма сбора за передачу
RIR	Сумма сбора за передачу
ARIN	300 долл. США
RIPE	Бесплатно
APNIC	20% годовой платы за число передаваемых адресов IPv4
LACNIC	Первоначальный сбор 200 долл. США Менее /19 – 1000 долл. США /19 и более – 1500 долл. США
AFRINIC	Менее /22 – бесплатно От /22 до /20 и более – 1750 долл. США От /20 до /18 – 2000 долл. США

Тем, кто, как и я, лишь выходит на вторичный рынок адресов, я советую очень внимательно изучить эти материалы RIR. Список брокеров – это, конечно, хорошо, но если вам нужно продать или сдать в аренду блок адресов, поиск подходящего брокера может стать непростой задачей. Самая большая проблема в том, что четких правил покупки, продажи и аренды б/у адресов не существует. В отличие от вторичного авторынка, здесь нет ни надзорных органов, ни даже консенсуса о том, что значит качество продукта. Как видно из приведенного выше процесса, неопределенность и потенциальные проблемы могут возникнуть на каждом из пяти этапов.

Есть и еще один момент, который, казалось бы, должен быть очевидным, но неочевиден: этот рынок только для юрлиц. Если блок принадлежит вам лично, вам придется сначала передать его в собственность юридического лица. Обратите внимание, что мой блок был зарегистрирован на мою S-корпорацию (названную моим именем, что сильно облегчило процесс передачи активов от нью-йоркского юрлица миссурийскому). Если бы я изначально зарегистрировал свой блок на себя как на частное лицо, мне бы, возможно, пришлось попотеть, доказывая, что я – это я.

Подводные камни в процессе передачи адресов

В этом разделе мы поговорим о некоторых моментах, которые следует иметь в виду, выходя на рынок.

Во-первых, нужно сразу определиться: продажа или аренда? Этот вопрос не так прост, и ответ на него зависит от того, сколько адресов вам нужно и зачем. Ниже я поговорю об этом подробнее, но это самое первое решение, которое вам нужно будет принять, и данных для него часто оказывается недостаточно.

В отличие от авторынка, здесь нет ни установившейся практики, ни руководств по тому, как выбирать между продажей и арендой. Есть, разумеется, общая стоимость, и чтобы определить ее, вам нужно знать свой временной горизонт. Если вы покупатель, то нужны ли вам адреса на несколько лет или на несколько месяцев? Можете ли вы в конце концов перевести оконечные точки на IPv6, используя эти адреса?

Если же вы продавец, то что вам выгоднее: избавиться от актива и быстро получить деньги или же получать постоянный доход от аренды? Опять же, сдавая имущество, вы исходите из неких прогнозов о ценах на аренду, которые могут сбыться, а могут и нет. А теперь представьте себе, что вы обсуждаете этот вопрос со своим финдиректором, который не обязательно разбирается в тонкостях вторичного рынка адресов.

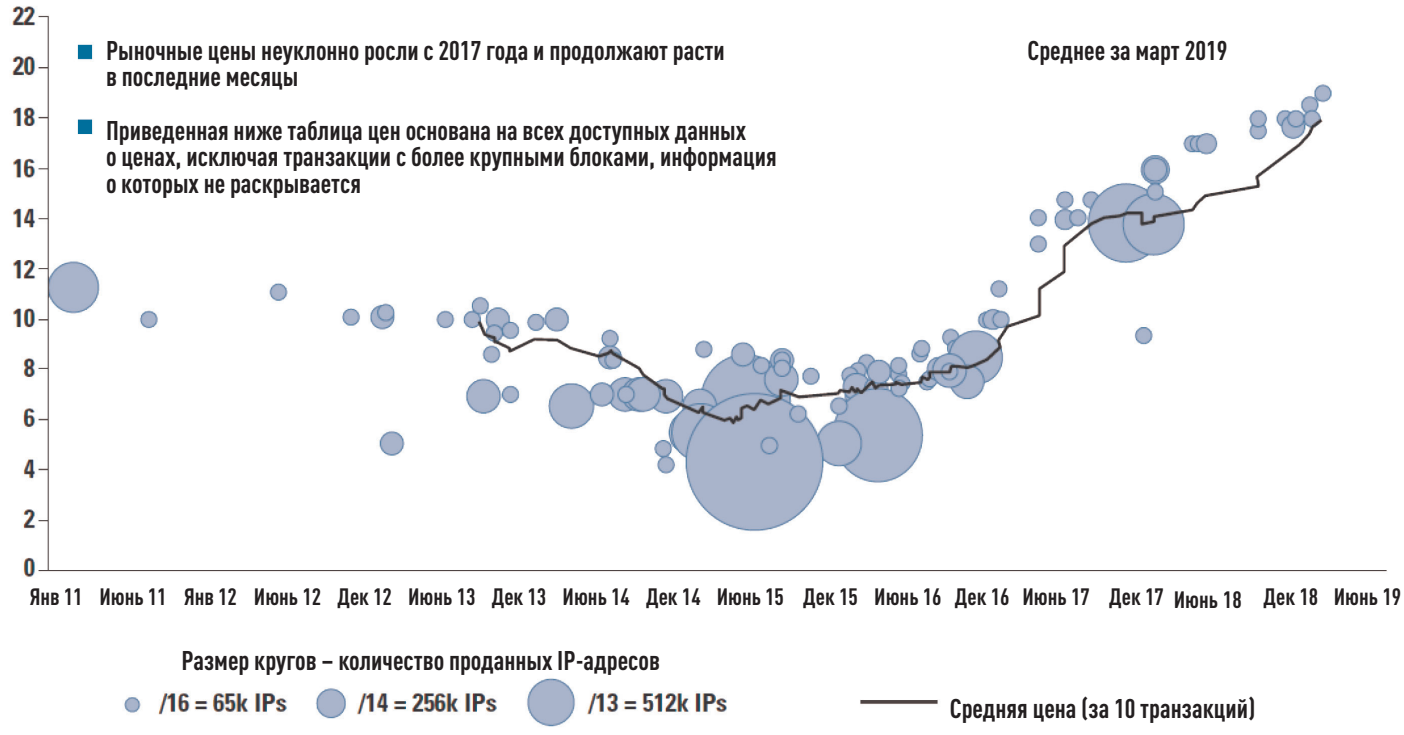
Определиться между покупкой или арендой может помочь размер нужного блока. Некоторые брокеры специализируются на крупных блоках – например, есть такие, кто отказывается иметь дело с чем-то меньше /24. «Если вы продаете большой блок (скажем, /16 или больше), вам нужен брокер, который способен быть эффективным посредником между вами и крупными покупателями», – написал мне Джефф Хьюстон в личном письме. Плюс к тому, если брокер перечисляет уже осуществленные сделки, это может помочь принять более информированное решение. Не все брокеры отличаются ценовой прозрачностью, а некоторые темнят больше, чем другие.

Например, один из брокеров, публикующих данные о собственных предыдущих продажах на аукционах, – это IPv4.Global[19]. Другой брокер, IPv4 Market Group, подготовил диаграмму изменения цен, которая приведена на рисунке 4 (сведения по состоянию на март 2019 г.)[23]. Независимо проверить эти данные никак нельзя, но, как минимум, видно, как менялся рынок за последнее десятилетие.

В начале января 2020 г. блоки /24 продавались по цене 20–24 долларов за IP-адрес, т.е. 5–6 тысяч долларов за весь блок. Стоимость аренды «гуляет» от 20 центов до 1,20 доллара за адрес в месяц, то есть по сравнению с продажами выйдет в ту же сумму в лучшем случае за два года, а в худшем – за все десять. Я решил продать свой блок: я хотел получить деньги, а сдавать адреса в аренду горел желанием не больше, чем физически сдавать свою бывшую квартиру. Кроме того, надо убедиться, что брокер, которого вы в конце концов выберете, признан тем RIR, к которому относится ваш блок.

Во-вторых, нет никакой гарантии, что любой из этих брокеров добросовестен и действительно выполнит свои обязательства – да что там, нет даже гарантии, что указанная на сайте RIR информация о нем и его контактных лицах

Рис. 4. Ценовые тренды на блоки IP-адресов с течением времени.



актуальна! Контролировать деятельность таких брокеров очень непросто, проблемой будет даже договориться о том, какие метрики использовать для такого контроля. Если только вы не знаете этих людей лично или через вторые руки, то, скорее всего, потребуется внимательно покопаться в данных брокеров на сайте RIR, чтобы определиться с тем, кому же доверить продажу вашего блока. Можно попробовать посмотреть их регистрационные данные в ARIN, если ваш блок относится к ARIN.

Одна из возможных стратегий выбора брокеров – посмотреть, насколько активно он участвует в различных комитетах по управлению Интернетом в вашем регионе (или как минимум посмотреть опубликованные списки участников). Здесь я исхожу из гипотезы, что брокер, чьи представители участвуют в мероприятиях IETF, RIR и сетевых операторов, таких как North American Network Operators' Group (NANOG)[20], надежнее тех, чьи люди на них не появляются. (PrefixBroker.com, например, на своем сайте утверждает, что участвовал в разработке правил передачи адресов для RIPE.)

На сайте IPv4 Market Group приведен список вопросов[21], которые следует задать потенциальному брокеру, в том числе, представляют ли они только одну сторону сделок (большинство работают и с покупателями, и с продавцами) и обеспечивают ли необходимую юридическую и страховую поддержку. Я решил, что это неплохая отправная точка.

Некоторые брокеры также занимаются другими видами деятельности (у одних есть профильные направления в составе той же компании, другие сами являются профильными подразделениями крупных корпораций). Кто-то работает в сетях и Интернете, например предоставляя услуги хостинга и облачных вычислений, другие занимаются защитой интеллектуальной собственности, третьи являются застройщиками. Эта информация может оказаться важной – или, напротив, исказить картину, если качество работы по другим направлениям окажется совершенно другим, чем в брокерской деятельности.

Одна из причин, по которым я выбрал IPv4.Global/Heficed – прозрачность работы: они показали мне активные аукционы и данные по прошлым продажам блоков прямо на своей домашней странице, а потом периодически рассылали мне уведомления об активных и закрытых аукционах.

Третий момент – проверка второй стороны сделки. Иными словами, если вы продаете, то как будете собирать и проверять информацию о своем покупателе, и наоборот?

Те, кто хочет сдать адреса в аренду, могут пожелать заключить долгосрочные контракты (например, на три года) для большей стабильности и для того, чтобы свести к минимуму смену арендаторов. «Я бы, пожалуй, встревожился, если бы брокер не принял тех или иных прямых действий для проверки данных продавца», – заметил Джефф Хьюстон в нашей переписке.

Последний момент в процедуре передачи адресов – понять, в каком состоянии находится сам блок. Нет никаких гарантий, что б/у блок не «загажен» спамерами или не использовался для других видов противоправной деятельности. «Общепринятых стандартов ведения бизнеса здесь нет, прозрачности почти нет, а ответственности еще меньше, – писал в 2018 году Марк Линдси в блоге в CircleID[13]. – Многие из участников рынка затрудняются сказать с юридической точки зрения, что же именно продается и покупается». У него тоже можно найти несколько советов о том, как проверить, можно ли иметь дело с другой стороной потенциальной сделки.

Большинство брокеров заверяют, что проводят проверку предыдущих владельцев блоков на предмет спама и другой противоправной деятельности. Но тут тоже вопрос: заверять они могут кого угодно в чем угодно, но с помощью каких средств они вас убеждают в своей правоте? Например, некоторые брокеры предлагают вам самому проверить черные списки (например списки Cisco Talos, Hetrixtools.com и IP-score.com), чтобы убедиться, что ваш блок там не значится. У IPv4 Market Group есть услуга вывода из черных списков[22], которая проверяет 90 таких списков. Цены на нее бывают разными, но, например, с меня они запросили 2000 долларов за эту услугу в рамках продажи моего блока /24. IPv4.Global проверяет 20 различных черных списков в рамках своих услуг.

Однако одно дело – выяснить, значится ли блок в черном списке, а совсем другое – убрать его оттуда. Если блок попал в черный список, его не удастся сдать в аренду, пока вы его оттуда не вытащите. А по словам Джеффа, «как только адрес попал в черный список, убрать его оттуда крайне трудно». Ни один из брокеров не назовет вам твердую сумму за очистку блока, потому что это зависит от того, в каком количестве черных списков он «засветился».

Так чем же кончилась история с моим блоком? Он ушел с аукциона за 10 дней. ARIN помогла мне переписать его на мое нынешнее юрлицо, взяв с меня еще $125 за разбирательства с legacy-статусом. Затем я вместе с брокером окончательно оформил продажу. Вся процедура с начала до конца заняла месяц, из которого примерно неделю я занимался первоначальным изучением вопроса и выбором брокера.

Итоги

Если описанная процедура кажется вам слишком трудоемкой, то, возможно, вам пока не стоит связываться со вторичным рынком. Но если вы не боитесь аналитической работы, вы в своей компании можете стать тем героем, который возьмется за эту новую задачу. Готовьтесь к тому, что на все про все – привести в порядок свое право собственности (если вы владелец legacy-блока), получить «добро» от юротдела и других подразделений компании, выбрать брокера и затем осуществить саму продажу – может уйти несколько месяцев.

Ссылки и дополнительная литература

1. Коллектив авторов, ConneXions—The Interoperability Report, Volume 8, No. 5, май 1994 г., спецвыпуск: IP: The Next Generation. Доступно на сайте The Charles Babbage Institute: http://www.cbi.umn.edu/hostedpublications/Connexions/index.html
2. Geoff Huston, "Opinion: The Mythology of IPv6," The Internet Protocol Journal, Volume 6, No. 2, июнь 2003 г.
3. Geoff Huston, "IPv4 Address Depletion and Transition to IPv6," The Internet Protocol Journal, Volume 10, No. 3, сентябрь 2007 г.
4. Коллектив авторов, The Internet Protocol Journal, Volume 14, No. 1, март 2011 г. Этот спецвыпуск целиком посвящен вопросам адресации и перехода.
5. Geoff Huston, презентация о нынешних проблемах IP-адресации, декабрь 2019 г. https://www.potaroo.net/presentations/2019-12-11-kismet-addresses.pdf
6. Daniel Karrenberg, Gerard Ross, Paul Wilson, and Leslie Nobile, "Development of the Regional Internet Registry System," The Internet Protocol Journal, Volume 4, No. 4, декабрь 2001 г.
7. Eric Bais, "Transferring IPv4 Resources in the RIPE region," июнь 2016 г. Опубликовано Prefix Broker как ebook. https://www.prefixbroker.com/ebook/
8. Frank Solensky, Proceedings of the 18th IETF, 1990. https://www.ietf.org/proceedings/18.pdf (см. его изначальные предсказания об исчерпании адресов на с. 67 PDF-документа)
9. Daniel Karrenberg, Yakov Rekhter, Eliot Lear, and Geert Jan de Groot, "Address Allocation for Private Internets," RFC 1918, февраль 1996 г.
10. Elise Gerich, "Guidelines for Management of IP Address Space," RFC 1366, октябрь 1992 г.
11. Elise Gerich, "Guidelines for Management of IP Address Space," RFC 1466, май 1993 г.
12. Kim Hubbard, Jon Postel, Mark Kosters, Daniel Karrenberg, and David Conrad, "Internet Registry IP Allocation Guidelines," RFC 2050, ноябрь 1996 г.
13. Пресс-релиз RIPE, ноябрь 2019 г.: "The RIPE NCC Has Run Out of IPv4 Addresses," https://www.ripe.net/publications/news/about-ripencc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses
14. Marc Lindsey, пост в блоге CircleID от июля 2018 г. "An Insider's Guide to the IPv4 Market – Updated," http://www.circleid.com/posts/20180710_an_insiders_guide_to_the_ipv4_market_updated/
15. Ссылки на веб-страницы RIR с описанием их правил передачи адресов: https://www.apnic.net/manage-ip/manage-resources/transfer-resources https://www.ripe.net/manage-ips-and-asns/resourcetransfers-and-mergers https://afrinic.net/resources/transfers https://www.arin.net/resources/registry/transfers https://www.lacnic.net/1019/2/lacnic/resourcestransference
16. Ссылки на опрос ресурсов WHOIS у каждого RIR: База данных AFRINIC: https://www.afrinic.net/whois-web/public/query База данных APNIC: https://wq.apnic.net/apnic-bin/whois.pl База данных ARIN: https://whois.arin.net/ База данных LACNIC: https://lacnic.net/cgi-bin/lacnic/whois База данных RIPE: https://www.ripe.net/manage-ips-and-asns/db
17. APNIC, зарегистрированные брокеры IPv4: https://www.apnic.net/manage-ip/manage-resources/transfer-resources/transfer-facilitators/
18. RIPE, брокеры: https://www.ripe.net/manage-ips-and-asns/resourcetransfers-and-mergers/brokers
19. ARIN, зарегистрированные сервисы передачи адресов: https://www.arin.net/resources/registry/transfers/stls/registered_facilitators/
20. IPv4.Global, данные по ценам с предыдущих аукционов: https://auctions.ipv4.global/prior-sales
21. NANOG, список участников совещания №77: https://events.nanog.org/events/nanog-77/attendees-15-13b224d66c30422494a9627a6dcb6c94.aspx
22. Pv4 Market Group, "Approved IPv4 Address Facilitator for Your IPv4 Needs, a Guide to Questions You Might Want to Ask Your Broker," https://ipv4marketgroup.com/ipv4-market-group/
23. IPv4 Market Group, служба исключения из черных списков. https://ipv4marketgroup.com/broker-services/ipv4-blacklist-removal/
24. IPv4 Market Group, "IPv4 Price Trends," https://ipv4marketgroup.com/ipv4-price-trends/
25. Prefix Broker: https://www.prefixbroker.com/
26. Heficed: https://www.heficed.com/
27. Richard Jimmerson, "On the 'Misuse' of the Internet Number Resource Transfer Market," блог команды ARIN, 26 августа 2020 г. https://teamarin.net/2020/08/26/on-the-misuse-ofthe-internet-number-resource-transfer-market/

Еще раз о приватности, безопасности и Интернетолизации «первого и последнего миллиардов»

Павел Храмцов

Домены и Интернет вещей

Новостные тренды последнего времени, как минимум с прошлого выпуска нашего журнала, не меняются. Безопасность, приватность, регулирование, Интернет вещей и искусственный интеллект. Они постоянно в фокусе внимания прессы и технологических дискуссий в рамках конференций, которые изменили свой формат с офлайна на онлайн, но не перестали быть центром обсуждения инноваций.

Одно из центральных мест на конференции APTLD79, которая прошла с 24 по 25 февраля 2021 года в онлайн-формате, стала тема «DNS и IoT».

Практически любой учебник или «толстая» книжка, посвященная теме DNS, начинается с мысли о том, что хосты (компьютеры и прочие электронные сетевые устройства) общаются между собой с использованием числовых адресов, а вот имена нужны только в качестве понятного интерфейса для взаимодействия человека и машины.

В контексте IoT, когда речь идет об m2m-взаимодействии (машина-машина), тезис от необходимости интерфейса с человеком и, соответственно, необходимость в использовании DNS выглядит на первый взгляд странным и сомнительным.

Тем не менее, DNS для IoT нужен. Например, в докладе Андрея Колесникова[1] были перечислены следующие области применения DNS в IoT:

- поиск облачных сервисов, которые помогают приборам выполнять их функции;
- поиск сайтов с обновлениями программного обеспечения для устройств IoT;
- поиск устройствами IoT сервисных платформ.

При этом было отмечено, что симбиоз устройств IoT и DNS позволяет как расширить возможности устройств, так и несет риски, например, для самого DNS.

В контексте IoT часто заходит речь о сетях 5G. Действительно, роль DNS в мобильных технологиях весома. DNS здесь используется не только для поиска традиционных интернет-ресурсов, но и для внутренних сервисных нужд, например так, как это описано в 3GPP TS 23.401[2]. Фактически речь идет об использовании DNS в качестве механизма конструирования имен путем поиска подстановок и преобразования строк идентификации ресурсов, а не о простом соответствии доменного имени IP-адресу.

В этой связи интересен взгляд на данный вопрос со стороны ICANN. Ален Дюран (Alain Durand) на конференции APTL79[3] проанализировал соответствие технологии DNS требованиям сетей 5G, в частности, по времени отклика на запрос, которое должно быть менее 10 мс. Правда, речь идет о традиционном поиске соответствий имени и адреса, а не о работе ядра системы 5G.

Рассуждения сводятся к тому, что при локальном агрессивном кэшировании задержки в системе DNS не будут иметь существенного влияния на время отклика, т.к. локальный кэш всегда будет отдавать ответы в рамках заданного ограничения в 10 мс, за исключением случаев, когда нужно будет первый раз обратиться в удаленный дата-центр, а таких случаев будет немного.

IETF110: широкий спектр обсуждений DNS

Любой IETF-форум является важной дискуссионной площадкой. Не стал исключением и IETF110. Самый широкий и основательный обзор дискуссий на IETF110 представил Джефф Хьюстон (Geoff Huston[4]). Не будем разбирать все темы, остановимся только на некоторых.

Во-первых, это RFC 8976. Документ описывает механизм контроля целостности файла зоны. Считается, что DNSSEC позволяет убедиться в достоверности информации, которую получает приложение, обратившееся к DNS, но при этом целостность самого зонного файла не гарантирована.

Никто не скрывает, что данный документ направлен на борьбу с недобросовестным использованием копий, например, корневой зоны в рамках подхода, описанного в RFC 7706, 8806.

Следующая тема — это DNS-cookies[5]. Особенность транспорта UDP, который до сих пор доминирует в DNS, позволяет реализовать множество атак, как на систему DNS, так и с использованием системы DNS. Для ограничения количества запросов, которые направляются на DNS-серверы, часто используются Rate Limits, т.е. ограничения количества запросов с одного источника. Это приводит к снижению качества сервиса для добропорядочных пользователей.

Cookies позволяют более аккуратно отсекать неправильно настроенные источники запросов и тем самым обеспечивать стабильность качества сервиса DNS.

Еще одна долгоиграющая тема — это Query Name Minimization[6]. В рамках действующих в настоящее время стандартов исходный DNS-запрос направляется в неизменном виде всем авторитетным серверам, которые участвуют в рекурсивной цепочке поиска. Таким образом, и администратор авторитетного сервера корневой зоны, и администратор авторитетных серверов доменов первого/второго уровня, одним словом – все, имеют доступ к статистике обращений конечных клиентов определенного резолвера. Вообще говоря, в современных условиях борьбы за приватность такое положение дел следует признать неправильным.

QName Minimization предлагает передавать авторитетным серверам только ту информацию, на которую у них есть ответ, и не более, т.е., например, к авторитетным серверам корневой зоны будут поступать запросы только по информации, связанной с доменами первого уровня (TLD).

В рамках IETF110 продолжалось обсуждение расширения сфер применения DNS. В частности, этому посвящен драфт о встроенных сервисных записях ресурсов (SVCB и HTTPS)[7].

Тему сервисных записей мы уже затрагивали в контексте IoT, здесь речь в основном идет о записях, связанных с безопасностью. Частично данный документ отражает потребности CDN (получение авторитетных альтернативных точек обслуживания), а также связан с защитой информации.

Важным моментом в DNS является валидация точек делегирования. В стандарте RFC 1034 есть требование консистентности информации между родительской зоной и зоной-потомком. Но механизма, который обеспечивал бы такую консистентность, нет. Вопрос важный и довольно часто встречающийся в практике разбора некорректности работы DNS. Администратор зоны частенько забывает поменять информацию в родительской, внося изменения в свою зону. Администратор родительской зоны также может поменять информацию о делегировании дочерней зоны. Предлагается прояснить этот вопрос обработки такого рода ситуаций резолверами в отдельном RFC[8]. В основном, данный документ касается вопросов, связанных с DNSSEC и валидацией.

Данный список DNS-тем не исчерпывающий, но завершить его хочется вечным вопросом: почему нельзя DNS полностью перевести на транспорт TCP. Дискуссии об этом идут уже не один год. IETF110 в этом смысле не стал исключением. Ответ: накладные расходы при работе по TCP слишком велики. Но и отказываться от TCP тоже нельзя, глядя на все улучшения, которые за последние годы внесены в DNS.

Цена приватности

Приватность – это хорошо и важно. Но, как у всего, у приватности тоже есть цена. Для определенности остановимся на сравнении технологий «обычного» DNS (Do53) и DNS-over-TLS (DoT). Мы уже в контексте IoT упоминали о времени отклика при обращении к DNS. Эксперимент Trinh Viet Doan[9] позволяет сравнить традиционный протокол DNS (Do53) с DNS-over-TLS с точки зрения времени отклика на запрос пользователя (рис. 1).

В публикации указывается, что время отклика для большинства стандартных резолверов при использовании Do53 в рамках данного эксперимента укладывается в 10-30 мс, в то время как отклик при использовании протокола DoT для самых быстрых резолверов находится в интервале от 130 до 150 мс, т.е. разница в порядок.

Например, для разных регионов мира dnsperf приводит следующие средние времена отклика публичных резолверов[10] (рис. 2):

В данном случае приведено среднее время по всем регионам Земли. Времена больше 100 мс – это скорее исключение, чем правило.

Рисунок 1. Кумулятивная функция распределения ответа на запрос пользователя при использовании Do53 и DoT.

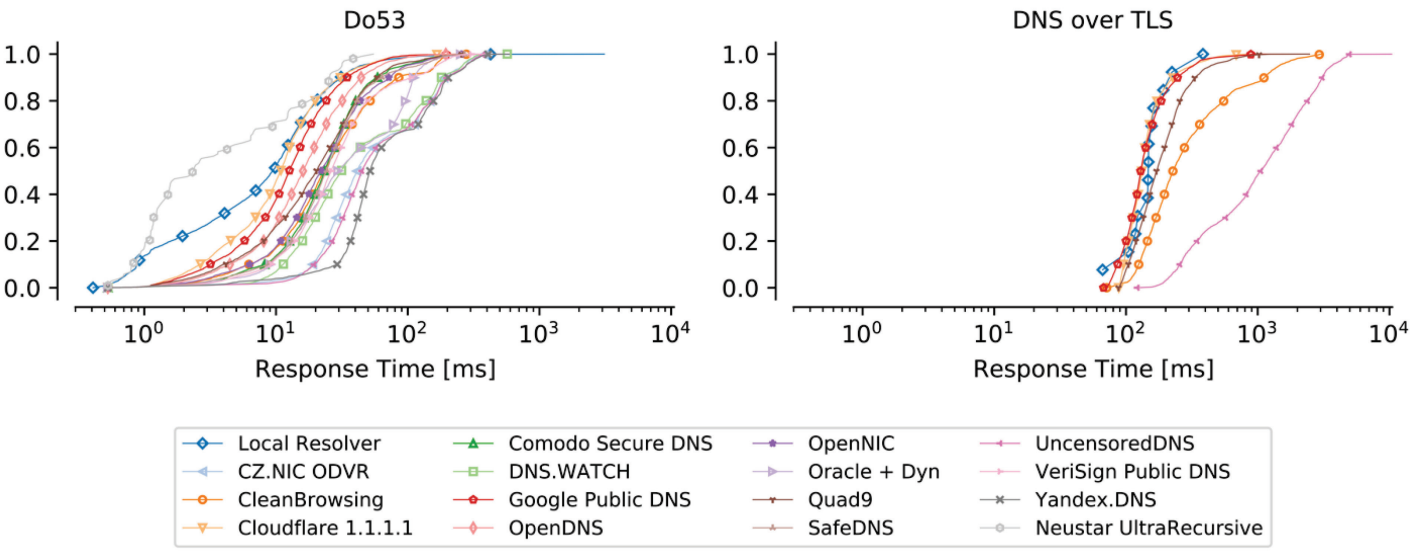
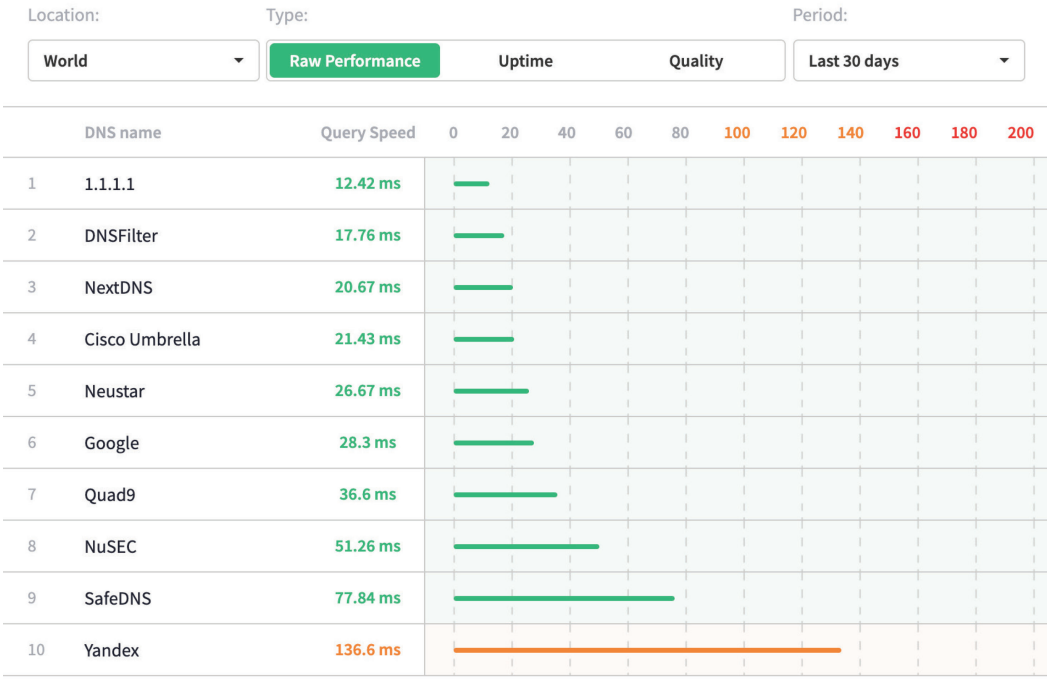


Рисунок 2. Средние времена отклика публичных резолверов.



Так что, приватность приватностью, а производительность диктует свои предпочтения.

Раз уж пришлось сослаться на статистику открытых резолверов, то уместно будет в контексте обсуждения приватности и безопасности упомянуть об интервью[11] Билла Вудкока (Bill Woodcock), председателя совета учредителей Quad9 (седьмая позиция на рис. 2), которое он дал представителям CENTR.

Quad9 уделяет много внимания сохранению приватности своих клиентов. Это стало причиной переезда компании из США в Швейцарию, что само по себе уже любопытно.

Quad9 первой внедрила на своих резолверах DoT. И, похоже, не шла навстречу всем запросам американских правоохранителей. В связи с такой политикой компании интервьюер из CENTR задал вопрос о борьбе с противоправным использованием доменных имен, о блокировках и других инструментах фильтрации, применяемых компанией. Вопрос был задан в контексте блокировок так называемых ковидных сайтов (ложные новости о распространении вируса, методах лечения, лекарствах, прививках, мошенничество со справками, некорректная статистика и др.) со ссылкой на исследование Университета Мичигана[12].

Вудкок сообщил, что Quad9 на своих серверах активно применяет фильтрацию. В среднем серверы компании блокируют в моменте доступ к примерно 3,4 млн доменных имен, связанных с фишингом и распространением вредоносного ПО. Это количество изменяется ежедневно в приделах 300 тыс. имен. Бывают и ложные срабатывания фильтров. Ошибка составляет около 2%.

В общем, DNS Blacklists используется не только Spamhous-ом, но и остальными компаниями, которые предоставляют публичные сервисы, даже теми, которые ставят приватность своих пользователей на первое место и меняют из-за этого юрисдикцию.

Любопытно, что массированная дискуссия по поводу приватности в DNS, вызванная протоколами DNS-over-HTTPS и DNS-over-TLS, вызвала различного рода инициативы в Европе, призванные регулировать обмен информацией. 30 марта 2021 года свет увидел документ «European DNS Resolver Policy»[13]. В нем обсуждаются обязанности DNS-провайдеров по удовлетворению требований GDPR, которые при применении DoH и DoT могут быть с легкостью обойдены. Документ есть, а механизмы его соблюдения пока не очень понятны.

Завершая тематику DNS, нельзя пройти мимо последнего издания «VerisignIndustry Brief»[14].

Ряд показателей этой публикации постоянно вызывают некоторое удивление, как, например, количество доменов в национальном домене .ru[15], но тем не менее, нахождение домена .ru на девятом месте среди всех доменов верхнего уровня глаз радует. Среди страновых доменов .ru занимает шестое место по количеству зарегистрированных доменов второго уровня.

Еще одну историю по поводу приватности и безопасности, на мой взгляд, довольно любопытную, рассказал ресурс Motherboard[16]. Речь идет о покупке американскими военными «гражданских» данных геолокации для Командования специальных операций у компании X-Mode.

Дело в том, что X-Mode платила разработчикам мобильных приложений за включение своих SDK в эти самые приложения. Приложения передавали данные геолокации в X-Mode, а та уже этими данными торговала.

Утверждается, что данные были анонимизированы, но военные уверены, что привязать их к конкретным персонам не составляет труда.

X-Mode, по словам своего генерального директора, имела доступ к трекам 25 млн устройств в США и 40 млн устройств за их пределами. SDK от X-Mode используется примерно в 400 приложениях.

Похоже, стоит поинтересоваться, какие приложения стоят на ваших устройствах и какой SDK использовался при их разработке.

Миссионеры

В заключение - новости совсем из другой области, но связанные с популяризацией Интернета.

Компания Aphabet (материнская компания Google) закрыла проект Loon[17]. Loon стартовал в 2013 году и своей задачей ставил обеспечение Интернетом на приличной скорости всех людей в богом забытых уголках Земли.

Сделать это предполагалось при помощи стратостатов и беспроводной оптики. К сожалению, проект не «взлетел», как говорится. И причина была не в самой возможности организации такой сети, а в отсутствии платежеспособности стран «последнего миллиарда». И хотя в Кении Loon смог в итоге стать коммерческим, для продолжения проекта в глобальном масштабе этого оказалось явно недостаточно.

Но технологии Loon не пропали зря. Например, беспроводная оптическая связь в настоящее время используется в проекте Taara[18].

Любопытно, что кроме очевидных областей применения беспроводной оптической связи, таких как труднодоступные районы, лесные массивы, реки или железнодорожные пути, т.е. все те случаи, когда прокладка кабеля затруднена или невозможна по объективным причинам, в проекте также указаны и участки земли в частной собственности с высокой стоимостью.

В настоящее время разработчики Taara сосредоточены на достижении надежной связи со скоростью 20+ Gbps на расстояние в 20+ км.

Возможно, что если бы проект широкополосной связи развивался в США, а не для «последнего миллиарда», то его не закрыли бы, а дождались реализации правительственной инфраструктурной программы, которую продвигает администрация нового президента США[19].

В рамках этой программы предполагается потратить $100 млрд на развитие широкополосной связи и дотянуться этой связью до «самых отдаленных уголков» их «необъятной страны».

Звучит знакомо. Интересно, какой будет результат.

Ссылки

1. https://aptld.org/wp-content/uploads/6-1-IoT-DNS-IOTAS.pdf
2. https://www.etsi.org/deliver/etsi_ts/123400_123499/123401/15.04.00_60/ts_123401v150400p.pdf
3. https://aptld.org/wp-content/uploads/6-3-DNS-IoT_A-view-from-ICANN-Office-of-the-CTO.pdf
4. https://blog.apnic.net/2021/04/01/dns-at-ietf-110/
5. https://tools.ietf.org/html/rfc7950
6. https://tools.ietf.org/html/rfc7816
7. https://tools.ietf.org/html/draft-ietf-dnsop-svcb-https-04
8. https://tools.ietf.org/html/draft-ietf-dnsop-ns-revalidation-00
9. https://blog.apnic.net/2021/04/13/measuring-dns-over-tls-from-the-edge/
10. https://www.dnsperf.com/#!dns-resolvers
11. https://centr.org/news/blog/quad9.html
12. https://censoredplanet.org/assets/covid.pdf
13. https://europeanresolverpolicy.com/
14. https://www.verisign.com/assets/domain-name-report-Q42020.pdf
15. По данным cctld.ru на момент публикации Verisign в домене RU было зарегистрировано 4982070 доменов, а не 5,7 млн, как указано в Verisign. Возможно, что в статистику попадают не только домены второго уровня.
16. https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x
17. https://x.company/projects/taara/
18. https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/?fbclid=IwAR3ZV48F3dIMcE4tImsQPBESKWVY1ZN75MmLh-jwdC8NfIXwsCjINfKX84E
19. https://blog.x.company/loons-final-flight-e9d699123a96

Рисунок 3. Стратостат проекта Loon (фото с сайта блога компании x.company).

Безопасность российского доменного пространства
До, во время и после пандемии

Год назад во второй половине марта стало очевидно, что все происходящее, к сожалению, всерьез и надолго, и пандемия коронавируса COVID-19 вносит очень серьезные коррективы не только в офлайновую, но и в онлайновую жизнь. При этом вопросы безопасности в онлайне (впрочем, как и в офлайне) практически сразу вышли на первый план. Естественно, возник вопрос, что Координационный центр доменов .RU/.РФ как национальная регистратура может сделать в рамках своих полномочий и умений, чтобы сохранить стабильность хотя бы внутри системы регистрации российских национальных доменов — ведь любые кризисные ситуации влияют на поведение людей, и часто это влияние непредсказуемо. Итак, вот шаги, которые были сделаны КЦ для стабилизации ситуации в доменном пространстве.

Мониторинг «коронадоменов»: пандемия, вакцинация, выплаты

Уже в середине марта 2020 года был оперативно организован мониторинг так называемых коронаассоциированных регистраций новых имен в доменах .ru и .рф. Запустив мониторинг, мы заодно посмотрели и исторические данные — за январь и февраль 2020 года, когда угроза уже была явной, но в пандемию еще никто не верил. Не верили в нее и доменные инвесторы, а также кибермошенники — сколь-нибудь значимый рост числа регистраций произошел только в начале марта, а пик пришелся на 17 марта.

Максимальное число «коронарегистраций» было зафиксировано в марте и апреле прошлого года — 1936 и 1555 доменных имен соответственно (рис. 1). Менее всего такими доменами пользователи интересовались в январе и сентябре 2020 года: тогда российские доменные зоны пополнились 90 и 120 коронавирусными доменами соответственно. За год в список «коронадоменов» было добавлено 4907 доменных имен в .ru и 984 в .рф; в общей сложности к концу 2020 года в российских доменных зонах насчитывался 5891 домен, тематически связанный с пандемией (подробная информация на рис. 2).

Рисунок 1.

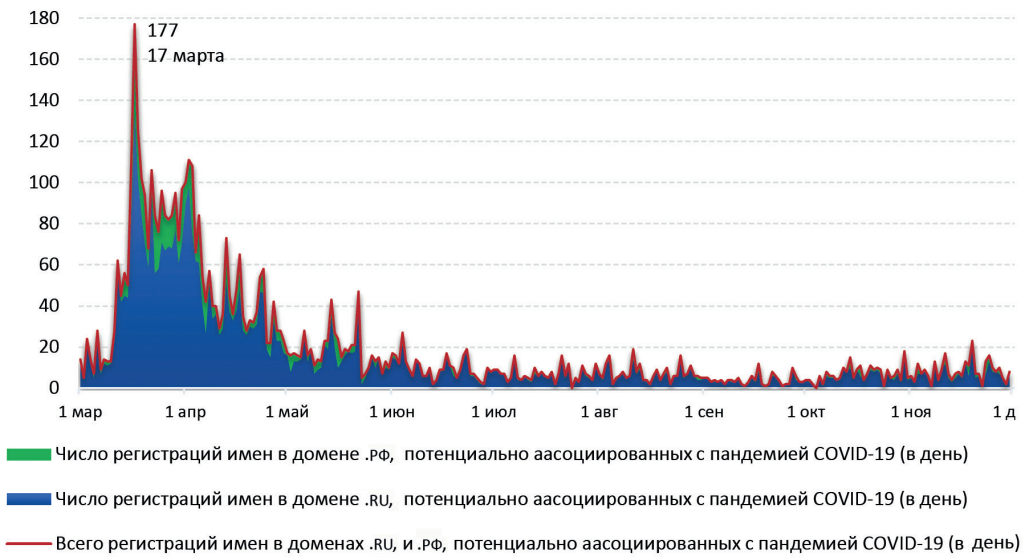


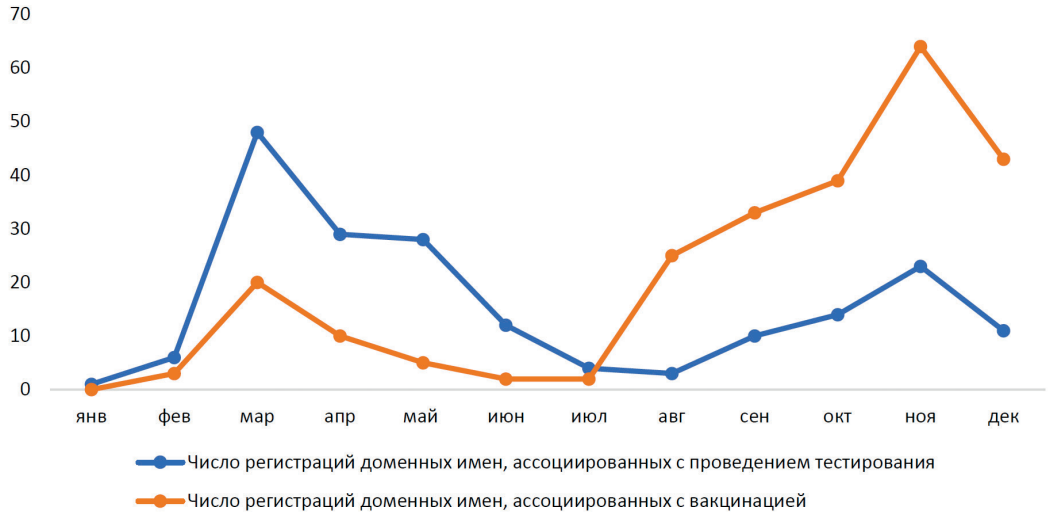
Рисунок 2.

	.RU	.РФ	Всего
Январь	67	23	**90**
Февраль	211	31	**242**
Март	1 573	363	**1 936**
Апрель	1 278	277	**1 555**
Май	458	101	**559**
Июнь	275	26	**301**
Июль	194	20	**214**
Август	205	23	**228**
Сентябрь	104	16	**120**
Октябрь	177	35	**212**
Ноябрь	208	45	**253**
Декабрь	157	24	**181**

Достаточно сложным оказался вопрос выбора ключевых слов для мониторинга. Естественно, что были однозначные ключевые слова, но также каждый новый этап (например, введение пропускного режима или начало выплат детский пособий) добавлял свою лепту в пополнение списка ключевых слов. При этом подход к мониторингу был очень взвешенным.

Любое важное событие в стране или мире вызывает свой, пусть и разный по силе отголосок в доменной среде. В середине мая было объ-

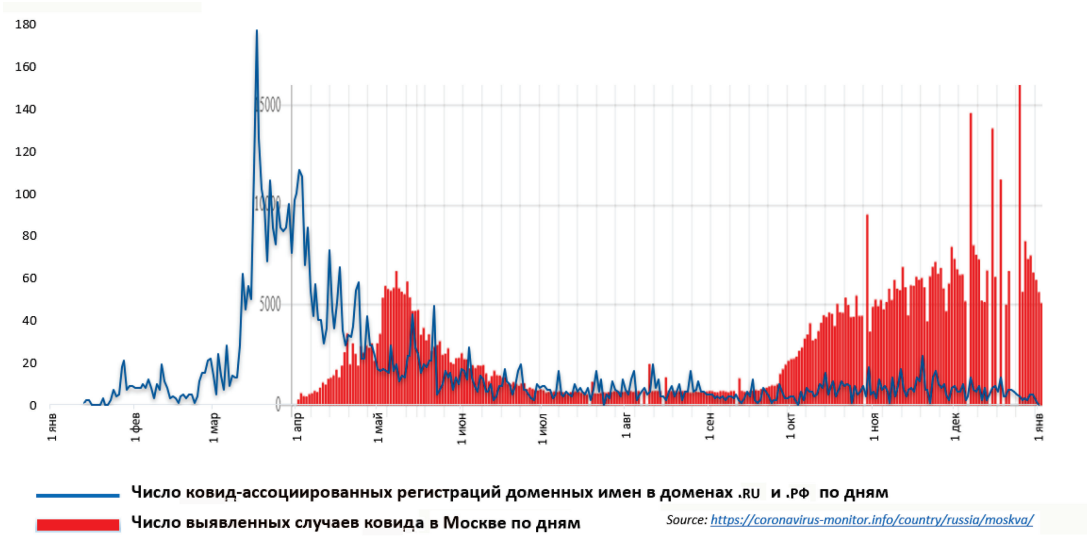
Рисунок 3.



напоминает инкубационный период. Коллективный разум уже осознал угрозы, а тело отреагировало с задержкой. Во «вторую волну» такого эффекта уже не было.

Не стоит думать, что все доменные имена, в которых есть ключевые слова, несут в себе какой-то негативный смысл. Это и информационные ресурсы, и вполне легальные интернет-магазины, и многое другое. Например, всем известный официальный ресурс стопкоронавирус.рф тоже содержит ключевое слово и даже не одно.

Рисунок 4.



И в этом свете очень показательна картина сравнения темпов регистрации «коронаассоциированных» доменов в Европе и в России – здесь можно наблюдать схожие паттерны поведения. Может быть не совсем корректно сравнивать происходившее в абсолютных величинах, т.к. европейские пользователи регистрировали похожие имена и в доменах своих стран, но общий тренд в России и в Европе очень похож: отрицание – ажиотаж – плато – спад (рис. 5).

явлено о выплатах пособий семьям с детьми, и это событие сразу же отразилось в мониторинге. В этом случае интерес был кратковременным, но тем не менее даже 1-2 фишинговых ресурса могли нанести ощутимый удар по достаточно уязвимой категории пользователей.

На рис. 3 представлена динамика регистраций доменных имен в домене .ru, которые ассоциировались с проведением тестирования и вакцинацией.

Кстати, очень показательно было сравнивать динамику заболеваемости и числа регистраций доменных имен (рис. 4) — особенно интересные закономерности выявились в «первую весеннюю волну». Временной лаг между всплесками числа регистраций и ростом заболеваемости составил примерно две недели, что подозрительно

Другой показательный пример: компания Dataprovider проводила исследование регистрации во всем мире доменов, содержащих слово corona и remote (отсылка к удаленной работе). Пик регистраций в мире также пришелся на середину марта.

Рисунок 5.

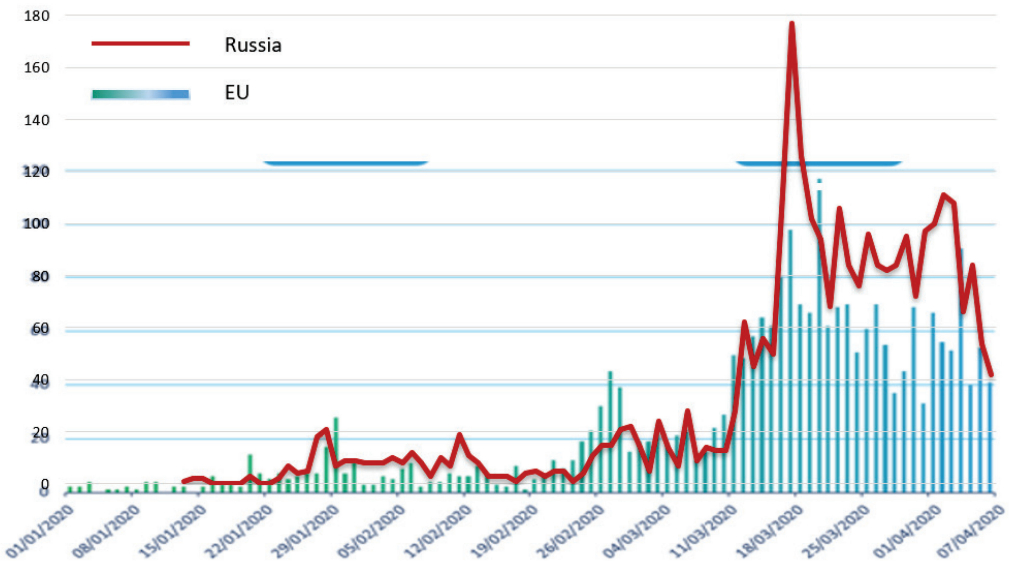
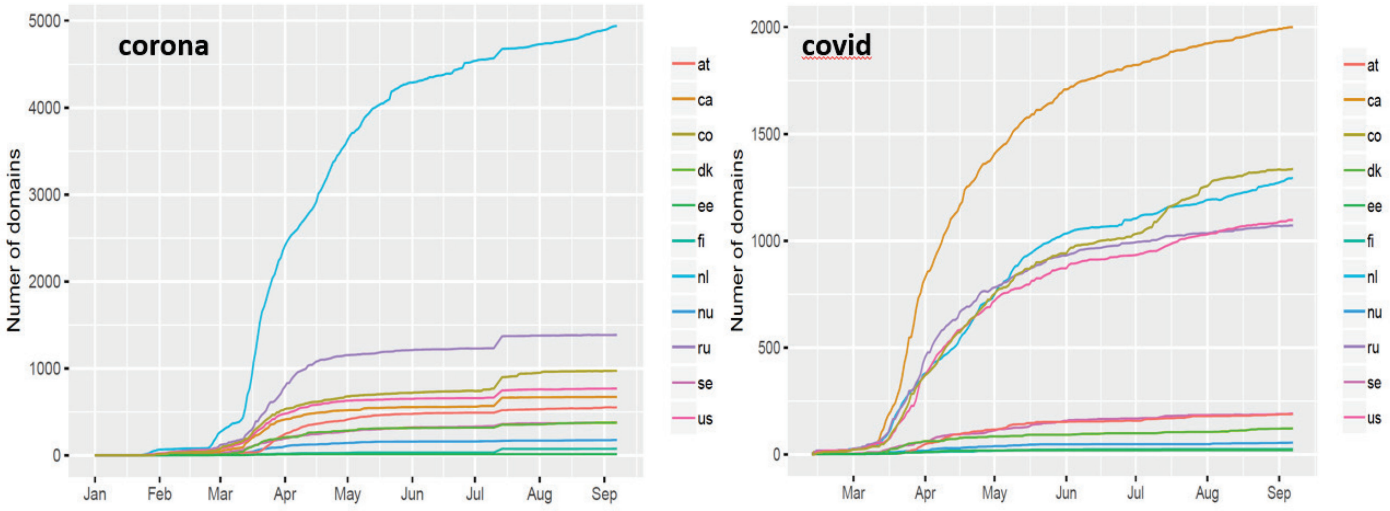


Рисунок 6.
Число регистраций доменов, содержащих слово «corona» или «covid» в некоторых ccTLD.111111111111111111



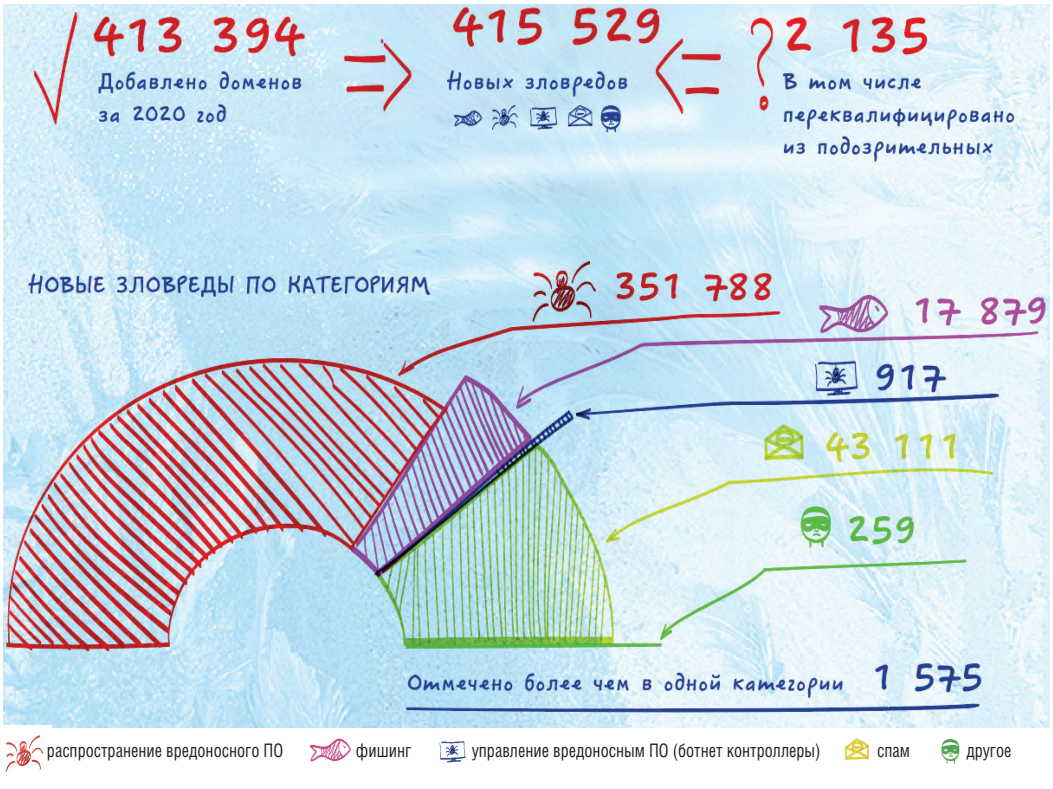
Source: Open INTEL https://openintel.nl/

Обеспечиваем безопасность пользователей

Безусловно, Координационный центр не остался безучастным к проблемам, которые возникли в доменном пространстве в связи с пандемией COVID-19. С первых дней эскалации кризиса Координационный центр не только инициировал мониторинг COVID-ассоциированных регистраций новых имен в доменах .ru и .рф, но и привлек к этой работе институт компетентных организаций, а также информационно-аналитическую платформу «Нетоскоп». Общей задачей было выявить потенциально опасные ресурсы (например, те, которые могли бы использоваться для фишинга или распространения вредоносного ПО) и снизить возможный вред от них с помощью наших «патрульных», т.е. уже упомянутых компетентных организаций.

Координационный центр внедрил практику взаимодействия с организациями, компетентными в определении нарушений в сети Интернет, еще в 2012 году. Эти организации, сейчас их 10, наделены Координационным центром правом направлять аккредитованным регистраторам требования о прекращении делегирования доменных имен для подобных ресурсов. В свою очередь, регистраторы, руководствуясь правилами регистрации доменных имен в доменах .ru и .рф, вправе прекратить делегирование доменных имен по запросам компетентных организаций.

Рисунок 7.



Отчет проекта «Нетоскоп» за 2020 год
(Источник: https://netoscope.ru/ru/reports/archive)

В августе 2020 года заработал проект «Доменный патруль», где представлены все компетентные организации и собраны новости интернет-безопасности, информация о киберугрозах, инструкции, как поступить, если пользователь столкнулся с одной из таких угроз, скажем, с мошенничеством, и главное – перечень «горячих линий» компетентных организаций. Любой пользователь может обратиться на линию и сообщить об обнаруженном им случае неподобающего использования

доменного имени, меры будут приняты оперативно. Также здесь происходит оперативный обмен запросами о прекращении или, наоборот, восстановлении делегирования доменных имен между КО и регистраторами. На рис. 8 и 9 приведены данные отчета по результатам взаимодействия компетентных организаций и регистраторов в рамках проекта «Доменный патруль» за 2020 год (Источник: https://tldpatrol.ru/ upload/iblock/137/KO_2020.pdf)

Также с 2012 года существует проект «Нетоскоп». Это первый в России информационно-аналитический ресурс, посвященный информационной безопасности в доменном пространстве. В рамках проекта была разработана специальная платформа, с помощью которой участники проекта могут обмениваться информацией и совершенствовать свои алгоритмы поиска «зловредных» ресурсов. Посетителям сайта доступен онлайн-сервис по проверке доменных имен на использование в «зловредной» активности, зафиксированной компаниями-участниками проекта. В базу данных проекта «Нетоскоп» участниками было добавлено более 400 тысяч доменных имен, включая второй уровень и более низкие. Львиная доля этих ресурсов была ассоциирована с распространением вредоносного ПО.

От компетентных организаций было получено более 10 тысяч обращений о прекращении делегирования, из них около девяти тысяч - фишинговые ресурсы. Эти данные почти на 40% выше тех, с которыми был закончен 2019 год.

Почти 90% запросов были связаны с доменами, которые вели на фишинговые ресурсы. Специалисты по кибербезопасности хорошо знают, что фишинговый сайт существует не более суток, а основной поток пользователей попадает на него в течение нескольких часов. Поэтому крайне важно, чтобы меры по прекращению доступа к ресурсу были приняты быстро. В рамках проекта «Доменный патруль» взаимодействие экспертов и аккредитованных регистраторов отработано на отлично, и скоординированность действий всех сторон позволяет значительно сокращать число жертв сетевых мошенников.

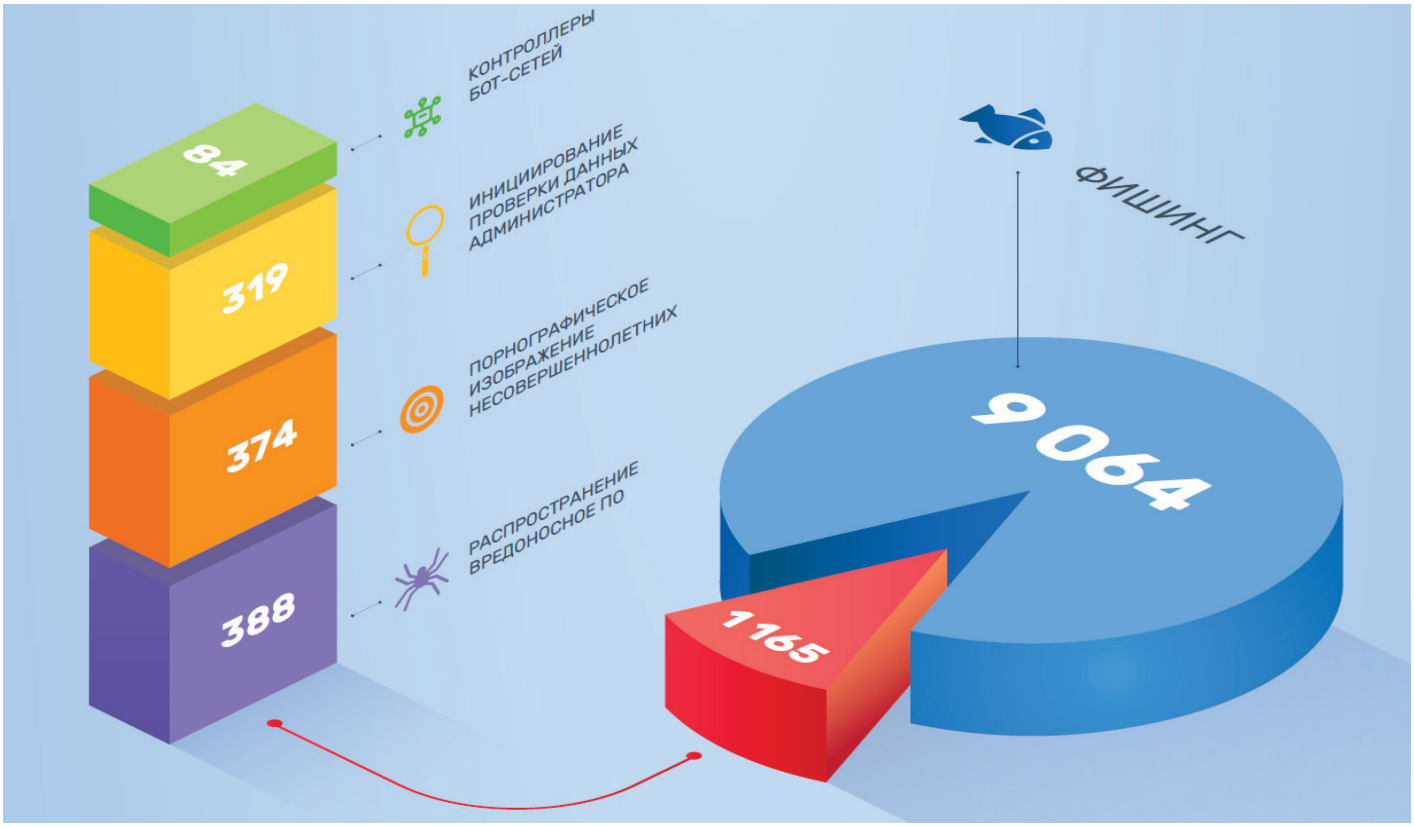
Например, «Лаборатория Касперского», входящая в состав института компетентных организаций, установила в своих продуктах флаг «угроза потери данных» для 1901 «корона-домена» за год: 1600 в .ru и 301 в .рф – это около 32% от общего количества коронавирусных доменных имен. Установка такого флага означает, что все устройства, защищенные антивирусом «Лаборатории», получат информацию об этих доменных именах и предупредят пользователей, которые заходят на них, о возможной угрозе.

Сотрудничество КО с аккредитованными регистраторами не первый год доказывает свою эффективность. По итогам 2020 года большинство ресурсов так или иначе прекратило свое существование (или по крайней мере нанесение вреда другим пользователям). В отдельных случаях регистраторы не усматривали оснований для прекращения делегирования, по таким случаям мы проводим дополнительные исследования для определения слабых мест отработанной схемы. Или, наоборот, сильных мест, т.к. от ошибок не застрахована даже самые компетентные организации.

Главный приоритет – безопасность доменного пространства

Несмотря на то, что 2020 год потребовал от Координационного центра доменов .RU/.РФ очень серьезных усилий в борьбе с фишингом, связанным с «коронавирусными» доменами, не прекращалась и основная работа по обеспечению безопасности реестров российских национальных доменов.

Рисунок 8.



Так, осенью 2020 года в режиме опытной эксплуатации началось предоставление услуги по депонированию реестров российских национальных доменов .ru и .рф. Проект по внедрению дополнительных организационно-технических мер, направленных на обеспечение непрерывности функционирования системы адресации, а также обеспечивающих дополнительную защиту прав администраторов и пользователей доменных имен путем внедрения на российской платформе механизмов, предоставляющих дополнительные гарантии сохранности информации о доменных именах и бесперебойного функционирования системы адресации в целом, был инициирован еще в 2019 году по поручению министерства цифрового развития, связи и массовых коммуникаций РФ.

А в марте 2021 года Координационный центр доменов .RU/.РФ начал осуществлять депонирование данных (Data Escrow) уже в штатном режиме. Агентом депонирования является АО «Центр взаимодействия компьютерных сетей «MSK-IX» – единственная аккредитованная ICANN компания для Data Escrow в России. Техническую поддержку оказывает «Технический центр Интернет» – оператор реестров доменов .ru и .рф.

Цель депонирования – принятие дополнительных мер по обеспечению сохранности информации, содержащейся в реестрах, повышение устойчивости функционирования системы регистрации и дополнительная защита прав администраторов доменных имен в случае нарушения работы систем основного оператора реестров. В отличие от общих доменов верхнего уровня (gTLD), депонирование данных реестров не является обязательным для регистратур национальных доменов верхнего уровня (ccTLD).

Уроки кибербезопасности для пользователей

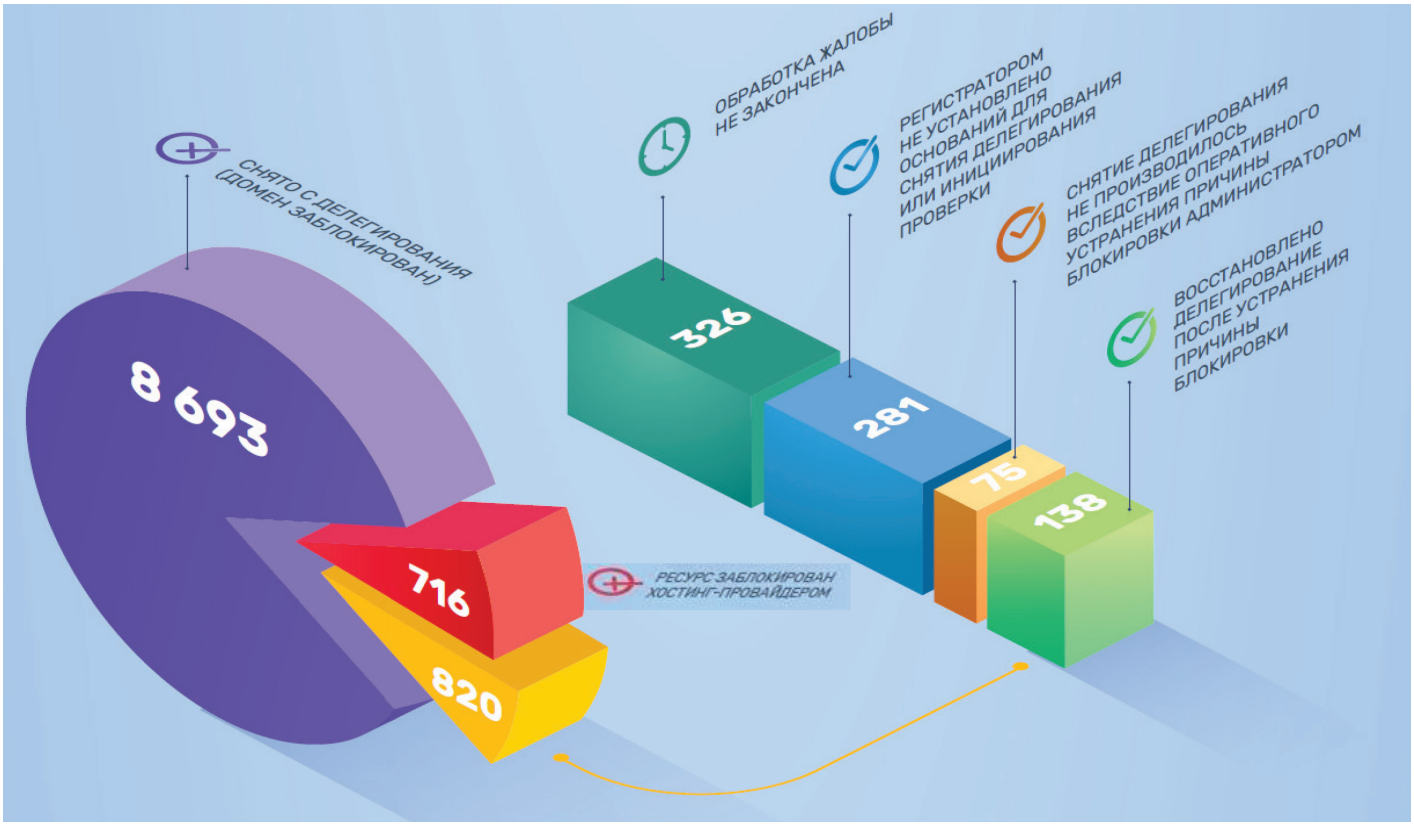
Какие бы усилия по обеспечение безопасности в интернете ни предпринимались, без повышения киберграмотности пользователей значительных успехов в этом направлении ожидать не приходится. Поэтому Координационный центр доменов .RU/.РФ старается просвещать пользователей по вопросам безопасного использования веб-ресурсов. Например, в рамках интерактивного проекта «Изучи интернет – управляй им», где устройство Интернета и цифровых технологий можно изучать с помощью игр. Несколько игровых модулей проекта как раз посвящены теме безопасности: охране персональных данных, фишингу, защите от разнообразных интернет-угроз.

В 2021 году выпущена брошюра «Азбука доменной безопасности», предназначенная для администраторов доменных имен. Эта брошюра подскажет, о чем нужно помнить и на что обращать внимание, чтобы защитить свое доменное имя и связанные с ним данные.

В ней есть очевидные правила, которые, однако, очень часто не соблюдаются пользователями, например: «Будьте предельно бдительны при работе с панелью управления доменным именем, не раскрывайте свои авторизационные данные третьим лицам».

А есть и специфические советы: «Критично относитесь к письмам продлить срок регистрации доменного имени, обращайте внимание на адрес отправителя и указанную контактную информацию». Это важно перепроверять, т.к. кибермошенники нередко выдают себя за регистраторов, отправляя владельцам доменных имен ложные письма об истечении срока их регистрации и необходимости срочного продления. Если отнестись к этому невнимательно, то можно оказаться на крючке мошенника: вы лишитесь домена, а ваш сайт – имени, адреса в Интернете.

Рисунок 9.



MSK IX

10
ГОРОДОВ

500+
УЧАСТНИКОВ

42
ПЛОЩАДКИ

21
УЗЛЕЛ DNS-СЕТИ

ПОДКЛЮЧЕНИЯ ДО
100G

ТРАФИК
3,3Тбит/с

MSK-IX ускоряет коммуникации между интернет-компаниями, предоставляя нейтральную платформу Internet eXchange для обмена IP-трафиком между сетями и глобальную распределенную сеть DNS-серверов для поддержки корневых доменных зон.

Более 500 организаций используют сервисы MSK-IX для развития сетевого присутствия в 10 городах. К MSK-IX подключены операторы связи, социальные сети, поисковые системы, видеопорталы, провайдеры облачных сервисов, корпоративные и научно-образовательные сети.

127083, г. Москва, ул. 8 Марта, д. 1, стр. 12
тел.: +7 495 737-92-95
www.msk-ix.ru

+7 495 737-92-95

WWW.MSK-IX.RU