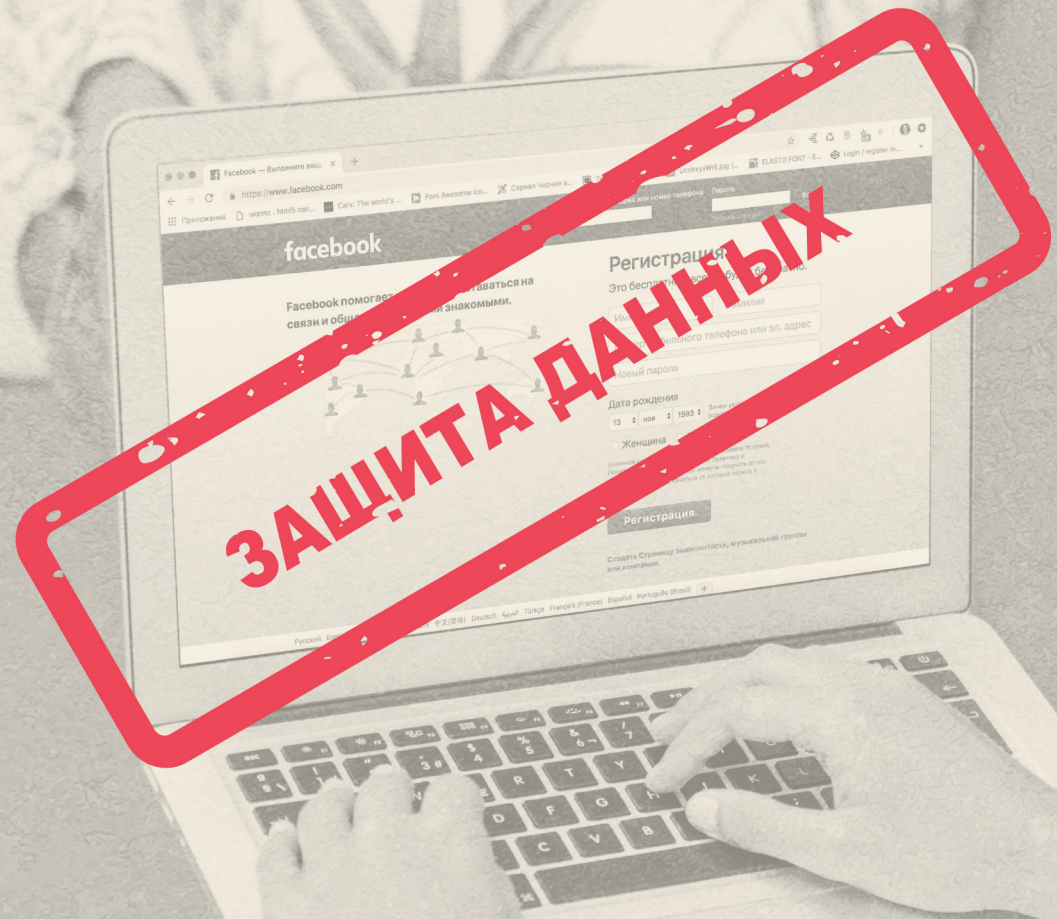
№10
ноябрь 2018

MSK IX

Интернет изнутри



Интернет в цифрах
Защита персональных данных
с.8

Всеобъемлющая безопасность электронной почты в Интернете
Угрозы аутентичности и конфиденциальности электронной почты
с.10

Угрозы доверия(ю)
Основной тренд современного развития технологий
с. 42

Календарь событий
Лучшие события 2018-2019 года
с. 56

Конфиденциальность

Деятельность IETF в области конфиденциальности

Основные протоколы Интернета, такие как DNS, HTTP, SMTP, были разработаны во время, когда вопросы безопасности и сценарии атак выглядели более безобидно

с. 26

Содержание:

Передовица
с. 4

Криптофанатики
Быть может, IETF действительно не права, и власть в ней захватили криптофанатики?

Интернет в цифрах
с. 8

Защита персональных данных
Какие данные шифруют организации

Технология в деталях
с. 10

Всеобъемлющая безопасность электронной почты в Интернете
Угрозы аутентичности и конфиденциальности электронной почты

Стандарты Интернета
с. 26

Деятельность IETF в области конфиденциальности
Шифрование по-прежнему является приоритетом в IETF

Политика
с. 30

Регулирование персональных данных в правовой системе Европейского Союза
Регламент GDPR

Безопасность
с. 42

Угрозы доверия(ю)
Основной тренд современного развития технологий

Новости науки и техники
с. 46

Безопасность и современные тренды
Монополизация DNS

Новости науки и техники
с. 52

Новости доменной индустрии
Лучшие события года

Календарь событий
с. 56

2018-2019 год
Журнал «Интернет изнутри» рекомендует

Журнал «Интернет изнутри»
По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №10, дата выхода: ноябрь 2018 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

Дизайн:
Чернега Наталья

Корректор:
Рябова Наталья

«В Интернете никто не знает, что ты собака»

главный редактор,
Андрей Робачевский

Дорогой читатель!

Тема этого юбилейного (!) номера – **«Конфиденциальность»**. Этим весьма емким термином мы постарались охватить более широкий спектр проблем. Это и собственно конфиденциальность, и анонимность, и защита личной информации, но также и технологии, и юридические аспекты данной области.

Поэтому в этом номере вы сможете познакомиться с истоками криптографического энтузиазма в IETF, о которых рассказывает Джеф Хьюстон в статье «Криптофанатики», и узнать о проблемах и решениях безопасности и защиты конфиденциальности в системе электронной почты, и подробнее познакомиться с вопросами регулирования персональных данных в правовой системе Европейского Союза в статье Мадины Касеновой. В разделе «Новости науки и техники» Павел Храмцов останавливается на нескольких темах, связанных с доверием – еще один связанный с конфиденциальностью аспект.

В 1993 году в журнале The New Yorker появился рисунок карикатуриста Питера Штейнера с подписью «В Интернете никто не знает, что ты собака». Это наблюдение, неоспоримое 25 лет назад, сегодня нуждается в существенной корректировке. Проблема, конечно, в слове «никто».

Рисунок Питера Штейнера
в журнале «Нью-Йоркер», 1993 г.

Сегодня возможность сохранения анонимности существенно ограничена. Считается само собой разумеющимся, что социальные сети знают о нас больше, чем мы сами - в конце концов, многие прямо или косвенно (тем, как мы реагируем на сообщения в сети, какие новости предпочитаем и т.д.) охотно делятся там личной информацией.

Но для простого пользователя, даже при желании, анонимность почти невозможно сохранить. Мало кого удивляет, что предлагаемая реклама удачно соответствует недавнему поиску в вебе, пусть и на другом устройстве. А это лишь верхушка айсберга консолидации персональных данных.

Иногда можно услышать, что конфиденциальность не так важна, если нечего скрывать. На первый взгляд, это действительно так - в большинстве индивидуальных случаев результатом нарушения конфиденциальности может быть неудобство. Однако пренебрегая индивидуальной конфиденциальностью, мы неосознанно вносим вклад в социальную проблему общественного масштаба.

Как заметил профессор Гарвардского университета Джонатан Зиттран в своей книге *«Будущее Интернета - и как его предотвратить»*, *«Сердце проблемы конфиденциальности следующего поколения возникает из-за аналогичных, но нескоординированных действий людей, которые могут быть объединены по-новому»*.

В нашем оцифрованном мире действия и связанные с ними данные не забываются, они накапливаются и могут быть объединены и использованы неведомыми сегодня способами. Это еще одна из причин, почему так важна конфиденциальность.

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.

Криптофанатики

Джефф Хьюстон (Geoff Huston)

Я хочу кратко изложить свою позицию по поводу недавней статьи Тони Рутковски (Anthony Rutkowski) в CircleID (http://www.circleid.com/posts/20180225_humming_an_open_internet_demise_in_london/), где он называет IETF сборищем «криптофанатиков». С его точки зрения, IETF занимается вредительством, пытаясь запрятать как можно больше протоколов Интернета внутрь шифрованных сеансов. Тони утверждает, что работа ETSI над протоколами безопасности для сетевых приставок является более разумным подходом, а массовое включение TLS в стандарты протоколов IETF приведет лишь к тому, что регуляторы заставят сетевых операторов повсеместно блокировать сеансы TLS в своих сетях.

Быть может, IETF действительно не права, и власть в ней захватили криптофанатики, которые протал-кивают шифрование всего и вся в ущерб интересам дела?

Если оглянуться на несколько десятилетий назад, когда все мы писали и внедряли протоколы, передававшие данные в открытую, так и хочется поразиться нашей тогдашней наивности. Но так ли справедлива эта оценка? Интернет далеко не сразу превратился в новый глобальный протокол коммуникации. Поначалу это был гораздо менее амбициозный эксперимент по конструированию сетей с коммутацией пакетов. Он вырвался на свободу из лаборатории, пожалуй, даже не только из-за простоты и врожденной масштабируемости своей структуры, но и просто потому, что других вариантов, которые были бы популярны у компьютерщиков, попросту не было. Но, так или иначе, тогда мало кто задумывался о шифровании полезной нагрузки или даже самих протоколов.

Да, мы знали, что во времена сетей на общей шине Ethernet можно было включить «неразборчивый» (promiscuous) режим и прослушивать весь трафик в канале, но мы были уверены, что только сетевые администраторы знают, как это делается – но если уж нельзя доверять админу, то кому вообще можно верить? Потом появился Wi-Fi, и нас ждало отрезвление. Теперь мои данные, в том числе все мои пароли, стали в открытую передаваться по радио, где их мог подслушать каждый, кто знал, как это делается. Стало как-то более неуютно. Но меня грела мысль, что у тех, кто слушает мой трафик, чистые и благородные мотивы. Они перенастраивают на лету мои параметры управления TCP, чтобы я не «отжирал» слишком много ресурсов их драгоценной сети. Они перехватывают мой веб-трафик и обслуживают его из локального кэша лишь затем, чтобы мой браузер быстрее работал. Они прослушивают мои запросы DNS и выборочно модифицируют ответы лишь затем, чтобы защитить меня. Да, меня прослушивают, но это все для того, чтобы сделать мою жизнь лучше, быстрее, эффективнее. Как однажды заметил Хэл Вариан (Hal Varian), главный экономист Google, спам появляется лишь потому, что данные о пользователе неполны. Если бы отправитель назойливой рекламы правда знал о вас все, это был бы не спам, а дружелюбная, своевременная и очень полезная подсказка. По крайней мере, так нам говорили. Все это для того, чтобы помочь Интернету стать быстрее, полезнее и – хотя тут, надо признать, логика хромала – безопаснее.

Но однажды вся эта наивная вера в сеть рухнула, как карточный домик, под грузом всего двух слов: Эдвард Сноуден.

Из материалов, опубликованных Эдвардом Сноуденом, вырисовывался совсем другой сетевой мир: мир, насквозь пронизанный слежкой американских спецслужб. Ведь одно дело – подслушивать переговоры преступников, а совсем другое – довести слежку до таких немыслимых высот, что она превратилась в гигантскую тайную операцию, в чьи

тенета попались абсолютно все. Перед нами встал призрак «1984» Джорджа Оруэлла: казалось, что под колпаком у спецслужб вскоре окажется не только каждый человек и каждое действие, но и каждая мысль.

Неудивительно, что на волне откровений Сноудена IETF забила тревогу из-за размытия норм, призванных охранять частную жизнь каждого из нас. Цитирую RFC 7258:

«Всеобъемлющий мониторинг (Pervasive Monitoring, PM) – широко распространенное (и зачастую скрытное) наблюдение путем сбора протокольных образцов, включая содержимое данных приложений или метаданные протоколов (например, заголовки). Активное или пассивное «прослушивание» (wiretap) и анализ трафика (например, поиск корреляций и синхронизации или измерение размера пакетов) или «взлом» (subverting) криптографических ключей, применяемых для защиты протоколов, также могут быть частью всеобъемлющего мониторинга. Отличительной особенностью PM в большей степени является отсутствие избирательности и очень широкий охват, чем новые способы взлома технических средств. С технической точки зрения сообщества IETF, PM представляет собой атаку на приватность пользователей и организаций в сети Интернет».

IETF заявила, что «IETF будет стремиться к разработке спецификаций, позволяющих смягчить влияние таких атак».

Звучит грозно. Похоже, Интернет начинает закручивать вконец разболтанные гайки. Сеть, по которой передаются наши пакеты, перестала быть верным товарищем, помогающим нам общаться. Теперь ее считают опасной, ядовитой средой, которой нельзя доверять ни на йоту. А раз уж доверять ей нельзя, то, значит, не покажем врагу ни бита данных и заставим пользователей верифицировать все транзакции!

И, кажется, это мнение упало на благодатную почву. Программы, подобные Let's Encrypt, свели к нулю стоимость сертификатов открытых ключей для доменных имен. В результате безопасные веб-службы из экзотической роскоши превратились в товар, доступный каждому. А сейчас один из самых популярных браузеров в Интернете стремится объявить «небезопасными» все открытые веб-страницы (http://www.zdnet.com/article/google-tightens-noose-on-http-chrome-to-stick-not-secure-on-pages-with-search-fields/). Тот же браузер предпочитает использовать зашифрованный транспорт везде, где возможно (QUIC), пряча от сети не только полезную нагрузку, но сам транспортный протокол целиком. Похоже, что в наши дни единственный протокол, у которого есть шанс пройти по Интернету, должен быть упакован в безопасную полезную нагрузку сеанса TLS, и это не осталось незамеченным. Для начала начнем хотя бы использовать порт 443 (HTTPS). Еще лучше – станем использовать QUIC. Теперь мы не просто шифруем полезную нагрузку, но окутываем криптографической завесой все управление транспортным потоком.

Но прозвучали и голоса против. Кое-кто настолько привык к тому, что сеть делится информацией направо и налево, что стал на это полагаться. Как отмечено в статье Тони Рутковски, в наших сетях существует целый мир промежуточного ПО, которому для работы необходимо видеть пользовательский трафик, в том числе и внутри отдельных сеансов. Даже так называемые безопасные сеансы тоже уязвимы (https://blog.cloudflare.com/understanding-the-prevalence-of-web-traffic-interception/). Различные методы борьбы с DDoS-атаками на сетевом уровне опираются на способность вычленить паттерны злонамеренного или иного вредоносного трафика в сети. А многие сетевые операторы считают возможность проверять сетевой трафик чуть ли не своей прерогативой.

Такая позиция отнюдь не нова. Когда в 1872 году телеграфная линия соединила Австралию с остальным миром, стоимость телеграфного сообщения с Великобританией была заоблачно высока. За телеграмму из тридцати слов среднему человеку пришлось бы выложить трехнедельную зарплату. Неудивительно, что пресса, которая активно пользовалась телеграфом, стала использовать шифр – и чтобы сэкономить за счет большей степени сжатия, и чтобы скрыть содержание своих сообщений от конкурентов. Результат был предсказуем: австралийская телеграфная служба запретила передачу любых кодов и шифровок.

Положит ли тотальное шифрование конец всем видам кэширования контента в сети? Вряд ли. Да, сторонние кэши контента страдают от шифрования сеансов, но это не значит, что контент больше не кэшируется. Стала бурно развиваться сеть распределения контента, в которой кэши находятся под контролем издателей контента или их уполномоченных агентов. В результате пользователь получает локальную доставку контента вместе с шифрованием носителя, а впридачу еще и возможность проверки получаемого материала на подлинность.

Пожалуй, более важен другой вопрос: действительно ли повсеместное шифрование станет настоящей бедой для спецслужб? Это тоже вряд ли. Я практически не сомневаюсь, что те, у кого есть веские основания бояться подслушивания, и так все шифруют. Спецслужбы наверняка хотят получить не четкую картину действий явного врага в Интернете,

а возможность наблюдать за всей сетевой средой, собирая и вычленяя из этого огромного пула паттерны данных для последующего анализа.

В том-то и загвоздка. С одной стороны, каждому из нас нужна хоть какая-то приватность, и мы держимся за нее. Мы хотим, чтобы наши логины и пароли были в безопасности – как минимум, чтобы нас не обокрали или не подставили. Но в то же время мы хотим, чтобы государство нас защищало, в том числе и от тех, кто хочет нас обокрасть или подставить. А для этого ему нужна техническая возможность. Где же провести черту? Следует ли нам отринуть шифрование и вернуться к открытой передаче данных, чтобы насытить неутолимую жажду спецслужб знать все о каждом нашем чихе? Или постараться, чтобы наши разговоры хотя бы не лежали открыто на виду у тех, у кого есть силы и желание прослушивать сеть?

Нет сомнений, что текущая позиция технологического сообщества, выраженная IETF, очень сильно склоняется в сторону приватности. Можно ожидать дальнейшего распространения TLS, маскирующих транспортных протоколов типа QUIC, а также бешеной эскалации паранойи со стороны приложений, которые больше не доверяют сети. Ведь стоит потерять доверие – и восстановить его становится невероятно трудно. В нашем случае сеть потеряла доверие приложений, работающих с ней, и доверие пользователей, стоящих за приложениями. Мне кажется, что поздно умерять пыл, когда речь идет о масштабах шифрования на сетевом уровне – этот поезд ушел и в обозримом будущем не вернется!

Однако у меня есть подозрение, что спецслужбы уже переориентировались на другие источники. Раз уж бурный поток данных из сети обмелел и пересох, то почему бы не переключиться на данные, собранные серверами контента? Там их едва ли не больше. Если крупные фабрики контента собрали обо мне столько данных, то наверняка «те, кому надо» станут давить на них с целью эти данные заполучить. Поэтому я не тешу себя надеждами на то, что у меня теперь стало больше приватности. Скорее уж, меньше.

Короче, как поют The Who, «Meet the new boss. Same as the old boss»[1].

Оговорка

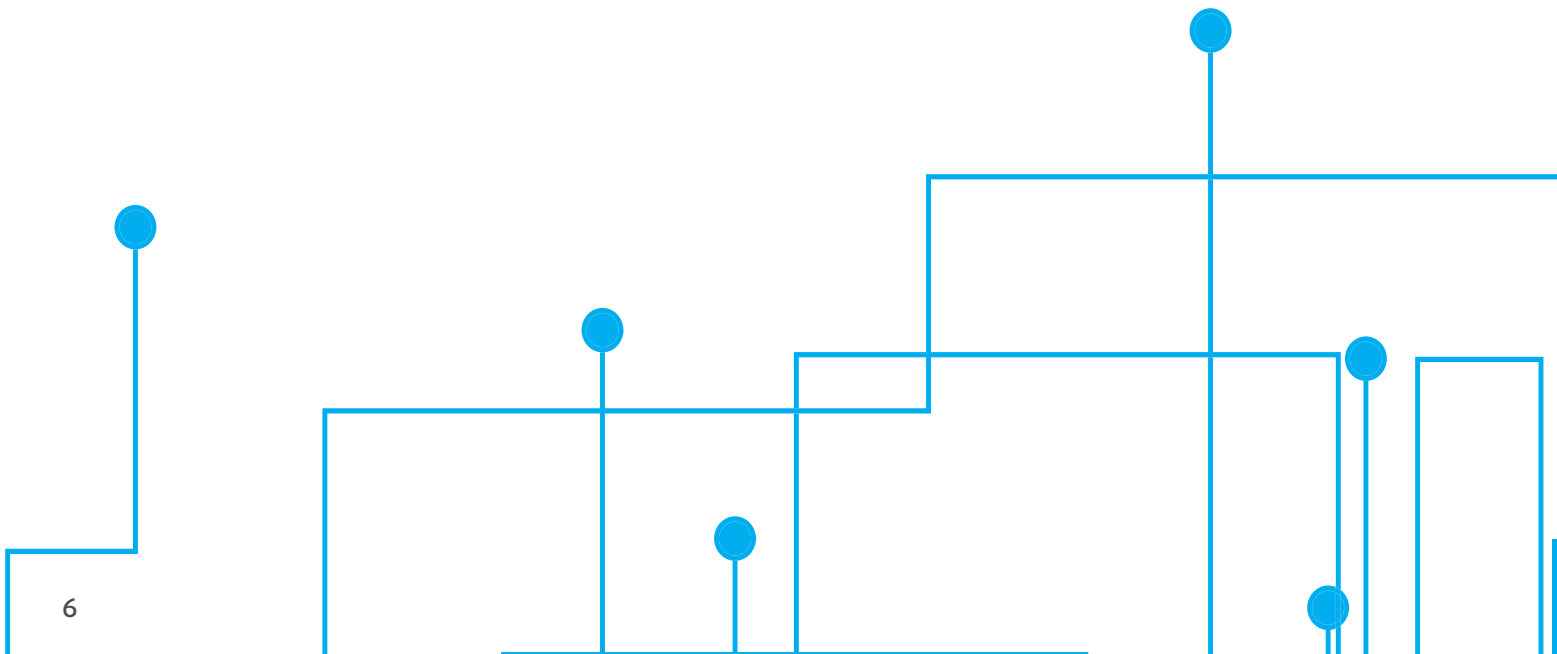
Кстати говоря, песня The Who, из которой взяты эти строки, – Won't Get Fooled Again Пита Таунсенда – впервые была записана в начале 1971 года в рамках заброшенного потом проекта LifeHouse. В апреле 1971 года ее записали снова, добавив синтезатор, и выпустили в виде сингла, а в августе того же года она вышла на альбоме Who's Next. Эта песня, которой The Who с тех пор закрывают все концерты, – практически ровесница Интернета!

Изложенные выше воззрения могут не совпадать с позицией Asia Pacific Network Information Centre.

Ссылки

1. Дословно – «Знакомьтесь, ваш новый босс. Такой же, как старый». Если искать русский аналог, то ближе всего окажется старинная пословица «Вот тебе, бабушка, и Юрьев день» – Перев.

Источник: http://www.potaroo.net/isp-col/2018-03/pe.html



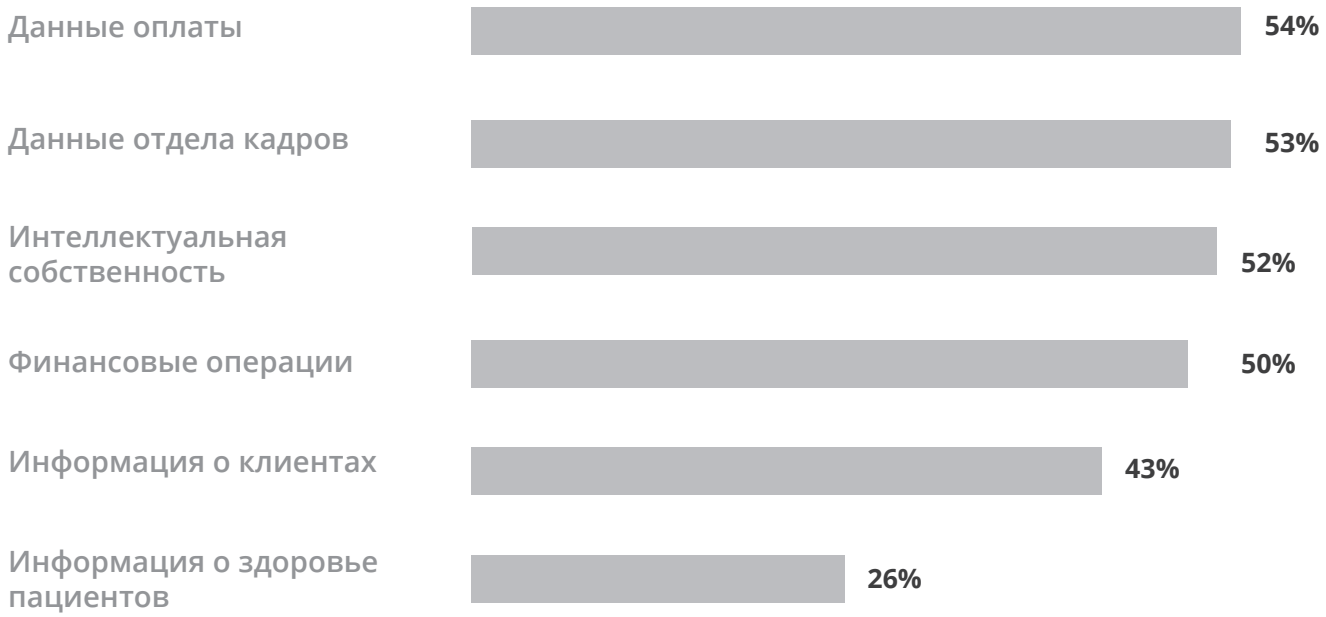
Об авторе

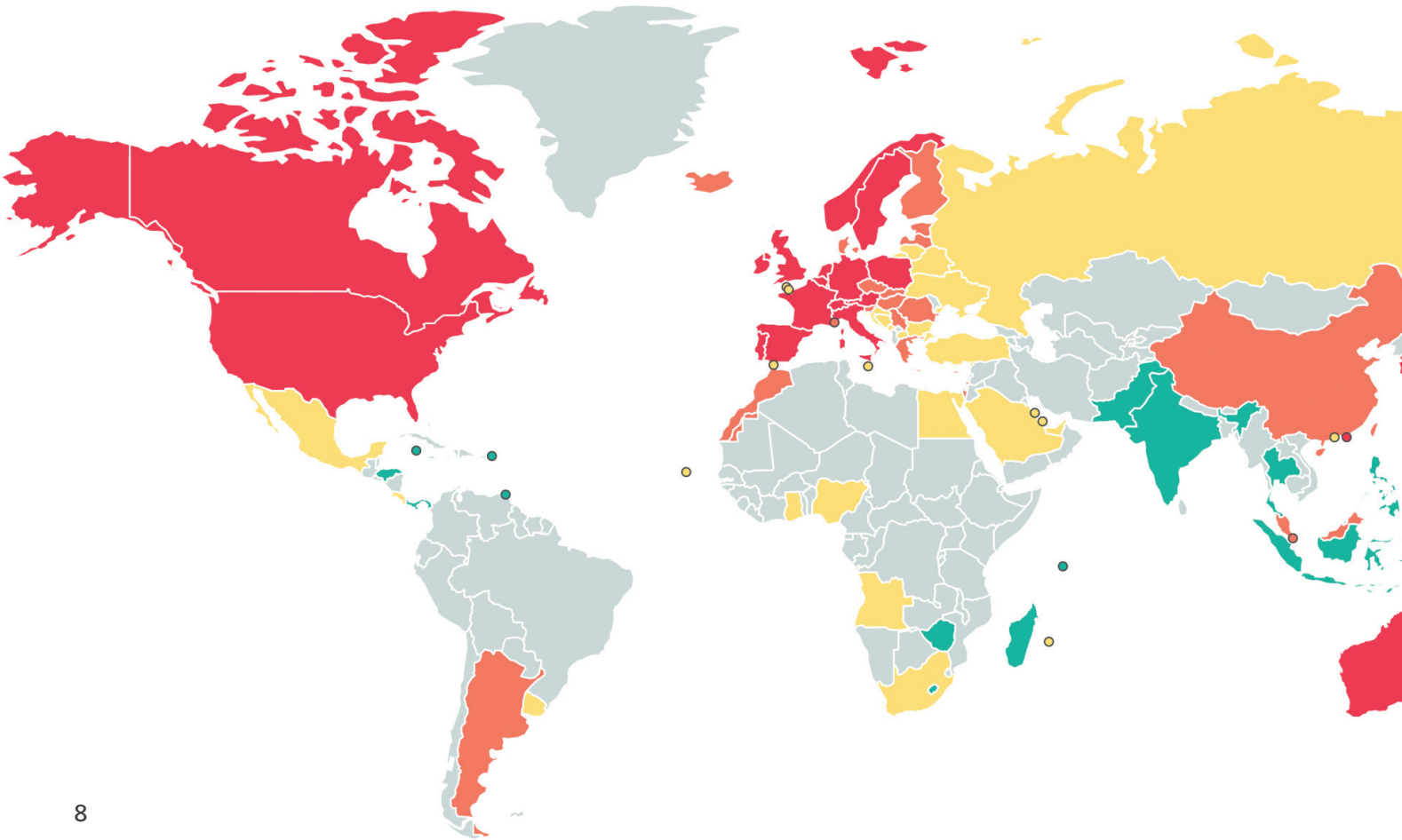
Джефф Хьюстон (Geoff Huston), B.Sc., M.Sc. – главный исследователь APNIC, региональной интернет-регистратуры, обслуживающего Азиатско-Тихоокеанский регион.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

КАКИЕ ДАННЫЕ ШИФРУЮТ ОРГАНИЗАЦИИ

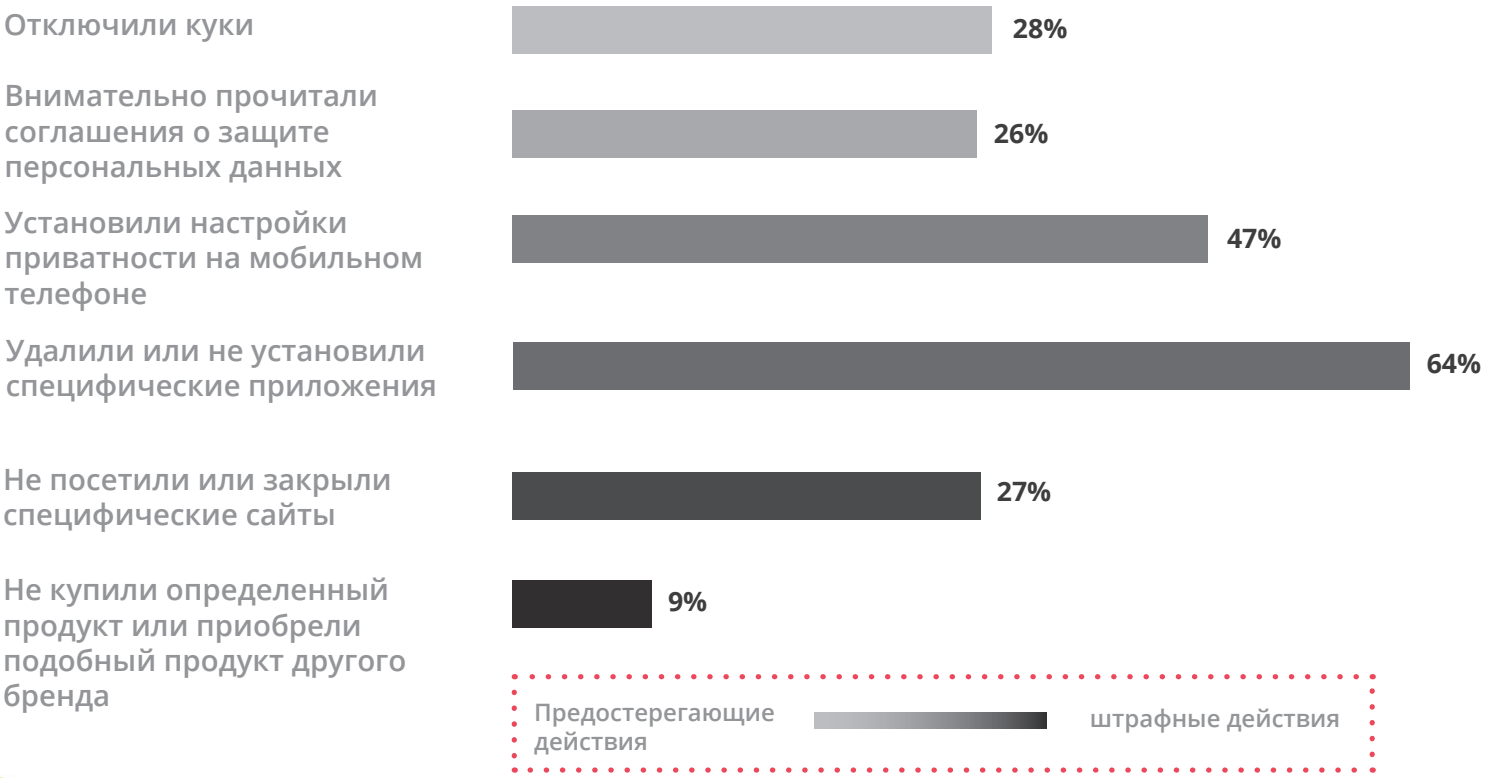
Источник: Ponemon Institute, GLOBAL ENCRYPTION TRENDS STUDY

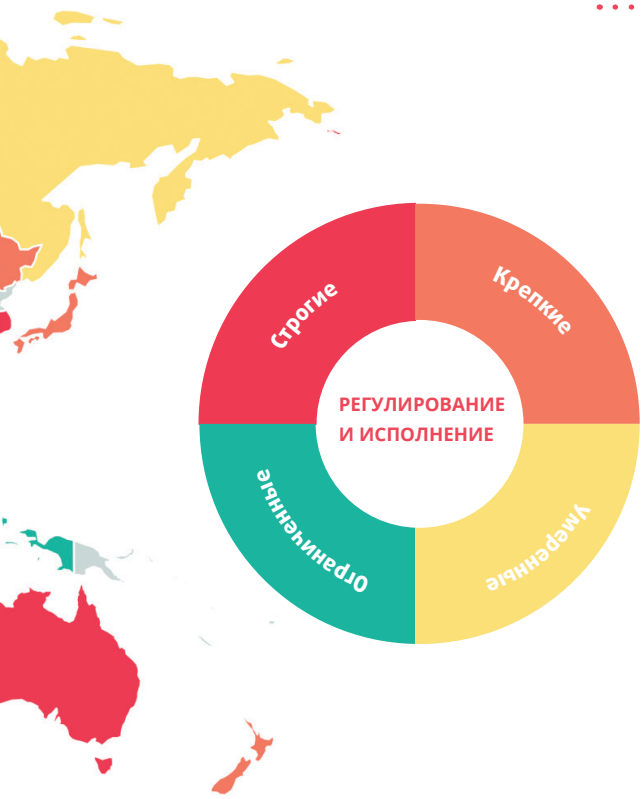




ПРОЦЕНТ АМЕРИКАНСКИХ РЕСПОДЕНТОВ, ПРИНЯВШИХ МЕРЫ В ПРОШЕДШИЕ 12 МЕСЯЦЕВ ИЗ-ЗА ОПАСЕНИЙ ПО ПОВОДУ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ

Источник:
Delloitte/SSI 2016, customer survey





ЗАКОНЫ ЗАЩИТЫ ДАННЫХ ПО ВСЕМУ МИРУ

Источник:
DLA PIPER, Data protection laws

Всеобъемлющая безопасность электронной почты в Интернете

Уильям Стеллингс (William Stallings), независимый консультант

Электронной почтой пользуются повсеместно и организации, и частные лица. При этом сама электронная почта уязвима к целому ряду угроз безопасности. Угрозы безопасности электронной почты можно весьма общо разбить на следующие категории:

- *Угрозы аутентичности*: могут привести к несанкционированному доступу к корпоративной системе электронной почты. Сюда же относится обман адресата, т.е. ситуация, когда отправитель письма выдает себя за другого.
- *Угрозы целостности*: могут привести к несанкционированному изменению содержимого электронного письма.
- *Угрозы конфиденциальности*: могут привести к несанкционированному разглашению конфиденциальной информации.
- *Угрозы доступности*: могут перекрыть конечным пользователям возможность получать или отправлять электронную почту.

Для содействия борьбе с этими категориями угроз *Национальный институт стандартов и технологии* (National Institute of Standards and Technology, NIST) опубликовал документ SP 800-177[1], в котором содержатся рекомендации по укреплению доверия к электронной почте. Этот документ представляет собой одновременно обзор имеющихся стандартизованных протоколов и набор рекомендаций по использованию этих протоколов для того, чтобы противостоять угрозам безопасности электронной почты.

Для лучшего понимания тем, излагаемых в настоящей статье, целесообразно иметь общее представление об архитектуре электронной почты в Интернете. В настоящее время она определяется стандартом RFC 5598[2]. Начнем с обзора основных концепций.

На самом фундаментальном уровне архитектура электронной почты в Интернете состоит из «мира пользователей» в виде *почтовых агентов* (Message User Agent, MUA) и «мира передачи» в виде *службы обработки сообщений* (Message Handling Service, MHS), состоящей из *агентов пересылки сообщений* (Message Transfer Agent, MTA). MHS получает сообщение от пользователя и доставляет его одному или нескольким другим пользователям, создавая виртуальную среду обмена данными MUA-MUA. Эта архитектура включает в себя три типа взаимодействия. Первое – непосредственно между пользователями: MUA должен форматировать сообщения от имени автора так, чтобы MUA получателя мог показать их адресату в читабельном виде. Также требуется взаимодействие между MUA и MHS – сначала тогда, когда MUA передает сообщение MHS, а потом когда MHS доставляет его MUA получателя. Также требуется взаимодействие между компонентами MTA по пути передачи сообщения по MHS.

На рис. 1 показаны основные компоненты почтовой архитектуры Интернета, в том числе следующие:

- *Почтовый агент* (MUA): работает от имени пользователей и приложений пользователей. Является их представителем в почтовом сервисе. Как правило, эта функция расположена на компьютере пользователя и называется почтовым *клиентом* – либо в локальной сети и называется локальным почтовым *сервером*. MUA автора форматирует сообщение и выполняет первоначальную передачу его в MHS посредством *агента отправки почты* (Mail Submission Agent, MSA). MUA получателя получает почту для хранения или показа пользователю-адресату.
- *Агент отправки почты* (MSA): получает сообщение, отправленное MUA, и применяет политики хостингового домена и требования стандартов Интернета. Эта функция может располагаться вместе с MUA или быть реализована в качестве отдельной функциональной модели. В последнем случае для передачи данных между MUA и MSA используется протокол SMTP.
- *Агент пересылки сообщений* (MTA): передает сообщения на следующий узел почтовой системы. Он похож на коммутатор пакетов или IP-маршрутизатор, в том смысле, что его задача – осуществлять оценку маршрутизации и передавать сообщения ближе к адресату. Несколько MTA последовательно пересылают сообщение, пока оно не достигнет нужного MDA. Кроме того, MTA дописывает в заголовок сообщения информацию о трассировке. Для обмена данными между разными MTA, а также между MTA и MSA/MDA, используется протокол SMTP.
- *Агент доставки почты* (Mail Delivery Agent, MDA): MDA отвечает за передачу сообщений от MHS в *хранилище сообщений* (Message Store, MS).

- *Хранилище сообщений* (MS): MUA может использовать долгосрочный MS. MS может располагаться на удаленном сервере или же на той же самой машине, что и MUA. Как правило, MUA извлекает сообщения с удаленного сервера с помощью протокола *POP* (Post Office Protocol) или *IMAP* (Internet Message Access Protocol).

Как мы скоро увидим, важным элементом обеспечения безопасности почты является *шифрование с открытым ключом*. В свою очередь, использование шифрования с открытым ключом зависит от использования *сертификатов открытого ключа*. В сущности, сертификат открытого ключа состоит из а) самого открытого ключа и б) идентификатора пользователя, принадлежащего владельцу ключа, а весь блок подписывается доверенной третьей стороной. Обычно открытые ключи создаются и используются с помощью такого третьего лица, как *центр сертификации* (Certificate Authority, CA). CA – это организация, пользующаяся доверием сообщества пользователей, например, государственное или финансовое учреждение. Перечислим основные элементы в схеме CA:

1. Клиентское ПО создает пару ключей: один открытый и один закрытый. Клиент подготавливает неподписанный сертификат, в который входят ID пользователя и его открытый ключ. Затем клиент отправляет неподписанный сертификат безопасным способом в CA.

2. CA генерирует подпись, вычислив хэш-сумму неподписанного сертификата и зашифровав хэш закрытым ключом CA; зашифрованный хэш называется подписью, или сигнатурой (signature). CA дописывает полученную подпись к неподписанному сертификату, а затем отправляет подписанный таким образом сертификат клиенту.

3. Клиент может отправить свой подписанный сертификат любому другому пользователю. Этот пользователь может проверить действительность сертификата, вычислив его хэш (без подписи), расшифровав подпись с помощью открытого ключа CA и сравнив хэш с расшифрованной подписью.

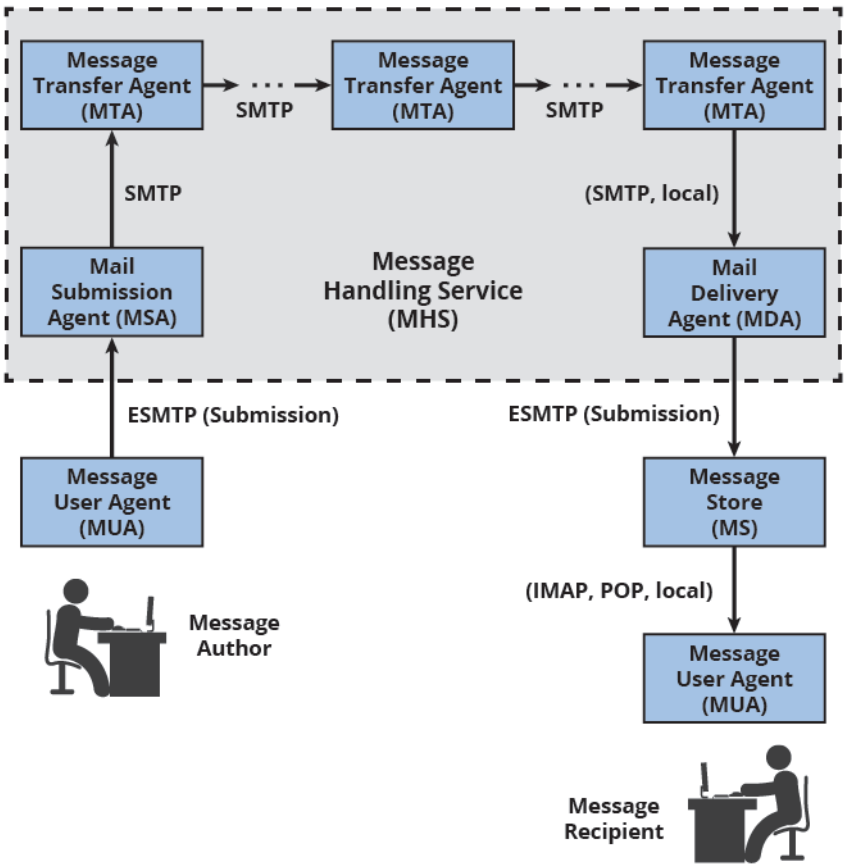
Если все пользователи подписывают свои сертификаты в одном и том же CA, это означает, что такой CA пользуется общим доверием. Все сертификаты пользователей можно поместить в каталог для доступа всем пользователям. Кроме того, пользователи могут напрямую передавать свои сертификаты друг другу. В любом случае, когда пользователь B получает сертификат пользователя A, то B убежден, что сообщения, которые он подпишет открытым ключом A, будут защищены от прослушивания и что сообщения, подписанные закрытым ключом A, будет невозможно подделать.

Если сообщество пользователей достаточно велико, работать всем с одним и тем же CA может быть нецелесообразно. Дело в том, что поскольку все сертификаты подписаны тем же самым CA, то у каждого пользователя-участника должна быть копия открытого ключа самого CA – она нужна ему для проверки подписей. И такой открытый ключ должен быть передан каждому пользователю абсолютно безопасным способом (в отношении целостности и аутентичности), чтобы пользователь доверял сертификатам этого CA.

Получается, что когда пользователей достаточно много, имеет смысл завести несколько CA, каждый из которых рассылал бы свой открытый ключ той или иной части пользователей. На практике существует не один CA, а целая иерархия. Такая система усложняет вопросы рассылки ключей и доверия, но основные принципы остаются теми же самыми.

Следует упомянуть ряд проблем, связанных с CA. Как можно понять из предыдущего абзаца, иерархическая структура CA может стать неуклюжей и плохо масштабироваться. Тем не менее, эта структура до сих пор является предпочтительной и рекомендуется стандартом SP 800-177. Также есть отдельный вопрос безопасности.

Рис. 1. Функциональные модули и стандартные протоколы в почтовой архитектуре Интернета.



Глобальная система CA в последние годы становилась мишенью для атак, среди которых было и несколько успешных. Один из способов защитить CA от компрометации – это использование *системы имен доменов* (DNS), чтобы домены могли выбирать для себя желательные сертификационные CA или вендоров CA. А такое использование DNS требует, чтобы сама DNS была защищена с помощью *DNSSEC* (Domain Name System Security Extensions), как описано ниже.

Пользователи, не знакомые с криптографией открытого ключа, концепциями аутентификации и цифровых подписей – либо желающие освежить свои знания по этому вопросу, – могут ознакомиться с информационным документом *Crypto Portal*[3], содержащим краткое и простое изложение темы. Полезный обзор концепций CA и сертификата открытого ключа содержится в NIST SP 800-32[4].

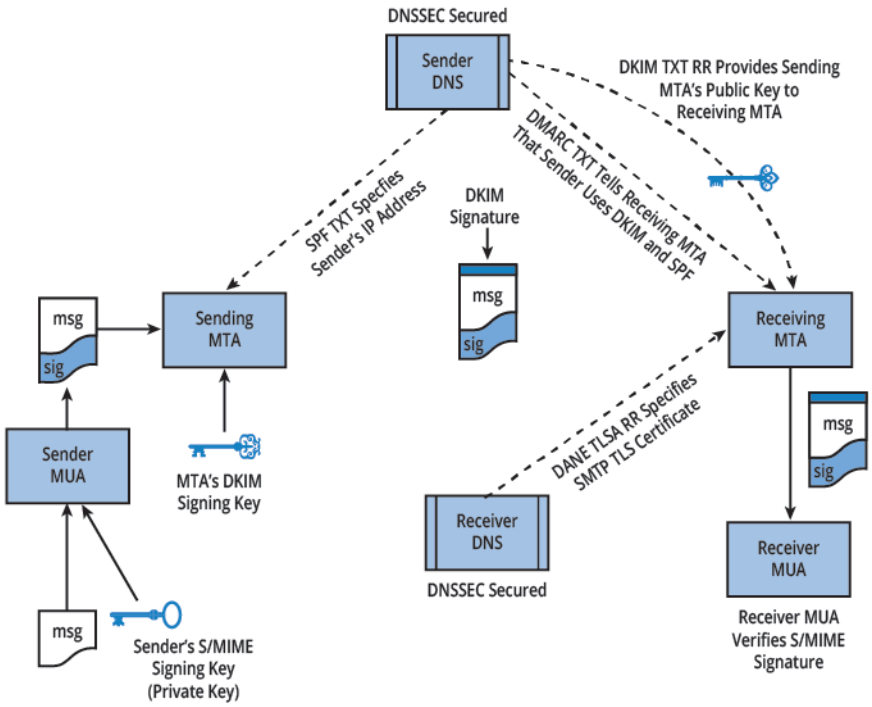
Доверенная электронная почта

В SP 800-177 описаны и рекомендованы следующие протоколы и стандарты:

- *STARTTLS*: расширение безопасности SMTP, позволяющее клиенту и серверу SMTP договориться об использовании TLS (Transport Layer Security) для того, чтобы наладить закрытый обмен данными с аутентификацией по Интернету.
- *S/MIME (Secure Multipurpose Internet Mail Extensions)*: обеспечивают аутентификацию, целостность, невозможность отказа (nonrepudiation, посредством цифровых подписей) и конфиденциальность (посредством шифрования) сообщений SMTP.
- *DANE (DNS-Based Authentication of Named Entities)*: предназначен для исправления недостатков системы *центров сертификации* (CA) за счет создания альтернативного канала аутентификации открытых ключей на основе DNSSEC. В результате те же самые отношения доверия, которые используются для сертификации IP-адресов, используются для сертификации серверов, работающих по этим адресам.
- *SPF (Sender Policy Framework)*: позволяет владельцу домена указать IP-адреса MTA, уполномоченных отправлять почту от имени домена. SPF использует DNS для того, чтобы владельцы доменов могли создавать записи, связывающие доменное имя с конкретным диапазоном IP-адресов или уполномоченных MTA. Получатель просто сличает *текстовую запись* SPF (TXT) в DNS, чтобы проверить, имеет ли право предполагаемый отправитель сообщения использовать такой исходный адрес. Почта, поступающая не с уполномоченных IP-адресов, отбрасывается.
- *DKIM (DomainKeys Identified Mail)*: позволяет «акторам» электронной почты (авторам или операторам) надежно приписать к сообщению свое доменное имя с помощью криптографических методов, чтобы механизмы фильтрации могли выработать точную репутацию домена. MTA могут подписывать выбранные заголовки и тело сообщения. Такая подпись подтверждает исходный домен письма и обеспечивает целостность тела сообщения.
- *DMARC (Domain-based Message Authentication, Reporting, and Conformance)*: публикует требование того, чтобы доменное имя автора было аутентифицировано по DKIM и/или SPF, чтобы владелец домена затребовал от получателя обработку неаутентифицированной почты с помощью этого домена, а также механизм отчетности для отправки отчетов от получателей владельцам доменов. DMARC сообщает отправителям о пропорциональной эффективности их политик SPF и DKIM, а также сигнализирует получателям, какие действия нужно предпринять в различных ситуациях индивидуальных и массовых атак.

На рис. 2 показано, как эти компоненты взаимодействуют между собой, обеспечивая аутентичность и целостность сообщения. Для простоты не показано, что S/MIME также

Рис. 2. Взаимосвязь DNSSEC, SPF, DKIM, DMARC, DANE и S/MIME для обеспечения аутентичности и целостности сообщений.



DANE = DNS-based Authentication of Named Entities
DKIM = DomainKeys Identified Mail
DMARC = Domain-based Message Authentication, Reporting, and Conformance
DNSSEC = Domain Name System Security Extensions
SPF = Sender Policy Framework
S/MIME = Secure Multi-Purpose Internet Mail Extensions
TLSA RR = Resource Record

обеспечивает конфиденциальность сообщений путем их шифрования. Вместе эти протоколы обеспечивают всеобъемлющую стратегию безопасности электронной почты в Интернете. В этой статье мы приведем обзоры каждого из них.

STARTTLS:

Существенным обновлением безопасности SMTP стал STARTTLS, определенный в RFC 3207[5]. STARTTLS позволяет добавить к обмену данными между агентами SMTP конфиденциальность и аутентификацию. Благодаря этому агенты SMTP могут защитить часть своей коммуникации или всю ее от прослушивания и атак, установив сеанс TLS (Transport Layer Security) в рамках соединения SMTP. STARTTLS широко используется. Его поддерживают Amazon, Facebook, Google, Microsoft, Yahoo и другие[6]. В 2014 Facebook (которая ежедневно рассылает миллиарды почтовых сообщений) провела исследование, обнаружившее, что 76% имен хостов, получающих почту от Facebook, поддерживают STARTTLS[7].

TLS – это уровень безопасности, реализуемый прямо поверх TCP. TLS – это стандарт Интернета, пришедший на замену *Secure Sockets Layer* (SSL) и обладающий практически тем же функционалом[8]. При использовании TLS у приложения есть *адрес сокета* TLS и оно взаимодействует с сокетом адреса TLS у удаленного приложения. Эти адреса отличаются от адресов, используемых теми же приложениями при работе непосредственно поверх TCP. Функции безопасности TLS прозрачны для приложения и для TCP. Поэтому ни TCP, ни приложение не нужно модифицировать для внедрения функций безопасности SSL. TLS обеспечивает три категории: безопасность, конфиденциальность и аутентификацию.

Если клиент не начинает соединение через порт с поддержкой TLS, сервер может ответить сообщением, указывающим, что возможен вариант STARTTLS.

Тогда клиент может отдать команду STARTTLS в потоке команд SMTP, и обе стороны установят безопасное подключение TLS. STARTTLS сейчас работает у многих поставщиков услуг электронной почты и на многих почтовых серверах[9, 10], включая Amazon, Comcast, Dropbox, Facebook, Google, Microsoft и Yahoo.

Как описано в SP 800-177, STARTTLS может быть уязвим к атакам типа «промежуточное звено» или MITM (*Man-In-The-Middle*), когда инициируется по запросу сервера. В этом случае «промежуточное звено» получает запрос STARTTLS с сервера в ответ на запрос соединения и вычеркивает его.

Запросивший клиент не видит запрос о переходе на TLS и продолжает работать с незащищенным соединением. Однако авторы SP 800-177 решили, что какая-то защита лучше, чем никакой, а потому до тех пор, пока TLS не станет повсеместным и не будет активироваться автоматически, серверы с поддержкой TLS должны предлагать клиентам применить команду STARTTLS. Клиенты TLS должны пытаться либо сразу использовать STARTTLS, либо отдать эту команду по запросу.

S/MIME

Secure/Multipurpose Internet Mail Extension (S/MIME) – это безопасное дополнение к интернет-стандарту электронной почты MIME[11]. S/MIME – это комплексная функция, определенная во многих документах. Наиболее важные документы, описывающие S/MIME, включают следующие[12–19]:

- *RFC 5750, S/MIME Version 3.2 Certificate Handling*: описывает соглашения по использованию сертификата X.509 в S/MIME v3.2.
- *RFC 5751, S/MIME Version 3.2 Message Specification*: основной определяющий документ для создания и обработки сообщений S/MIME.
- *RFC 4134, Examples of S/MIME Messages*: примеры тел сообщений, отформатированных с использованием S/MIME.
- *RFC 2634, Enhanced Security Services for S/MIME*: описывает четыре дополнительных расширения безопасности для S/MIME.
- *RFC 5652, Cryptographic Message Syntax (CMS)*: описывает CMS. Этот синтаксис служит для цифрового подписания, генерации дайджеста, аутентификации и шифрования произвольного содержимого сообщений.
- *RFC 3370, CMS Algorithms*: описывает соглашения по использованию нескольких криптографических алгоритмов с CMS.
- *RFC 5752, Multiple Signatures in CMS*: описывает использование нескольких параллельных подписей в сообщении.
- *RFC 1847, Security Multiparts for MIME — Multipart/Signed and Multipart/Encrypted*: описывает систему, в рамках которой можно применять службы безопасности к частям тел сообщений MIME. Использование цифровых подписей важно для S/MIME, как мы покажем ниже.

Функционал S/MIME встроен в большинство современных почтовых программ и средств взаимодействия между ними. S/MIME реализует четыре службы для почты: аутентификацию, конфиденциальность, сжатие и совместимость почты.

Аутентификация осуществляется с помощью цифровой подписи. Обычно это RSA с SHA-256. Последовательность следующая:

1. Отправитель создает сообщение.
2. С помощью SHA-256 генерируется 256-разрядный дайджест сообщения.
3. Дайджест шифруется по RSA закрытым ключом отправителя, результат приписывается к сообщению. Также к нему приписывается идентификационная информация подписавшего, которая позволит получателю извлечь нужный открытый ключ.
4. Получатель расшифровывает и восстанавливает

дайджест сообщения по RSA с помощью открытого ключа отправителя.

5. Получатель генерирует новый дайджест сообщения и сравнивает его с расшифрованным хэшем. Если они совпадают, сообщение признается подлинным.

Комбинация SHA-256 и RSA дает эффективную схему применения цифровой подписи. Поскольку RSA – очень сильный алгоритм, получатель может быть уверен, что цифровая подпись могла быть создана только обладателем парного закрытого ключа. А благодаря применению мощного SHA-256 получатель может быть уверен, что никто больше не смог бы создать новое сообщение, которое совпадает с хэшем, а следовательно, с подписью исходного сообщения.

Хотя цифровые подписи обычно хранятся приписанными к сообщению или файлу, подписанному ими, это не всегда так: поддерживаются и отдельные подписи. Отдельная подпись (detached signature) может храниться и передаваться отдельно от подписанного ею сообщения. Этот вариант полезен в целом ряде ситуаций. Например, пользователь может вести отдельный журнал подписей всех отправленных или полученных сообщений. Другое соображение – отдельная подпись исполняемой программы может обнаруживать последующее заражение вирусом. И, наконец, отдельные подписи можно использовать в случае, когда документ (например, юридический контракт) должны подписать несколько сторон. Подпись каждого лица независима и потому применяется только к документу. В противном случае пришлось бы вкладывать подписи, как матрешки: второе лицо подписывало бы и документ, и подпись первого, и так далее.

S/MIME обеспечивает *конфиденциальность* путем шифрования сообщений секретным ключом, известным также как *симметричный ключ* (symmetric key). Чаще всего используется AES (Advanced Encryption Standard) со 128-разрядным ключом в режиме CBC (Cipher Block Chaining). Сам ключ также зашифрован, обычно по RSA, как объясняется ниже.

Как всегда, нужно решить проблему рассылки ключей. В S/MIME каждый симметричный ключ, называемый *ключом шифрования контента* (content-encryption key), используется только один раз. Это значит, что для каждого нового сообщения генерируется новый случайный ключ. Поскольку ключ шифрования контента одноразовый, он привязан к сообщению и передается вместе с ним. Для защиты ключа он зашифровывается открытым ключом получателя.

Последовательность действий выглядит так:

1. Отправитель генерирует сообщение и случайное 128-разрядное число, которое станет ключом шифрования контента для этого сообщения и только для него.

2. Сообщение зашифровывается сгенерированным ключом шифрования контента.

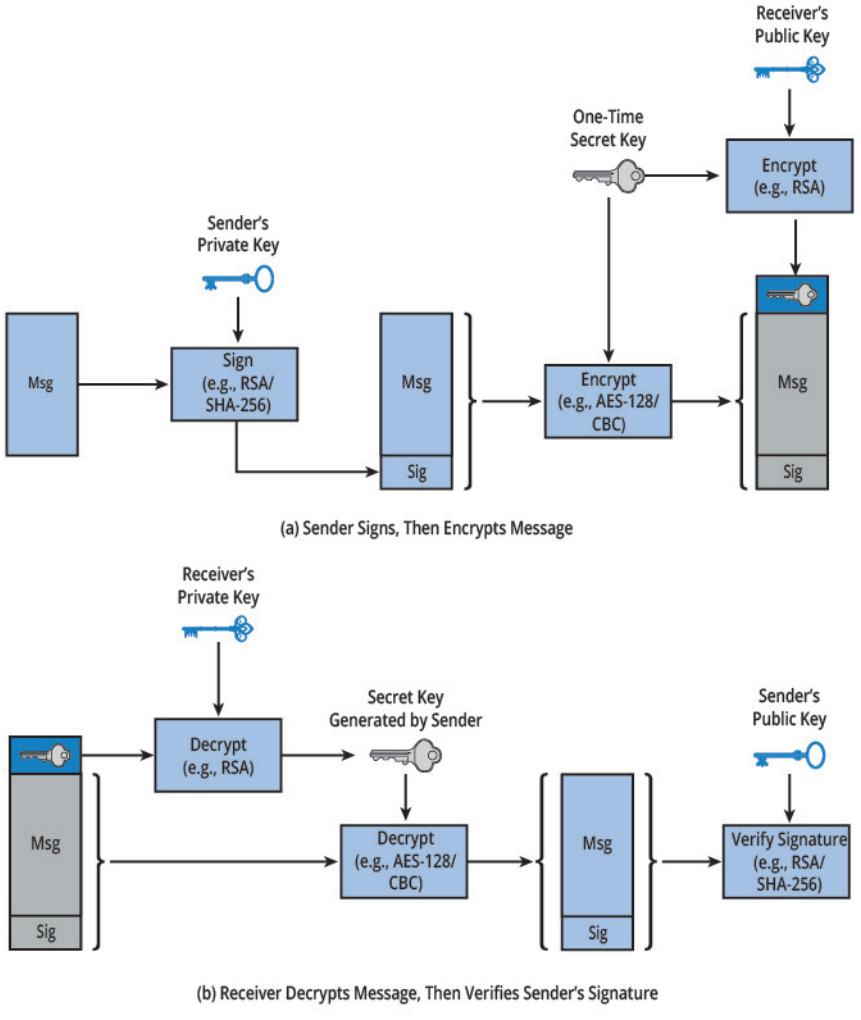
3. Ключ шифрования контента шифруется по RSA открытым ключом получателя, результат приписывается к сообщению.

4. Получатель расшифровывает и восстанавливает ключ шифрования контента по RSA собственным закрытым ключом.

5. Сообщение расшифровывается ключом шифрования контента.

Как видно на рисунке 3, для одного и того же сообщения

Рис. 3. Упрощенная функциональная схема S/MIME.



реализуются и конфиденциальность, и шифрование. На рисунке показана последовательность, в которой для простого текстового сообщения генерируется подпись и добавляется к сообщению. Затем и текстовое сообщение, и подпись зашифровываются единым блоком с помощью симметричного шифрования, а ключ симметричного шифрования зашифровывается открытым ключом.

В S/MIME операции подписания и шифрования сообщения могут выполняться в любом порядке. Если сообщение сначала подписывается, идентичность отправителя оказывается скрыта шифрованием. Кроме того, обычно гораздо удобнее хранить подпись с текстовой версией сообщения. Также, для целей верификации третьими сторонами, если сначала выполняется подписание, то третьей стороне не нужно возиться с симметричным ключом во время проверки подписи.

Если же сначала выполняется шифрование, можно проверить подпись, не раскрывая содержание сообщения. Этот вариант может быть полезен в ситуациях, когда требуется автоматическая проверка подписи и для такой проверки не нужен открытый ключ. Однако в этом случае получатель не может установить, есть ли связь между подписавшим сообщение и незашифрованным содержимым письма.

При использовании S/MIME хотя бы часть передаваемого блока зашифрована. Если используется только служба подписи, то шифруется дайджест сообщения (закрытым ключом отправителя). Если используется служба конфиденциальности, то шифруется и сообщение, и подпись (если есть) - разовым симметричным ключом. Поэтому часть всего получившегося блока состоит из потока произвольных 8-разрядных октетов. Однако многие системы электронной почты могут работать только с блоками, содержащими текст в кодировке ASCII. Для *совместимости* S/MIME содержи службу, которая преобразует сырой 8-битовый двоичный поток в поток печатаемых символов ASCII. Этот процесс называется 7-битной кодировкой (7-bit encoding). Для этой цели, как правило, используется преобразование Base64. Каждая группа из трех октетов двоичных данных преобразуется в четыре символа ASCII.

S/MIME также может выполнять *сжатие* сообщения. Сжатие позволяет сэкономить место и при передаче почты, и при хранении файлов. Сжатие можно применять в любой момент относительно подписания и шифрования.

RFC 5751 содержит следующие директивы:

- Сжатие зашифрованных данных в двоичной кодировке не рекомендуется, поскольку большого эффекта не даст. В то же время данные в кодировке Base64 сжимаются прекрасно.

- Если используется алгоритм сжатия данных с потерями, а также подписание, то сначала следует сжимать, а потом подписывать.

SP 800-177 рекомендует использовать аутентификацию по цепочке сертификатов от известного центра сертификации. Кроме того, в SP 800-177 сказано, что пользователи, которым требуется больше уверенности в том, что предоставленный открытый ключ соответствует домену отправителя, могут использовать механизм DANE-S/MIME[20], при котором можно независимо извлечь сертификат и ключ из DNS и выполнить их аутентификацию по описанному ниже алгоритму DANE.

Кроме того, в SP 800-177 отмечается, что MUA обычно используют закрытые ключи S/MIME для расшифровки почтового сообщения при каждом его показе, но в хранилище сообщение хранится зашифрованным. Такой режим не рекомендуется, так как получатели зашифрованных сообщений вынуждены бессрочно хранить свой закрытый ключ. Более разумно расшифровывать сообщения до отправки на хранение. При этом само хранилище целесообразно защитить с помощью адекватных криптографических методов (например, шифрования диска), что даст защиту как для зашифрованной, так и для незашифрованной почты.

OpenPGP

PGP (Pretty Good Privacy) был разработан Филом Зиммерманом (Phil Zimmermann) в качестве общедоступного бесплатного (freeware) пакета, который позволил бы частным лицам безопасно обмениваться почтовыми сообщениями, не вверяя их защиту никаким организациям. Работы по разработке стандартов Интернета для PGP начались очень давно[21], приведя в конце концов к появлению *OpenPGP*. OpenPGP[22, 23] – это проект стандарта Интернета, который обеспечивал бы аутентификацию и конфиденциальность электронной почты. По назначению и функционалу он близок к S/MIME, но использует другие форматы сообщений и ключей, а также другой подход к созданию и применению сертификатов. В SP 800-177 перечислено множество проблем OpenPGP, в том числе неудобство пользования, плохая масштабируемость при рассылке ключей и отсутствие аутентификации владельцев ключей. Подробно этот вопрос обсуждается в [24] и [25]. Соответственно, авторы SP 800-177 рекомендуют использовать только S/MIME, а от OpenPGP отказаться.

DNS и DNSSEC

В этом разделе мы приведем краткий обзор DNS и DNSSEC, понимание которых нам понадобится в следующих разделах. *Система доменных имен* (Domain Name System, DNS) – это служба поиска в каталогах, которая устанавливает соответствие между именем хоста в Интернете и его цифровым IP-адресом. DNS состоит из четырех элементов. Пространство доменных имен имеет древовидную структуру и служит для идентификации ресурсов в Интернете. База данных DNS – это набор записей о ресурсах, собранный в распределенную БД; по идее, каждый узел и каждый лист в дереве пространства имен служит именем для набора данных (например, IP-адрес и сервер имен для данного доменного имени), который хранится в *записях ресурсов* (Resource Record, RR). *Серверы имен* – это серверные программы, которые содержат информацию о части древовидной структуры доменных имен и связанных RR. *Резолверы* (Resolver) – это программы, извлекающие информацию из серверов имен в ответ на запросы клиентов. Типовой запрос клиента выглядит как запрос IP-адреса,

соответствующего конкретному доменному имени.

База данных DNS разделена на тысячи *зон*, которые управляются отдельно и отдельными администраторами. Используя эту базу данных, серверы DNS реализуют службу каталогов «имя-адрес» для сетевых приложений, которым нужно найти тот или иной сервер приложений.

TLS – это уровень безопасности, реализуемый прямо поверх TCP. TLS – это стандарт Интернета, пришедший на замену Secure Sockets Layer (SSL) и обладающий практически тем же функционалом[8]. При использовании TLS у приложения есть адрес сокета TLS и оно взаимодействует с сокетом адреса TLS у удаленного приложения. Эти адреса отличаются от адресов, используемых теми же приложениями при работе непосредственно поверх TCP. Функции безопасности TLS прозрачны для приложения и для TCP. Поэтому ни TCP, ни приложение не нужно модифицировать для внедрения функций безопасности SSL. TLS обеспечивает три категории: безопасность, конфиденциальность и аутентификацию.

DNSSEC (Domain Name System Security Extensions, расширения безопасности DNS)[26] используются несколькими протоколами, обеспечивающими безопасность электронной почты. DNSSEC обеспечивают сквозную защиту благодаря использованию цифровых подписей, созданных администраторами отвечающих зон и проверенных программами-преобразователями получателя. В частности, DNSSEC устраняют необходимость доверять промежуточным серверам имен и резолверам, которые кэшируют записи DNS, поступающими от администратора отвечающей зоны до того, как они поступят к источнику запроса. DNSSEC состоят из набора новых типов записей ресурсов и ряда модификаций существующего протокола DNS.

В сущности, DNSSEC разработаны для защиты клиентов DNS от поддельных или модифицированных записей ресурсов DNS. Для такой защиты используются цифровые подписи, которые обеспечивают: (1) аутентификацию источника данных, чтобы гарантировать, что RR действительно поступила из правильного источника; и (2) проверку целостности данных, чтобы гарантировать неизменность содержимого RR. Администратор зоны DNS подписывает каждый *набор записей ресурсов* (Resource Record set или RRset) в зоне и публикует этот набор цифровых подписей, вместе с открытым ключом администратора зоны, в самом DNS.

В DNSSEC доверие к открытому ключу источника (для проверки подписей) устанавливается не путем обращения к третьей стороне или цепочке третьих сторон (как в цепочках PKI [Public-Key Infrastructure]), а благодаря тому, что оно начинается с доверенной зоны (например, корневой) и создает цепочку доверия вплоть до текущего источника ответа. Цепочка создается путем последовательных проверок подписей открытого ключа дочерней зоны своим родителем. Открытый ключ доверенной зоны называется *якорем, или точкой доверия* (trust anchor).

DANE

DANE (DNS-Based Authentication of Named Entities)[27, 28] – это протокол, который помогает доменам указать, каким сертификатам X.509 (массово используемым для TLS) следует доверять в этом домене. DANE позволяет привязывать сертификаты к именам DNS посредством DNSSEC. Этот протокол был предложен в стандарте RFC 6698[29] как метод аутентификации клиента и сервера TLS без центра сертификации (CA).

Если вкратце, DANE представляет собой альтернативный механизм безопасной рассылки информации о доменных именах с помощью DNS. В DANE определен новый тип записей DNS, который позволяет доменам подписывать заявления о том, какие объекты уполномочены представлять домен. Приложения могут либо использовать эти записи в дополнение к существующей системе CA, либо создать новую цепочку доверия, основанную на DNS.

Основанием для разработки DANE стала уязвимость центров сертификации в глобальной системе *инфраструктуры открытого ключа* (PKI). Разработчики каждого браузера и каждой операционной системы ведут свой список корневых сертификатов CA, служащих якорями доверия. Эти сертификаты называются *корневыми сертификатами* (root certificates) ПО и хранятся в его банке корневых сертификатов. Схема PKI позволяет получателю сертификата проследить его вплоть до корня. До тех пор, пока корневой сертификат остается надежным и аутентификация происходит успешно, клиент может поддерживать безопасность соединения. Но если любой центр сертификации в Интернете (а их сотни) окажется скомпрометирован, вся система может рассыпаться, как карточный домик. Хакер может получить закрытый ключ CA, получать сертификаты под фальшивым именем или добавлять фальшивые сертификаты в корневой банк. Глобальная инфраструктура PKI не имеет границ, и компрометация одного лишь центра сертификации подрывает целостность всей системы PKI. Кроме того, в некоторых CA «просто» плохо с практиками безопасности. Например, некоторые CA выдавали wildcard-сертификаты, владельцы которых имеют право выпускать субсертификаты для любого домена или объекта в любой точке земного шара.

DANE предназначен для того, чтобы отойти от системы CA

как источника безопасности и заменить ее на DNSSEC. Этот протокол хорошо описан в RFC 6698:

«Протокол DANE (DNS-Based Authentication of Named Entities) предлагает возможность использовать инфраструктуру DNSSEC для хранения и подписания ключей и сертификатов, используемых TLS. DANE задуман как предпочтительная основа для привязки открытых ключей к именам DNS, поскольку лица, поручающиеся за привязку данных открытого ключа к данным DNS, являются теми же лицами, которые отвечают за управление теми самыми именами DNS. Хотя получившаяся система и имеет некоторые оставшиеся уязвимые места с точки зрения безопасности, она ограничивает масштаб заявлений, которые может сделать любое лицо, соответственно масштабу именования, реализованному иерархией DNS. В результате DANE воплощает «принцип наименьших привилегий» в безопасности, который отсутствует в нынешней модели публичных центров сертификации».

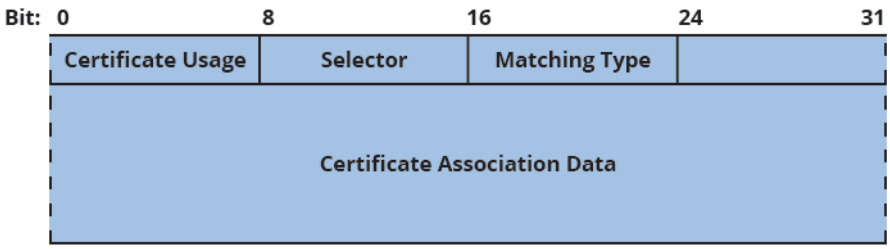
В DANE определяется новый тип записей DNS, получивший название TLSA, который может применяться как безопасный метод аутентификации сертификатов SSL/TLS. TLSA позволяет:

- указать границы того, какой CA может поручиться за сертификат или какой конкретно сертификат конечного объекта PKI валиден;
- указать, что сертификат службы или CA может быть аутентифицирован напрямую в DNS.

TLSA RR позволяет привязать выпуск и доставку сертификатов к конкретному домену. Владелец серверного домена создает запись ресурсов TLSA, которая идентифицирует сертификат и его открытый ключ. Когда клиент получает сертификат X.509 в процессе установки соединения TLS, он сверяется с TLSA RR для соответствующего домена и сопоставляет данные TLSA с сертификатом в рамках процедуры проверки сертификата на клиенте.

На рис. 4 изображен формат TLSA RR в том виде, в котором она передается запрашивающему. Она состоит из четырех полей. Поле *Certificate Usage* определяет четыре различных модели использования – для пользователей, которым требуются разные формы аутентификации. Перечислим эти модели:

Рис. 4. Формат передачи TSLA RR.



- *PKIX-TA (ограничение CA)*: указывает, каким CA можно доверять для аутентификации сертификата службы. Эта модель использования ограничивает круг CA, которые могут выпустить сертификат для данной конкретной службы на хосте. Цепочка сертификатов сервера должна пройти проверку PKIX, которая заканчивается на доверенном корневом сертификате, хранящемся на клиенте.
- *PKIX-EE (ограничение сертификатов служб)*: определяет, каким конкретно сертификатам служб оконечных объектов можно доверять для той или иной службы. Эта модель использования ограничивает круг оконечных сертификатов, которые могут использоваться для данной конкретной службы на хосте. Цепочка сертификатов сервера должна пройти проверку PKIX, которая заканчивается на доверенном корневом сертификате, хранящемся на клиенте.
- *DANE-TA (задание якоря доверия)*: указывает управляемый доменом CA, который должен служить якорем доверия. Эта модель использования позволяет администратору имен доменов указать новый якорь доверия – например, если домен выпускает собственные сертификаты силами собственного CA, который вряд ли окажется в наборе якорей доверия конечных пользователей. Цепочка сертификатов сервера самовыпускается и не должна проходить проверку на доверенном корневом сертификате, хранящемся на клиенте.
- *DANE-EE (сертификат, выданный доменом)*: указывает управляемый доменом CA, который должен служить якорем доверия. Такое использование сертификатов позволяет администратору имен доменов выпускать сертификаты для домена, не привлекая сторонний CA. Цепочка сертификатов сервера самовыпускается и не должна проходить проверку на доверенном корневом сертификате, хранящемся на клиенте.

Первые две модели использования предназначены для того, чтобы сосуществовать с публичной системой CA и усиливать ее. Последние две модели работают без публичных CA.

Поле *Selector* указывает, нужно ли сопоставлять полный сертификат или только значение открытого ключа. Сопоставление осуществляется между сертификатом, представленным в ходе переговоров TLS, и сертификатом из TLSA RR. Поле *Matching Type* указывает, как выполняется сопоставление сертификатов. Варианты следующие: полное совпадение, совпадение хэшей SHA-256 и совпадение хэшей SHA-512. *Certificate Association Data* – это сырые данные сертификата в шестнадцатеричном формате.

DANE может применяться совместно с SMTP поверх TLS, как описано в STARTTLS, чтобы полнее обеспечить безопасность доставки электронной почты. DANE может аутентифицировать сертификат

сервера отправки SMTP, с которым взаимодействует пользовательский почтовый клиент (MUA). Также он может аутентифицировать подключения TLS между серверами SMTP (MTA). Использование DANE с SMTP задокументировано в RFC 7672[30].

Как уже обсуждалось, SMTP может использовать расширение STARTTLS, чтобы выполнять SMTP поверх TLS, чтобы все почтовое сообщение плюс конверт SMTP оказались зашифрованы. Этот вариант применяется, если обе стороны поддерживают STARTTLS. Даже если для обеспечения конфиденциальности задействован TLS, он уязвим к следующим типам атак:

- хакер может отрезать объявление о поддержке TLS и заставить установить соединение без TLS;
- соединения TLS часто не аутентифицируются (например, повсеместно используются самоподписанные и несовпадающие сертификаты).

DANE может решить обе проблемы. Домен может использовать наличие TLSA RR в качестве индикатора того, что необходимо шифрование, тем самым устранив возможность злонамеренного отказа от него. Домен может аутентифицировать сертификат, используемый при настройке соединения TLS, с помощью TLSA RR, подписанной по DNSSEC.

DNSSEC может применяться совместно с S/MIME, чтобы полнее обеспечить безопасность доставки электронной почты, аналогично DANE. Такое применение задокументировано в RFC8162[21], в котором предложена новая SMIMEA DNS RR. Цель SMIMEA RR – связать сертификаты с доменными именами DNS.

Сообщения S/MIME часто содержат сертификаты, которые могут оказаться полезны при аутентификации отправителя сообщения и при шифровании ответных сообщений. Для этого требуется, чтобы получающий MUA проверял сертификат предполагаемого отправителя. SMIMEA RR могут стать безопасным методом такой проверки.

В сущности, SMIMEA RR будет иметь тот же самый формат и содержимое, что и TLSA RR, и тот же самый функционал. Разница в том, что SMIMEA RR рассчитана на потребности MUA в работе с доменными именами, указанными в почтовых адресах в теле сообщения, а не с доменными именами, значащимися во внешнем конверте SMTP.

SPF (Sender Policy Framework)

Sender Policy Framework (SPF) – это стандартный способ для домена отправителя указать список MTA, уполномоченных отправлять почту от имени домена. SPF решает следующую проблему: в нынешней инфраструктуре электронной почты любой хост может поставить любое доменное имя в любой идентификатор в заголовке письма: не требуется, чтобы хост ставил обязательно имя домена, где он сам находится.

Такая свобода самовыражения влечет за собой два больших недостатка:

- Она очень сильно мешает бороться со спамом, или, выражаясь формальным языком, *несанкционированными массовыми почтовыми рассылками* (Unsolicited Bulk E-mail или UBE). Обработчикам почты трудно отфильтровывать почту от известных источников спама.
- *Домены административного управления* (Administrative Management Domain, ADMD) закономерно озабочены простотой, с которой можно использовать чужие доменные имена, часто со злонамеренными целями.

Однако основным ограничением SPF является то, что он заставляет почту идти по определенному пути и ломается, когда легитимная почта отклоняется от этого пути – в частности, когда сообщение проходит через список рассылки.

SPF определен в RFC 7208[31]. Он представляет собой протокол, посредством которого ADMD могут уполномочивать хосты использовать свои доменные имена в полях **MAIL FROM** и **HELO**. (Следует отметить, что это доменное имя представляет собой обратный адрес для сообщений об ошибках и не обязано совпадать с адресом отправителя.) Совместимые с этим стандартом ADMD публикуют записи SPF в DNS с указанием того, каким хостам разрешается использовать доменные имена, а совместимые со стандартом получатели почты используют опубликованные записи SPF для проверки полномочий MTA-отправителей с помощью конкретного **HELO** или **MAIL FROM**.

SPF работает путем проверки IP-адреса MTA соседнего клиента выше по течению на предмет политик, закодированных в любой записи SPF, обнаруженной в домене отправителя. Домен отправителя – это домен, задействованный в соединении SMTP, а не домен, указанный в поле Author From заголовка сообщения, отображаемом в MUA. Поэтому проверки SPF можно применять до получения содержимого письма от отправителя.

На рисунке 5 приведен пример того, как можно использовать SPF. Предположим, что IP-адрес отправителя **192.168.0.1**. От MTA с доменным именем **mta.example.net** приходит сообщение. Отправитель в конверте ставит в теге

Рис. 5. Пример: заголовок конверта SMTP не совпадает с заголовком сообщения.

```
S: 220 foo.com Simple Mail Transfer Service Ready
C: HELO mta.example.net
S: 250 OK
C: MAIL FROM:<alice@example.org>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: To: bob@foo.com
C: From: alice.sender@example.net
C: Date: Today
C: Subject: Meeting Today
. . .
```

MAIL FROM значение **alice@example.org**, т.е. указывает, что сообщение исходит из домена **example.org**. Но в заголовке сообщения указано **alice.sender@example.net**. Получатель по SPF запрашивает SPF RR, соответствующую **example.org**, чтобы проверить, указан ли IP-адрес **192.168.0.1** в списке как уполномоченный отправитель, и принимает меры по результатам проверки RR.

Домен отправителя должен идентифицировать всех отправителей в данном домене и добавить эти данные в DNS в виде отдельной ресурсной записи. Затем домен отправителя кодирует соответствующую политику для каждого отправителя с помощью синтаксиса SPF. Кодирование осуществляется в записи ресурса TXT DNS в виде списка механизмов и модификаторов. Механизмы служат для определения IP-адреса или диапазона адресов, с которыми нужно выполнить сравнение, а модификаторы указывают политику для соответствующего сравнения. Синтаксис SPF довольно сложен и может выражать сложные взаимоотношения между отправителями. См. RFC 7208.

Если SPF реализован у получателя, объект SPF использует домен адресов **MAIL FROM**: и IP-адрес отправителя из конверта SMTP для опроса SPF TXT RR. Проверки SPF можно начать до получения тела письма, что может привести к блокировке передачи содержимого сообщения. Или же можно получить и буферизовать все сообщение до окончания всех проверок. В любом случае проверки должны быть завершены до того, как почтовое сообщение отправится в папку «Входящие» конечного пользователя.

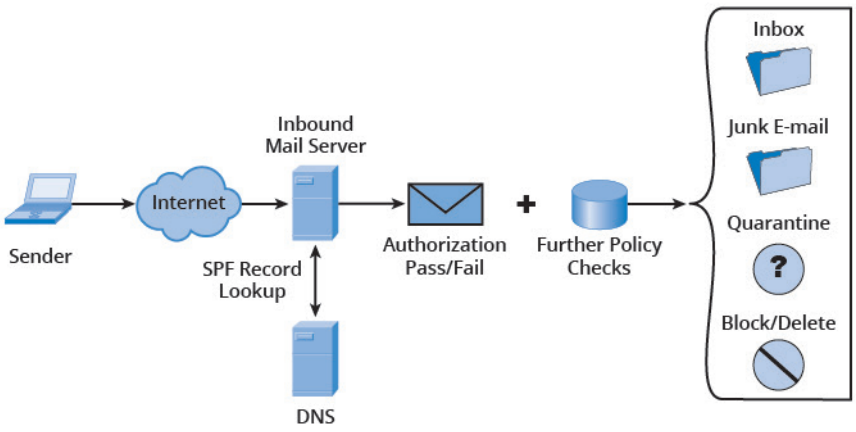
Проверка включает в себя следующие правила:

1. Если SPF TXT RR не возвращается, то по умолчанию сообщение будет принято.
2. Если SPF TXT RR содержит ошибки форматирования, то по умолчанию сообщение будет принято.
3. В противном случае судьбу сообщения определят механизмы и модификаторы в составе RR.

Если говорить об одном лишь SPF, можно спорить, правильно ли выбранное по умолчанию поведение – принять сообщение. Однако нужно иметь в виду, что SPF обычно работает вместе с целым рядом инструментов предотвращения злоупотреблений, а агрегированный механизм фильтрации обычно не принимает сообщение на основе результатов лишь одного из своих инструментов, такого как SPF.

Работа SPF проиллюстрирована на рис. 6. В 2016 году SPF был внедрен более чем в 27% всех доменов Интернета[32].

Рис. 6. Работа SPF.



DKIM

DKIM (DomainKeys Identified Mail) позволяет лицу, роли или организации, являющимися владельцами домена подписания, принять на себя некую ответственность за сообщение, связав с ним свой домен[33]. Домен может быть организацией автора сообщения, операционным реле или одним из их агентов. DKIM отделяет идентичность подписавшего сообщение от идентичности предполагаемого автора сообщения. Принятие ответственности проверяется зашифрованной подписью и прямым запросом на выдачу соответствующего открытого ключа к домену подписания.

Я неслучайно написал в начале предыдущего абзаца слово «некую». Дело в том, что текст, прямо «охваченный» подписью, не проверяется на аутентичность.

Получатели сообщения (или агенты, действующие от их имени) могут проверить подпись, напрямую запросив у домена подписания соответствующий открытый ключ, и таким образом установить, что сообщение было обработано кем-то, кто обладает закрытым ключом домена подписания. DKIM является стандартом Интернета и определен в документе RFC 6376[34]. DKIM широко используется целым рядом почтовых провайдеров, включая корпорации, госструктуры, Gmail, Yahoo и многих интернет-провайдеров (ISP). По состоянию на 2016 год DKIM, по оценке, использовался примерно на 40% сайтов в Интернете[35].

Административный блок (Administrative Unit, AU) – это часть пути почтового сообщения, которая находится под единым административным управлением. DKIM главным образом сосредоточен на хакерских атаках извне AU получателей и заявленного отправителя и борется с ними опосредованно, путем создания проверяемой подписи легитимных писем от административного блока.

В работе с такими внешними AU доверительные отношения, необходимые для отправки аутентифицированных сообщений, могут не существовать и недостаточно масштабируются для того, чтобы иметь практический смысл. В то же время при работе с такими AU имеются другие средства (такие как отправка аутентифицированных сообщений), которые легче внедряются и чаще применяются, чем DKIM. Внешние злоумышленники обычно пытаются сыграть на обезличенном характере электронной почты, благодаря которому большинство MTA получателей

принимают все поступившие письма, чтобы доставить их в свой локальный домен. Хакеры могут создавать сообщения без подписей, с неправильными подписями или же с правильными подписями, но из доменов с плохой отслеживаемостью. Они также могут выдавать свои сообщения за почтовые рассылки, поздравительные открытки или другие сообщения от легитимных агентов, которые отправляют сообщения или пересылают чужие.

DKIM предоставляет технику аутентификации электронной почты, прозрачную для конечного пользователя. В сущности, почтовое сообщение пользователя подписывается закрытым ключом административного домена, из которого исходит сообщение. Подпись охватывает все содержимое письма или же его часть, или же может вообще не охватывать его, но покрывает часть заголовков сообщения электронной почты.

Обратите внимание, что подпись используется необычно: она не удостоверяет подписанный объект. Здесь выбор того, что именно подписать, работает просто как способ приклеить фрагмент **d=domain name** ко всему сообщению способом, который трудно сымитировать. У получателя агент доставки почты может получить соответствующий открытый ключ по DNS и проверить подпись, тем самым убедившись, что сообщение поступило из заявленного административного домена. Таким образом DKIM позволяет организации поручиться за почтовое сообщение, отправленное из домена, который она не контролирует. Такой подход отличается от S/MIME, где для подписания содержимого сообщения используется закрытый ключ отправителя. Основания для DKIM базируются на следующих соображениях:

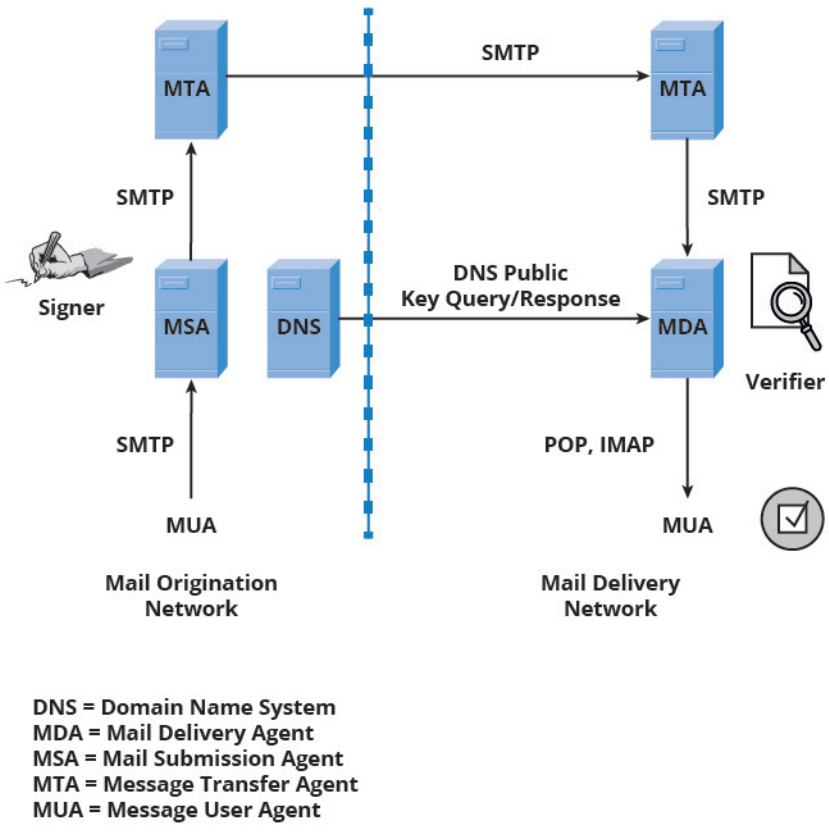
- Для работы S/MIME необходимо применение S/MIME и пользователем-отправителем, и пользователем-получателем. Почти у всех пользователей основная масса входящей почты не использует S/MIME, а основная масса почты, которую пользователь отправляет вовне, тоже предназначена лицам, не использующим S/MIME.
- S/MIME подписывает только содержимое письма. Поэтому заголовок по RFC 5322[36], описывающий источник письма, оказывается уязвимым.
- DKIM не включен в клиентские программы (MUA) и потому прозрачен для пользователя – последнему не нужно ничего делать.
- DKIM можно настроить так, чтобы он применялся ко всей почте из сотрудничающих доменов.
- DKIM позволяет добросовестному отправителю доказать, что именно он отправил данное письмо, и не допустить подделки подписи DKIM.

На рисунке 7 приведен простой пример работы DKIM. Начнем с того, что пользователь создает сообщение. Затем оно передается в *службу обработки сообщений* (MHS) и поступает в MSA, находящийся в рамках административного домена пользователя. Почтовый клиент генерирует электронное письмо.

Содержимое письма плюс избранные заголовки RFC 5322 подписываются провайдером почты с использованием закрытого ключа провайдера. Подписавший относится к какому-либо домену: это может быть корпоративная локальная сеть, ISP или открытая почтовая служба, такая как Gmail. Затем подписанное сообщение проходит по Интернету через несколько MTA. В точке назначения MDA извлекает открытый ключ поступившей подписи и проверяет ее, а затем передает сообщение почтовому клиенту получателя. По умолчанию используется алгоритм подписания RSA с SHA-256. Также можно использовать RSA с SHA-1.

На рисунке 8, взятом из RFC 5585[37], элементы работы DKIM показаны более подробно. Базовая обработка сообщений разделена между подписавшим *доменом административного управления* (ADMD) и проверяющим ADMD. В самом простом варианте эта процедура ограничивается исходным ADMD и ADMD доставки, но может включать в себя и другие ADMD по пути обработки.

Рис. 7. Простой пример внедрения DKIM.



Подписание осуществляется уполномоченным модулем в подписавшем ADMD, при этом используется закрытая информация из банка ключей. В пределах исходного ADMD подписать сообщение может MUA, MSA или MTA. Проверка тоже осуществляется уполномоченным модулем в подписавшем ADMD. Это может быть MTA, MDA или MUA в пределах ADMD получателя. Такой модуль проверяет подпись или определяет, нужна ли была такая подпись.

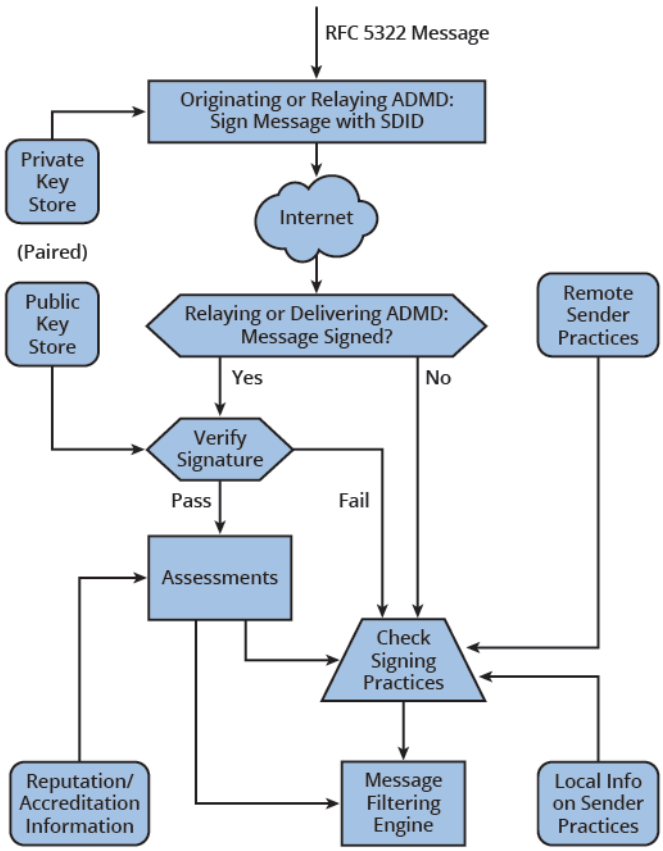
Для проверки подписи используется открытая информация из банка ключей. Если подпись проходит проверку, то выполняется оценка подписавшего по репутационной информации и такая информация передается в систему фильтрации сообщений.

Если подпись не проходит проверку либо подписи, использующей домен автора, просто нет, то можно извлечь (удаленно и/или локально) сведения о том, какая практика подписания действует для такого автора, и передать ее в систему фильтрации сообщений. Например, если отправитель (допустим, Gmail) использует DKIM, но подпись DKIM отсутствует, то сообщение считается злонамеренным.

Подпись вставляется в сообщение RFC 5322 в виде дополнительного поля в заголовке, начиная с ключевого слова Dkim-Signature. Вы можете увидеть примеры в собственном почтовом ящике, выбрав параметр View Long Headers (или похожий) для полученного письма.

Перед подписанием сообщения выполняется процедура,

Рис. 8. Функциональная схема DKIM.



называемая *каноникализацией* или *нормализацией* (canonicalization) (у этого термина встречается и перевод «канонизация», но я поостерегусь причислять электронную почту к лику святых – перев.) заголовка и тела сообщения RFC 5322. Нормализация необходима для того, чтобы сообщение могло «пережить» возможные мелкие изменения по пути доставки, такие как смена кодировки, обрезание хвостовых пробелов в строках, «свертывание» и «развертывание» строк заголовка. Задача нормализации в том, чтобы выполнить минимальное преобразование сообщения (для целей подписания: само сообщение не модифицируется, поэтому проверяющий будет должен нормализовать письмо еще раз) так, чтобы максимально повысить вероятность того, что у получателя получится то же самое каноническое значение. В DKIM определены два алгоритма нормализации заголовков («простой» – simple и «спокойный» – relaxed) и два алгоритма для тел (с теми же названиями). Простой алгоритм практически нетерпим к модификациям, в то время как спокойный нормально переносит обычные модификации.

DMARC

DMARC (Domain-Based Message Authentication, Reporting, and Conformance), определенный в RFC 7489[38], позволяет отправителям электронной почты указывать политику ее обработки, типы отчетов, которые могут возвращать отправителю получатели, и частоту таких отчетов.

DMARC работает с SPF и DKIM. SPF позволяет отправителям уведомлять получателей (по DNS) о том, легитимна ли почта, якобы поступившая от этого отправителя, и как с ней следует поступить: доставить, отметить как подозрительную или выбросить. Однако ни в SPF, ни в DKIM нет механизма, который бы сообщал получателям, что используется SPF или DKIM. Нет и механизма обратной связи, чтобы информировать отправителей об эффективности методов борьбы со спамом. Например, если получатель получает сообщение без подписи DKIM, то в DKIM нет возможности сообщить получателю, что это значит: письмо подлинное, но его отправитель не использует DKIM – либо что письмо поддельное. В сущности, DMARC решает эти проблемы, указывая: а) будет ли использоваться SPF и/или DKIM; б) как должен поступить получатель, если они не используются; и в) как получателям следует отправлять отчеты о совокупных результатах работы по домену.

DKIM, SPF и DMARC удостоверяют различные аспекты сообщения. DKIM удостоверяет домен, приписавший к сообщению подпись. SPF работает с конвертом SMTP, определенным по RFC 5321[39]. Он может удостоверить либо домен, указанный в поле **MAIL FROM** конверта SMTP, либо домен **HELO**, либо оба сразу. Эти домены могут быть разными и обычно не видны конечному пользователю.

DMARC удостоверяет домен From в заголовке сообщения по RFC 5322. Это поле играет центральную роль в работе DMARC, поскольку это обязательное поле заголовка, а потому оно обязательно будет присутствовать в совместимых сообщениях, а большинство

MUA интерпретируют поле From по RFC 5322 как источник сообщения и передают часть его содержимого конечным пользователям. Конечный пользователь считает адресом отправителя именно тот почтовый адрес, который значится в этом поле. Поэтому он является столь лакомой мишенью для злоумышленников.

DMARC требует, чтобы содержимое поля From совпадало с аутентифицированным идентификатором (Authenticated Identifier) в DKIM или SPF. В случае DKIM сличаются домен подписания DKIM и домен From. В случае SPF сличаются домен аутентификации SPF и домен From.

Отправитель почты, использующий DMARC, обязан использовать также SPF и/или DKIM. Отправитель публикует в DNS политику DMARC, которая указывает получателям, как обращаться с сообщениями, якобы поступившими из домена отправителя. Эта политика выражена в виде ресурсной записи DNS TXT, сопоставленной доменному имени отправителя. Кроме того, отправитель должен также указать почтовый адрес для отправки сводных и аналитических отчетов. Поскольку эти почтовые адреса публикуются в DNS TXT RR без шифрования, они легко обнаруживаются, а в результате становятся мишенями для спама. Поэтому публикатору DNS TXT RR нужно задействовать какие-либо контрмеры.

Аналогично SPF и DKIM, политика DMARC в TXT RR записана в виде последовательности пар «тег=значение», разделенных точками с запятой. После публикации DMARC RR сообщения от этого отправителя обычно обрабатываются следующим образом:

1. Владелец домена создает политику SPF и публикует ее в своей базе данных DNS. Владелец домена также настраивает свою систему для генерации подписей DKIM. И, наконец, владелец домена публикует в DNS политику обработки сообщений DMARC.

2. Автор создает электронное письмо и передает его в выделенную службу отправки сообщений домена.

3. Служба отправки передает нужные данные в модуль подписания DKIM, получает цифровую подпись DKIM и дописывает ее к сообщению.

4. Служба отправки передает подписанное сообщение своей выделенной транспортной службе для маршрутизации к указанному получателю (или получателям).

Сообщение, созданное на стороне отправителя, поступает в транспортную службу получателя (возможно, по пути пройдя через другие пункты пересылки). На стороне получателя при использовании DMARC происходит следующее:

1. Получатель выполняет стандартные проверки, такие как проверка по черным спискам IP-адресов и спискам репутации доменов, а также применение квот на письма от конкретного источника.

2. Получатель извлекает поле From по RFC 5322 из сообщения, получая адрес. Это должен быть один адрес допустимого формата, иначе письмо считается битым и отбрасывается.

3. Получатель запрашивает запись DMARC DNS для домена отправителя. Если такой записи нет, работа DMARC завершается.

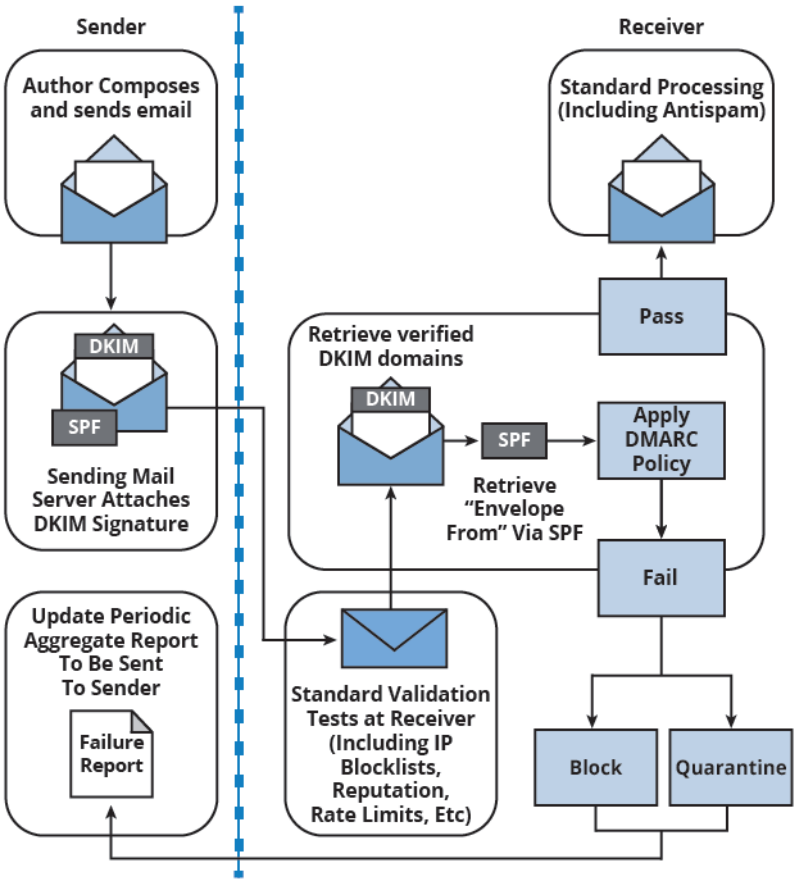
4. Получатель выполняет проверку подписи DKIM. Если в письме несколько подписей DKIM, одна должна пройти проверку.

5. Получатель запрашивает запись SPF для домена отправителя и выполняет проверки SPF.

6. Получатель выполняет проверку совпадения идентификаторов для поля RFC 5321 From и результатов, полученных из записей SPF и DKIM (если есть).

7. Результаты этих проверок передаются в модуль DMARC вместе с доменом автора. Модуль DMARC пытается извлечь политику из записей DNS для этого домена. Если ее нет, модуль DMARC определяет домен организации и пытается извлечь политику из

Рис. 9. Функциональная схема DMARC.



записей DNS уже для этого домена.

8. Если политика найдена, она комбинируется с доменом автора и результатами SPF и DKIM. По итогам генерируется результат политик DMARC (успех или неудача), а также (необязательно) могут генерироваться два типа отчетов.

9. Транспортная служба получателя по результатам работы DMARC либо доставляет сообщение в почтовый ящик адресата, либо выполняет другие действия в соответствии со своей локальной политикой.

10. При наличии запроса транспортная служба получателя собирает данные из сеанса доставки сообщения для обратной связи.

На рисунке 9, адаптированном с сайта **DMARC.org**, приведена сводная функциональная схема отправки и получения.

Отчеты DMARC дают отправителю обратную связь по его политикам SPF, DKIM, сличения идентификаторов и обращения с сообщениями. По результатам отправитель может доработать свои политики. Отправляются два типа отчетов: *сводные отчеты* (Aggregate Report) и *аналитические отчеты* (Forensic Report).

Сводные отчеты отправляются получателями периодически и содержат сводные данные по успехам и неудачам аутентификации сообщение, в том числе:

- политику DMARC отправителя за отчетный период;
- параметры обработки сообщений получателям (доставка, помещение в карантин, отказ);
- результаты SPF для данного идентификатора SPF;
- результаты DKIM для данного идентификатора DKIM;
- совпадение/несовпадение идентификаторов;
- результаты с разбивкой по поддоменам отправителя;
- пару доменов отправителя и получателя;
- примененную политику и ее отличия от запрошенной (если отличается);
- количество успешных аутентификаций;
- общее число полученных сообщений.

Эта информация помогает отправителю выявить пробелы в своей почтовой инфраструктуре и политике. Авторы SP 800-177 рекомендуют доменам отправителя начинать с политики DMARC **p=none**, чтобы судьба сообщения, не прошедшего ту или иную проверку, решалась локальными политиками получателя. По мере сбора сводных отчетов DMARC отправитель получит богатый материал для оценки того, в какой мере его почта проходит проверки внешними получателями, и сможет настроить политику **p=reject**, которая будет означать, что любые сообщения, не прошедшие проверки SPF, DKIM и совпадения, должны отбрасываться. Получатели же, проводя собственный анализ трафика, могут определить, является ли политика отправителя **p=reject** достаточно надежной для применения.

Аналитический отчет помогает отправителю настроить компоненты SPF и DKIM, а также оповещает его о том, что его домен стал частью фишинговой/спамерской кампании. Аналитические отчеты по формату аналогичны сводным, но со следующими отличиями:

- Получатели включают в отчет максимальную (в разумных пределах) часть сообщения и его заголовка, чтобы домен отправителя мог расследовать происшествие. Также добавляется поле *Identity-Alignment* с полями DKIM и SPF DMARC (при необходимости).
- Дополнительно может быть добавлено поле *Delivery-Result*. Если сообщение было подписано по DKIM, добавляются поля DKIM Domain, DKIM Identity и DKIM Selector. Дополнительно также могут быть добавлены поля DKIM Canonical для заголовка и тела.
- Добавляется дополнительное поле неудачной аутентификации DMARC – для случаев, когда сличение аутентификации дает несовпадение.

С момента своего появления DMARC сразу же стал популярен. Тысячи компаний с его помощью перехватили миллиарды злонамеренных писем, якобы исходивших из доменов этих компаний, защитив тем самым своих сотрудников и клиентов от фишинга, спама и т.д. Недавно два крупнейших почтовых провайдера в мире – Google и Yahoo – объявили, что распространяют эту защиту на новые интернет-домены под своим контролем[40].

Итоги

IETF разработала серию протоколов для обеспечения всеобъемлющей безопасности электронной почты в Интернете. Многие из них нашли широкое применение, и NIST рекомендует весь набор к использованию.

Благодарности

Автор пользуется случаем выразить свою благодарность рецензенту за множество подробных и дельных замечаний.

Источник: Internet Protocol Journal, vol. 19, No.3, http://ipj.dreamhosters.com/wp-content/uploads/issues/2016/ipj19-3.pdf

Ссылки

1. National Institute of Standards and Technology, «Trustworthy Email», NIST Special Publication 800-177, сентябрь 2016 г.

2. Dave Crocker, «Internet Mail Architecture», RFC 5598, июль 2009 г.

3. Crypto Portal, «Cryptology with Cryptool: Practical Introduction to Cryptography and Cryptanalysis», август 2010 г. https://www.cryptool.org/images/ct1/presentations/CrypToolPresentation-en.pdf

4. National Institute of Standards and Technology, «Introduction to Public Key Technology and the Federal PKI Infrastructure», NIST Special Publication 800-32, февраль 2001 г.

5. Paul Hoffman, «SMTP Service Extension for Secure SMTP over Transport Layer Security», RFC 3207, февраль 2002 г.

6. ZDNet, «Google, Microsoft, Yahoo: We want to stop e-mail snooping by fixing these encryption flaws», 21 марта 2016 г. http://www.zdnet.com/article/google-microsoft-yahoo-we-want-to-stop-e-mail-snooping-by-fixing-these-encryption-flaws/#!

7. Facebook, «The Current State of SMTP STARTTLS Deployment», 13 марта 2014 г. https://www.facebook.com/notes/protect-the-graph/ the-current-state-of-smtp-starttls-deployment/ 1453015901605223/

8. William Stallings, «SSL: Foundation for Web Security», *The Internet Protocol Journal*, Volume 1, No. 1, июнь 1998 г.

9. Andrea Peterson, «Facebook's security chief on the Snowden effect, the Messenger app backlash and staying optimistic», *The Washington Post*, 12 августа 2014 г.

10. David Cohen, «Facebook: 95% of Notification Emails Encrypted Thanks to Providers' STARTTLS Deployment», *AdWeek*, 19 августа 2014 г.

11. Marshall Rose and David Strom, «Secure E-Mail: Problems, Standards, and Prospects», *The Internet Protocol Journal*, Volume 2, No. 1, март 1999 г.

12. Sean Turner and Blake Ramsdell, «Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling», RFC 5750, январь 2010 г.

13. Sean Turner and Blake Ramsdell, «Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification», RFC 5751, январь 2010 г.

14. Paul Hoffman, «Examples of S/MIME Messages», RFC 4134, июль 2005 г.

15. Paul Hoffman, «Enhanced Security Services for S/MIME», RFC 2634, июнь 1999 г.

16. Russ Housley, «Cryptographic Message Syntax (CMS)», RFC 5652, сентябрь 2009 г.

17. Russ Housley, «Cryptographic Message Syntax (CMS) Algorithms», RFC 3370, август 2002 г.

18. Jim Schaad and Sean Turner, «Multiple Signatures in S/MIME», RFC 5752, январь 2010 г.

19. Sandy Murphy, Jim Galvin, Steve Crocker, and Ned Freed, «Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted», RFC 1847, октябрь 1995 г.

20. Paul Hoffman and Jakob Schlyter, «Using Secure DNS to Associate Certificates with Domain Names for S/MIME», RFC 8162, май 2017 г.

21. Philip Zimmermann, Derek Atkins, and William Stallings, «PGP Message Exchange Formats», RFC 1991, август 1996 г.

22. Hal Finney, Lutz Donnerhacke, Jon Callas, Rodney Thayer, and David Shaw, «OpenPGP Message Format», RFC 4880, ноябрь 2007 г.

23. Dave Del Torto, Michael Elkins, Raph Levien, and Thomas Roessler, «MIME Security with OpenPGP», RFC 3156, август 2001 г.

24. A. Whitten and J. Tygar, «Why Johnny can't encrypt: a usability evaluation of PGP 5.0», *Proceedings of the 8th conference on USENIX Security Symposium* - Volume 8 (SSYM'99), 1999 г.

25. Matthew Green, «What's the Matter with PGP?», Cryptography Engineering Blog, 13 августа 2014 г. http://blog.cryptographyengineering.com/2014/08/ whats-matter-with-pgp.html

26. Miek Gieben, «DNSSEC: The Protocol, Deployment, and a Bit of Development», *The Internet Protocol Journal*, Volume 7, No. 2, июнь 2004 г.

27. Richard Barnes, «Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)», RFC 6394, октябрь 2011 г.

28. Richard Barnes, «Let the Names Speak for Themselves: Improving Domain Name Authentication with DNSSEC and DANE», *The Internet Protocol Journal*, Volume 15, No. 1, март 2012 г.

29. Jakob Schlyter and Paul Hoffman, «The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA», RFC 6698, август 2012 г.

30. Viktor Dukhovni and Wesley Hardaker, «SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)», RFC 7672, октябрь 2015 г.

31. Scott Kitterman, «Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1», RFC 7208, апрель 2014 г.

32. «SPF-all Domain Survey», http://spf-all.com/stats.html

33. Barry Leiba and Jim Fenton, «DomainKeys Identified Mail (DKIM): Using Digital Signatures for Domain Verification», CEAS 2007 — *Fourth Conference on E-mail and Anti-Spam*, 2–3 августа 2007 г.

34. Murray Kucherawy, Dave Crocker, and Tony Hansen, «DomainKeys Identified Mail (DKIM) Signatures», RFC 6376, сентябрь 2011 г.

35. «Global DKIM Deployment», https://eggert.org/meter/dkim

36. Peter W. Resnick, «Internet Message Format», RFC 5322, октябрь 2008 г.

37. Tony Hansen, Dave Crocker, and Phillip Hallam-Baker, «DomainKeys Identified Mail (DKIM) Service Overview», RFC 5585, июль 2009 г.

38. Murray Kucherawy and Elizabeth Zwicky, «Domain-based Message Authentication, Reporting, and Conformance (DMARC)», RFC 7489, март 2015 г.

39. John C. Klensin, «Simple Mail Transfer Protocol», RFC 5321, октябрь 2008 г.

40. Dmarc.org, «Global Mailbox Providers Deploying DMARC to Protect Users», пресс-релиз Dmarc, 19 октября 2015 г.

Об авторе

Уильям Стеллингс (William Stallings), – независимый консультант и автор нескольких книг по безопасности, компьютерным сетям и компьютерной архитектуре. Его последняя книга – *Cryptography and Network Security* (Pearson, 2016 г.) Он держит сайт на **ComputerScienceStudent.com** с ресурсами для студентов в области компьютерных наук и профессионалов, а также входит в редакторский совет журнала *Cryptologia*. Имеет ученую степень Ph.D. по компьютерным наукам, присужденную Массачусетским технологическим институтом. Его электронный адрес: ws@shore.net.

Деятельность IETF в области конфиденциальности

Андрей Робачевский

Основные протоколы Интернета, такие как DNS, HTTP, SMTP, были разработаны во время, когда вопросы безопасности и сценарии атак выглядели более безобидно. Хотя работа по усилению защиты велась давно, разоблачения Эдварда Сноудена заставили многих по-другому взглянуть на проблему. Ведущая организация по разработке интернет-стандартов IETF не осталась в стороне и начала массивную работу по защите данных и конфиденциальности. О последних достижениях в этой области - эта статья.

Шифрование

Когда мы говорим о конфиденциальности и защите данных, шифрование безусловно является основной технологией. Поэтому шифрование по-прежнему является приоритетом в IETF. На протяжении нескольких декад IETF неустанно работает над повышением защищенности существующих и разрабатываемых протоколов посредством, в частности, поддержки аутентичности, конфиденциальности и целостности данных. Разоблачения Эдварда Сноудена придали сильный импульс этой работе.

Основная работа в этой области происходит в рабочей группе по безопасности транспортного уровня TLS (https://datatracker.ietf.org/wg/tls/about/), разрабатывающей основные спецификации, нескольких рабочих группах, посвященных тому, как применять работу рабочей группы TLS к различным приложениям, и исследовательской группе Crypto-Forum (CFRG, https://datatracker.ietf.org/rg/cfrg/about/), в которой основное внимание уделяется деталям основных криптографических алгоритмов.

Рабочая группа TLS является ключевой задачей IETF, разрабатывающей основные протоколы безопасности для Интернета. Итогом колоссальной работы стало утверждение спецификации TLS 1.3 в качестве стандарта IETF – RFC8446 (https://datatracker.ietf.org/doc/rfc8446).

«Колоссальной» - не является преувеличением: разработка стандарта заняла более четырех лет и 28 ревизий спецификации протокола. TLS 1.3 появился ровно десять лет спустя своего предшественника – протокола TLS 1.2. Неудивительно, что его появление представляет собой существенный шаг вперед в превращении Интернета в более безопасное и надежное место.

TLS 1.3 предлагает ряд технических преимуществ, таких как существенное уменьшение времени на создание соединения и возможность клиентам быстро возобновлять сеансы с серверов.

Не менее важно, что он также удаляет поддержку нескольких устаревших и небезопасных алгоритмов шифрования и хэширования, которые в настоящее время разрешены (хотя и не рекомендуются) для использования с более ранними версиями TLS, включая SHA-1, MD5, DES, 3DES и AES-CBC, и добавляет поддержку новых наборов шифров.

Другим важным изменением является переход от обмена ключами с использованием алгоритма RSA к алгоритму Ephemeral Diffie-Hellman (DHE). Причина в том, что ключ RSA сервера обычно не меняется в течение значительного периода времени, что означает, что любая компроментация этого ключа может привести к расшифровке ранее сохраненных сообщений. В новом протоколе ключ RSA используется только для аутентификации. Фактические ключи шифрования генерируются заново каждый сеанс с использованием Diffie-Hellman. Таким образом реализуется так называемая Forward Secrecy – невозможность декодирования ранее перехваченных сообщений в случае скомпрометированного ключа.

Это существенное усиление защищенности передачи данных представляет значительную проблему для так называемых решений сетевой безопасности, а проще – защитных экранов и других устройств инспектирования трафика. При использовании TLS 1.2 на этих устройствах достаточно было установить секретный ключ сервера для декодирования проходящего трафика. Схема работы по перехвату трафика показана на рис. 1. Как видно, при наличии предустановленного секретного RSA-ключа, устройство безопасности имеет возможность сгенерировать секретный ключ сеанса и таким образом инспектировать проходящий трафик. Этот подход широко используется в корпоративных

сетях для обеспечения политики безопасности. С приходом TLS 1.3 для этих целей придется искать другие решения.

В случае TLS 1.3 это возможно только путем создания двух защищенных каналов – от клиента к устройству и от устройства к серверу. Неудивительно, что эта проблема вызвала серьезные обсуждения, которые, к счастью, не привели к ослаблению защищенности протокола.

Протокол TLS 1.3 работает поверх TCP. Защита передачи данных на основе датаграммного протокола UDP не менее важна, тем более что все большее число приложений используют именно этот протокол. Рабочая группа TLS завершает работу над спецификацией DTLS 1.3 (https://datatracker.ietf.org/doc/draft-ietf-tls-dtls13/). Основная философия DTLS заключается в построении «TLS над транспортом датаграмм». Передача датаграмм не требует и не обеспечивает надежную или упорядоченную доставку данных. Протокол DTLS сохраняет это свойство для приложений, использующих такой тип передачи. Такие приложения, как потоковое мультимедиа, интернет-телефония и онлайн-игры, используют UDP для связи из-за чувствительного к задержке характера переносимых данных. Поведение таких приложений не изменяется, когда протокол DTLS используется для защиты связи, поскольку протокол DTLS не компенсирует потерянный или повторно запрошенный трафик данных. DTLS 1.3 обеспечивает такой же уровень защищенности передачи данных, что и TLS 1.3.

Server Name Indication (SNI)

Исторически сложилось так, что злоумышленники отслеживали использование веб-сервисов по трем каналам: поиск DNS-запросов, просмотр IP-адресов в заголовках пакетов и просмотр потока данных между пользователем и службами. Эти каналы постепенно закрываются. Растущая часть интернет-связи зашифровывается, в основном, с использованием TLS. Постепенное развертывание решений, таких как DNS в TLS RFC7858 «Specification for DNS over Transport Layer Security (TLS)» (https://datatracker.ietf.org/doc/rfc7858), затрудняет раскрытие информации DNS.

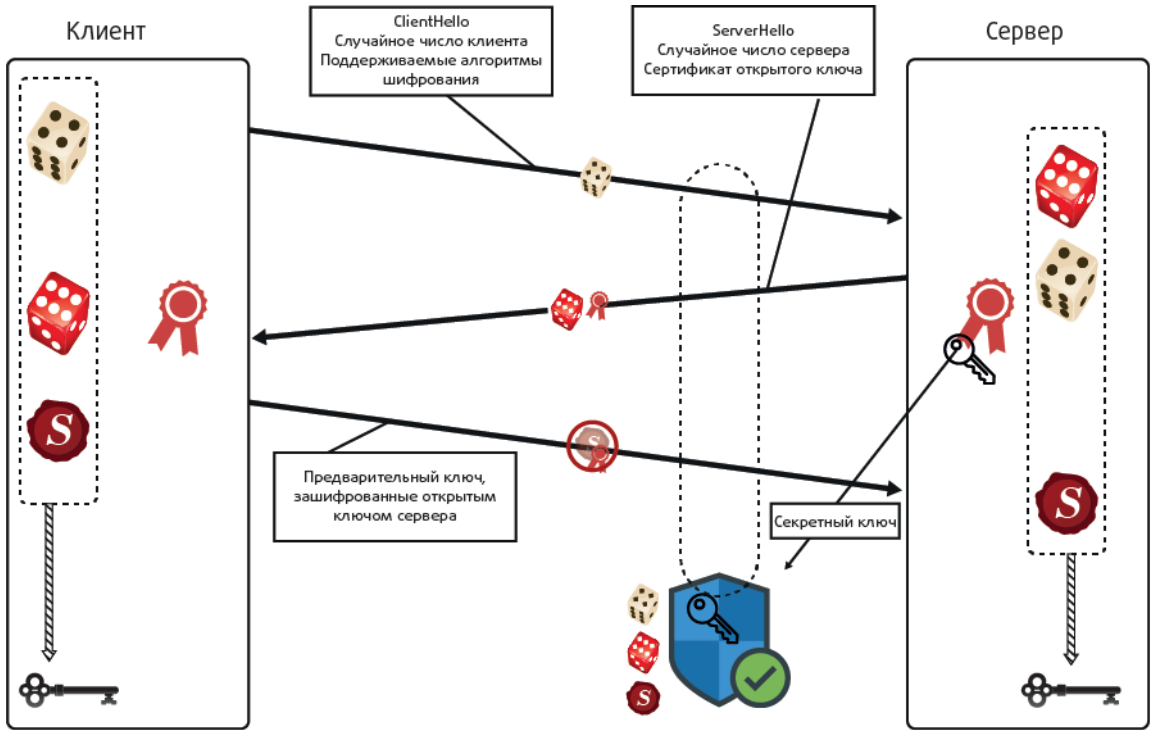
В то же время, все больше и больше сервисов размещаются на мультиплексированных серверах, исключая однозначную связь между IP-адресом и веб-сервисом. Типичным примером может служить несколько веб-сайтов, обслуживаемых одним и тем же веб-сервером. Однако для возможности использования защищенной сессии с помощью TLS, серверу необходимо знать, для какого имени предоставить серверный сертификат. Проблема в том, что в HTTPS обмен ключами происходит до того, как сервер получит первый веб-запрос; другими словами – сервер заранее не знает доменное имя веб-сервера, к которому хочет получить доступ клиент. Решением этой проблемы является информация об именах сервисов (SNI), а проще – имя виртуального веб-сервера, которое клиент посылает в процессе установления сеанса TLS.

Расширение SNI было стандартизовано в 2003 году в RFC3546 «Transport Layer Security (TLS) Extensions» (https://datatracker.ietf.org/doc/rfc3546). Оно содержит имя виртуального сервера, позволяющее установить соединение TLS с требуемым контекстом сервера. Текущую спецификацию расширения SNI можно найти в RFC6066 (https://datatracker.ietf.org/doc/rfc6066).

Этот элемент протокола передается в виде открытого текста. Поскольку другие методы мониторинга блокируются, мониторинг фокусируется на понятном SNI.

Спецификация SNI допускала разные типы имен серверов, но только вариант «имя хоста» был стандартизирован и

Рис. 1. Использование протокола RSA в версиях до TLS 1.3, позволяющее перехват и просмотр данных.



TLS 1.3 предлагает ряд технических преимуществ, таких как существенное уменьшение времени на создание соединения и возможность клиентам быстро возобновлять сеансы с серверов.

Не менее важно, что он также удаляет поддержку нескольких устаревших и небезопасных алгоритмов шифрования и хэширования, которые в настоящее время разрешены (хотя и не рекомендуются) для использования с более ранними версиями TLS, включая SHA-1, MD5, DES, 3DES и AES-CBC, и добавляет поддержку новых наборов шифров.

развернут. В этом варианте расширение SNI несет доменное имя целевого сервера. Расширение SNI отображается в текстовом виде в сообщении TLS «ClientHello».

Доступность имени хоста даже при использовании шифрования широко используется - и не всегда с хорошими намерениями. Известно, что эта информация полезна для блокирования трафика в целях цензуры, а также сбора частной информации о посещаемых сайтах. Рабочая группа TLS озадачилась этой проблемой и обсуждает возможное ее решение. Обсуждение возможных подходов описано в проекте стандарта «Issues and Requirements for SNI Encryption in TLS» (https://datatracker.ietf.org/doc/draft-ietf-tls-sni-encryption/).

Например, в отсутствие шифрования SNI на уровне TLS многие сайты полагаются на решение «HTTP Co-Tenancy». Соединение TLS устанавливается с единым фронт-сервером, а затем HTTP-запросы, принятые по этому соединению, направляются на соответствующий скрытый сервер. Например, TLS SNI может быть настроен на «fronting.example.com», фронт-сервер, и HTTP-запросы, отправленные по этому соединению, могут быть направлены на «hidden.example.com/some-content», обращаясь к скрытой службе. Это решение хорошо работает на практике, когда фронт-сервер и скрытый сервер являются «соарендаторами» одного и того же мультиплексированного сервера.

Это решение можно развернуть без изменения протокола TLS и оно не требует использования какой-либо конкретной версии TLS.

Шифрование на уровне протоколов приложений

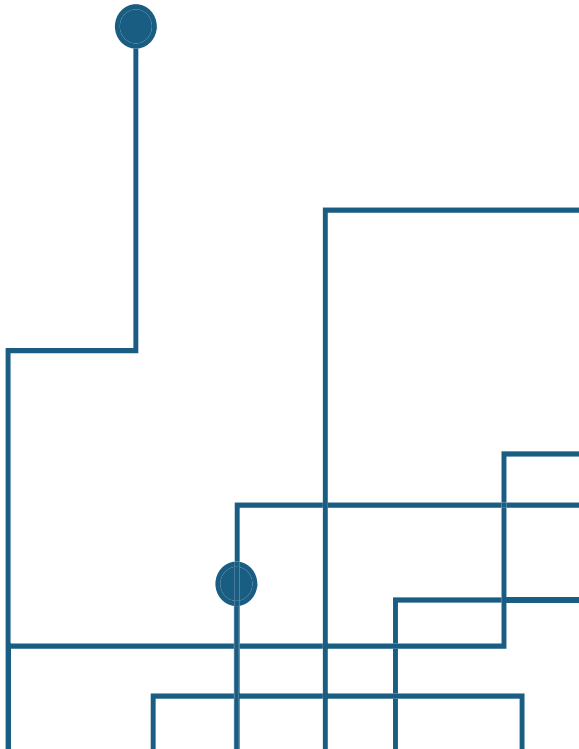
Рабочая группа «Использование TLS в приложениях» (UTA, https://datatracker.ietf.org/wg/uta/about/) была сформирована, чтобы разработать подходы для использования TLS с различными протоколами приложений. Она уже завершила работу над рядом документов, включая рекомендации по безопасному использованию TLS и DTLS, использование TLS для XMPP и использование процедур проверки подлинности сервера TLS для электронной почты.

Недавно завершилась работа над стандартизацией так называемой строгой транспортной безопасности (Strict Transport Security, STS) для почтовых серверов и пользовательских почтовых агентов, использующих протокол обмена почтовыми сообщениями SMTP.

Как известно, протокол SMTP не обеспечивает защиты данных. Для решения этой проблемы в настоящее время используется расширение STARTTLS для SMTP, задокументированное в RFC3207 «SMTP Service Extension for Secure SMTP over Transport Layer Security» (https://datatracker.ietf.org/doc/rfc3207), которое позволяет клиентам и серверам SMTP согласовывать использование канала TLS для шифрованной передачи почты.

Хотя этот оппортунистический протокол шифрования сам по себе обеспечивает высокий барьер против пассивного перехвата трафика, любой злоумышленник, который сможет удалить части сеанса SMTP (например, приглашение «250 STARTTLS»), или тот, кто может перенаправить весь SMTP-сеанс (возможно, перезаписав DNS-запись MX для доставки почты на домен), может выполнять атаки с понижением или перехватом.

Разработанный группой UTA механизм позволяет для доменов получателей, используя комбинацию DNS и HTTPS, указать:



- могут ли почтовые транспортные агенты MTA[1], отправляющие почту в этот домен, ожидать PKIX-аутентифицированной поддержки TLS;

- что клиент должен делать с сообщениями, когда TLS-сеанс не может быть успешно установлен.

Отчасти решение похоже на технологию DANE, которая использует наличие записей DANE TLSA для надежного оповещения поддержки TLS и публикации средств, с помощью которых клиенты SMTP могут успешно аутентифицировать законные SMTP-серверы. Однако, в отличие от DANE, использование которой требует поддержки DNSSEC, MTA-STS полагается на систему серверных сертификатов, обеспечивающих сегодня защиту веб-трафика.

Этот механизм задокументирован в RFC8461 «SMTP MTA Strict Transport Security (MTA-STS)» (https://datatracker.ietf.org/doc/rfc8461).

Как мы видим, работа по обновлению ключевых протоколов Интернета для лучшей защиты передаваемых данных и большей конфиденциальности не только не прекращается, но охватывает все новые области.

Ссылки

1. Для более подробного знакомства с работой электронной почты в Интернете и используемыми терминами я рекомендую прочитать статью «Всеобъемлющая безопасность электронной почты в Интернете» Уильяма Стеллингса, которую мы также публикуем в этом номере.

Регулирование персональных данных в правовой системе Европейского Союза

Мадина Касенова

Интернет, в силу своей уникальной технологической архитектуры, выступает критически важным элементом информационно-коммуникационных технологий, приобретая существенное (если не ключевое) значение в современной жизни человека, общества, государства. Интернет радикально и в трансграничном масштабе изменил взаимодействие лиц, расширив их коммуникативные возможности и сферы их «цифрового присутствия», что объективировало диверсификацию регламентации целого ряда отношений и, в частности, привело к тому, что данные личного характера (персональные данные/личная информация) стали самостоятельным объектом правового регулирования[1].

В нынешних условиях, когда выбор стратегического вектора социально-экономического развития современных государств ориентирован на «цифровую экономику»[2], данные личного характера приобретают особую экономическую значимость и коммерческую ценность[3]. Отнюдь не удивительно в этой связи появление таких фразеологизмов как «новая нефть» (*the new oil*)[4], «новая валюта цифрового мира» (*new currency of the digital world*)[5], «валюта будущего», устойчиво сопрягающихся с данными личного характера, в равной степени как и оценка «конфиденциальности» (*Privacy*) в качестве «высокостоимостной валюты» (*high-value currency*)[6].

Правовое регулирование сфер, связанных с данными личного характера, в правопорядках государств (его адекватность, эффективность, системность, динамика, тенденции развития) отличается плюрализмом, что во многом обусловлено разностью выбора способов и методов решения умножающегося числа вопросов, связанных с потенциальным «конфликтом» интенсификации использования таких данных и обеспечением их защиты, конфиденциальности, безопасности и т.д. Разумеется, что в условиях развития «цифровой экономики» этот «конфликт» будет нарастать и, как следствие, содержание и объем ряда понятий в правопорядках государств («персональные данные», «личная информация», «конфиденциальность», «неприкосновенность частной жизни» и др.), равно как и средства правовой защиты могут претерпеть радикальные изменения. Немаловажным фактором в этом контексте является и то, что трансграничная природа Интернета объективно требует международно-правового взаимодействия государств, прежде всего, при решении вопросов порядка трансграничного обмена данными и доступа к ним.

Обращение к подходам правового регулирования персональных данных в Европейском Союзе, безусловно, приобретает в настоящее время важное практическое значение для многих государств, в т.ч. и для Российской Федерации, и, как представляется, его целесообразно оценивать через призму отмеченных факторов.

Право Европейского Союза: предварительные замечания

Право Европейского Союза (далее – «Евросоюз» или «ЕС») обоснованно рассматривается как самостоятельная система, функционирование которой обеспечивается целостностью ее нормативного и институционального механизмов. Нормативный механизм правовой системы ЕС охватывает «первичное право», «вторичное право», а в качестве автономной категории источников права рассматривается прецедентное право Европейского суда (*European Court of Justice, ECJ*), в силу его соответствующих содержательных характеристик (далее – «Суд ЕС»)[7].

В праве ЕС основным понятием является «персональные данные» (*Personal Data*), которое закреплено и терминологически используется во всех правовых актах ЕС и стран-членов ЕС. Персональные данные квалифицируются применительно к физическим лицам, охватывая все циклы: сбор, обработка, накопление, хранение, доступ, обмен, передача и т.д., включая защиту конфиденциальности данных физических лиц (далее для целей настоящей статьи применяется условно-собирательный термин – «Использование и защита персональных данных»).

Источники «первичного права» ЕС, обладающие высшей юридической силой и систематизирующей ролью, обусловливают режим регулирования персональных данных в системе основных прав и свобод человека. Из этого исходят такие нормы «первичного права» как ст. 39 «Договора о Европейском Союзе» (далее – «Маастрихтский договор ЕС»), ст. 16 «Договора о функционировании ЕС» (далее – «Римский договор TFEU»), ст. 8 «Хартии Европейского Союза об основных правах» (далее – «Хартия ЕС об основных правах»), действующие в новейшей редакции 2007 года[8].

Регламент GDPR предметно ориентирован на частно-правовую сферу регулирования персональных данных. Из сферы действия GDPR исключены использование и защита персональных данных для целей предупреждения, расследования или судебного рассмотрения уголовных преступлений, либо приведения в исполнение уголовных наказаний, включая обеспечение защиты и предотвращения угроз общественной безопасности, свободное перемещение таких данных; также из сферы его действия исключены вопросы взаимодействия правоохранительных и судебных органов по уголовным делам и судопроизводству (преамбула (19), п. (d) ст. 2 GDPR).

Источники «вторичного права» ЕС охватывают нормативные акты руководящих органов ЕС (Парламента ЕС и/или Совета), принимаемые посредством обычной или особой законодательных процедур в форме директивы, регламента, решения, рекомендации и заключения. В системе источников «вторичного права» ЕС регламент, директива, решение – это юридически обязательные законодательные акты, принимаемые посредством законодательной процедуры, однако они различаются своей юридической силой[9]. В системе «вторичного права» ЕС нормативный акт, принятый Парламентом ЕС и Советом в форме *регламента*, находится «на вершине» иерархии источников. Регламент обладает общеобязательным действием, непосредственно применяется во всех странах-членах ЕС, всеми органами ЕС, а также лицами (физическими/юридическими), к которым он относится[10]. Регламент *de jure* не предполагает принятие имплементирующего национального акта, исключает действие национальных правовых актов в случаях «конфликта» между национальным правом и регламентом («приоритетный эффект применения»). Кроме того, регламент непосредственно применяется Судом ЕС, решения которого носят прецедентный характер, а также национальными органами правосудия.

Источником «вторичного права» ЕС является *директива* Парламента ЕС и Совета, которая наряду с *регламентом* относится к юридически обязательным законодательным актам. Юридическая сила *директивы* отличается от *регламента*: во-первых, она является актом «опосредованного» (не прямого) действия и предполагает «двухэтапную» реализацию, означающую ее транспонирование в правопорядок стран-членов посредством принятия соответствующего имплементирующего национального акта; во-вторых, ее адресатами выступают исключительно страны-члены (а не лица: физические и юридические); в-третьих, страны-члены самостоятельно определяют органы, способы и формы инкорпорации директивы в национальное право, с соблюдением ее целей, задач, а также установленных в ней сроков принятия имплементирующих национальных актов[11].

Институциональный механизм правовой системы ЕС обусловлен тем, что ЕС, с одной стороны, является уникальной международной межправительственной многосторонней региональной организацией интеграционного типа, которая обладает международной правосубъектностью, в т.ч. означающей право заключать международные договоры с международными организациями и государствами[12]; с другой стороны, в ЕС используется классическая «система разделения властей», присущая государствам. В институциональном механизме правовой системы ЕС «общесоюзные» органы (Парламент ЕС, Совет, Европейская Комиссия, Суд ЕС), в зависимости от предметной и функциональной компетенции, реализуют законодательные, исполнительные, распорядительные, финансовые и контрольные направления деятельности. Законодательная компетенция ЕС реализуется Парламентом ЕС и Советом посредством принятия правовых актов. Европейская Комиссия (далее – «Еврокомиссия») традиционно рассматривается в качестве главного исполнительного органа ЕС, вместе с тем, она участвует и в законодательном процессе, поскольку обладает правом законодательной инициативы[13].

В законодательной сфере деятельность Парламента ЕС, Совета и Еврокомиссии отражает существующий достаточно гибкий и подвижный механизм «разделения и взаимодействия» органов ЕС, основанный на принципе «скоординированной субординации» (*Subsidiarity Principe*)[14]. Так, Еврокомиссия вправе вносить на рассмотрение Парламента ЕС и Совета предложения по принятию конкретных нормативно-правовых актов (в форме директив, регламентов, решений), правомочна принимать нормативные акты общего действия в порядке «делегированного законодательства» и т.д.[15]

Высказанные предварительные замечания важны и для дальнейшего изложения, и для понимания общего контекста регулирования персональных данных в праве ЕС в его объективной обусловленности спецификой функционирования нормативного и институционального механизмов, а также присущей Евросоюзу международно-правовой правосубъектности.

Значение Директивы 95/46/ЕС

Принятая в 1995 году Парламентом ЕС и Советом Директива «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (далее – «Директива 95/46/ЕС»)[16], придала существенный импульс системному регулированию защиты персональных данных в ЕС и странах-членах ЕС. Директива 95/46/ЕС *de facto* и *de jure* закрепила формально-правовые рамки формирования общего правового режима персональных данных в ЕС и странах-членах ЕС. Такой режим зиждился на регулировании персональных данных физических лиц и прав на их защиту в системе основных прав и свобод человека, предусмотренной актами «первичного права» ЕС, и обеспечивался функционированием институционального механизма ЕС. Несомненно, Директива 95/46/ЕС сыграла систематизирующую и гармонизирующую роль в формировании общего «стандарта использования и защиты данных» в ЕС и странах-членах ЕС, даже несмотря на то, что в силу «опосредованного» применения, она не преодолела определённой разности подходов ее имплементации (транспонирования) в национальные правопорядки стран-членов ЕС.

Директива 95/46/ЕС очевидным образом придала дополнительный импульс дальнейшему развитию основ многостороннего международно-правового сотрудничества, которые были закреплены Конвенцией Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (далее – «Конвенция ETS 108»)[17]. Поправки, внесённые в 1999 году соответствующим Протоколом, позволили Евросоюзу участвовать в Конвенции ETS 108[18].

Немаловажно, что Директива 95/46/ЕС обусловила развитие формата билатерального международно-правового сотрудничества. Свидетельством этого служит факт заключения между США и Евросоюзом «Соглашения о безопасной гавани» (*U.S.-E.U. Safe Harbor Agreement*)[19]. Это соглашение (далее – «Соглашение Safe Harbor») относится к 2000 году, т.е. после вступления в силу Директивы 95/46/ЕС. Соглашение Safe Harbor, основываясь на шести базовых

принципах, предметно регулировало порядок осуществления трансграничной передачи персональных данных в коммерческих целях и распространялось на широкий круг лиц собирающих, обрабатывающих, хранящих и т.д. персональные данные.

Произошедшие за более чем двадцатилетний период действия Директивы 95/46/ЕС кардинальные технологические и социальные изменения, в свою очередь, обусловили необходимость изменения правового регулирования в ЕС и странах-членах ЕС сферы персональных данных, и это связывалось с необходимостью решения «двуединой задачи». Во-первых, следовало устранить сложившиеся различия законодательного регулирования и правоприменительной практики использования и защиты персональных данных в национальных правопорядках стран-членов ЕС, преимущественно связанные с разностью имплементации Директивы 95/46/ЕС. Во-вторых, следовало закрепить общий, единообразный и транспарентный правовой режим персональных данных на уровне Евросоюза, а также усовершенствовать институциональный механизм, обеспечивающий функционирование такого режима. Решить обозначенную «двуединую задачу» был призван законодательный акт – Регламент (ЕС) 2016/679 «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ ЕС (Общие положения о защите данных)», принятый 14 апреля 2016 года (далее – «Регламент GDPR» или «GDPR»).

Регламент GDPR

Регламент GDPR, согласно процедуре, вступил в силу на двадцатый день после его опубликования в Официальном журнале ЕС (т.е. в мае 2016 года), а с 25 мая 2018 года непосредственно и в полном объеме стал применяться в ЕС и в странах-членах ЕС[20]. Регламент GDPR – достаточно объёмный документ (173 пункта преамбулы и 99 статей). Содержательный анализ GDPR подробно прокомментирован российскими и зарубежными авторами[21], а также в исследованиях ряда авторитетных компаний (Baker&Mckenzie White&Case, Allen&Overy[22] и др.). Соответственно, в формате настоящей статьи представляется целесообразным обратиться к вопросам общеправового значения GDPR как для системы права ЕС, так и стран, не входящих в ЕС, а также для международно-правового сотрудничества государств.

Общеправовой контекст Регламента GDPR

Принятие нормативного акта в форме *регламента* в общеправовом плане «поднимает на высокий уровень» правовое регулирование использования и защиты персональных данных в ЕС, странах-членах ЕС, унифицируя его закреплением единого правового режима. «Единство» правового режима персональных данных основано и обеспечивается системой базовых принципов (п. 1 ст. 5 GDRP); общих операбельных понятий (ст. 4 GDRP); установлением требования о приведении в соответствие с его принципами и нормами всех нормативно-правовых актов ЕС, применимых к обработке персональных данных (п. 3 ст. 2 GDPR); закреплением комплекса прав субъекта персональных данных[23], при котором получение согласия субъекта данных выступает основополагающим (глава III GDPR), и т.д.

Так, в ряду общих операбельных понятий GDPR рассматривает понятия «персональные данные» (*personal data*) и «субъект данных» как ключевые. Ранее отмечалось, что понятие «персональные данные», согласно GDPR, применимо исключительно к физическому лицу, т.е. «субъекту данных», и независимо от национальной принадлежности или места жительства субъекта. GDPR содержательно раскрывает понятие «персональные данные», которое означает любую информацию, относящуюся к идентифицированному (идентифицируемому) физическому лицу, идентификация которого прямо или косвенно основывается на имени, идентификационном номере, сведениях о местоположении, идентификаторе в Интернете (онлайн-идентификатор), на одном или нескольких показателях, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица (п. (1) ст. 4 GDPR). Примечательно, что в GDPR прямо предусмотрена его «*неприменимость*» к обработке персональных данных юридических лиц и, в частности, к предприятиям, созданным как юридические лица, включая их наименование, организационно-правовую форму, а также реквизиты юридического лица (преамбула (14) GDPR). Отметим попутно, что российский законодатель также закрепляет понятие «персональные данные» и исходит из их применимости к физическому лицу; содержание этого понятия означает любую информацию, относящуюся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)[24].

Установление общих и равнозначных мер ответственности за нарушения обработки персональных данных физических лиц в ЕС также обеспечивает «единство» правового режима персональных данных (глава VIII GDPR). В силу непосредственной применимости GDPR, закрепление «общих мер ответственности» способствует единообразию формирования правоприменительной практики на уровне ЕС, в странах-членах ЕС, а также на практику Суда ЕС. Закрепление общих и равнозначных мер ответственности имеет важное значение, поскольку разность имплементации Директивы 95/46/ЕС в странах-членах ЕС, даже при определении размеров штрафных санкций, привела к весьма противоречивой практике[25].

«Единство» правового режима персональных данных обеспечивается функционированием общего и специального институционального механизма, охватывающего и уровень ЕС, и национальный уровень. GDPR в контексте правового режима персональных данных определяет параметры деятельности органов ЕС общей компетенции, в частности, закреплены полномочия Еврокомиссии по принятию актов в порядке делегированного законодательства по применению GDPR; обозначена компетенция Парламента ЕС и Совета: эти органы рассматривают, во-первых, отчёт, предоставляемый Еврокомиссией об оценке и анализе применения GDPR (отчёт передаётся начиная с 25 мая 2020 года и каждые последующие четыре года), во-вторых, ежегодные отчёты Европейского совета по защите данных (*EDPB*). Применение GDPR непосредственно связано и с деятельностью Суда ЕС как общего органа институциональной структуры ЕС, формирующего правоприменительную (прецедентную) практику.

Согласно GDPR, к органам специальной компетенции институциональной структуры ЕС отнесены Европейский совет по защите данных (*European Data Protection Board, EDPB*) – новый директивный и надзорный орган с правами юридического лица[26]; Европейский инспектор по защите данных (*European Data Protection Supervisor, EDPS*) и его персонал[27]. Кроме того, GDPR предусматривает функционирование национальных институциональных надзорных органов/органа (*Supervisory authority*), учреждение одного или нескольких полномочных государственных органов, инспектора по защите персональных данных (*Data Protection Supervisor*). В настоящее время во всех странах-членах ЕС созданы надзорные органы/орган[28], которые в т.ч. координированно сотрудничают между собой, с Еврокомиссией, а также Европейским Советом по защите данных (*EDPB*).

Регламент GDPR и контекст публично-правового регулирования персональных данных в Евросоюзе

Регламент GDPR предметно ориентирован на частно-правовую сферу регулирования персональных данных. Из сферы действия GDPR исключены использование и защита персональных данных для целей предупреждения, расследования или судебного рассмотрения уголовных преступлений, либо приведения в исполнение уголовных наказаний, включая обеспечение защиты и предотвращения угроз общественной безопасности, свободное перемещение таких данных; также из сферы его действия исключены вопросы взаимодействия правоохранительных и судебных органов по уголовным делам и судопроизводству (преамбула (19), п. (d) ст. 2 GDPR).

Безусловно, правовое регулирование использования и защиты персональных данных не может быть обеспечено без деятельности в т.ч. правоохранительных и судебных органов. В этой связи следует отметить временное совпадение принятия Регламента GDPR и Директивы (ЕС) 2016/680 «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных наказаний и о свободном перемещении таких данных и отмене рамочного решения Совета ЕС 2008/977/ JHA» (далее – «Директива 2016/680»)[29].

Директива 2016/680 исходит из общих правил защиты физических лиц в отношении обработки персональных данных в ЕС, и ее положения коррелируют с нормами «первичного права» ЕС, Регламентом GDPR и иными актами права ЕС[30]. Это свидетельствует о «комплексности подхода» правового регулирования персональных данных в ЕС в публично-правовом контексте. В этой связи важно обратить внимание, что 17 апреля 2018 года Еврокомиссия внесла на рассмотрение Парламента ЕС и Совета два предложения, а именно: «Предложение относительно принятия Директивы Парламента ЕС и Совета, утверждающей гармонизированные правила о назначении законных представителей в целях сбора доказательств в уголовном процессе» (далее – «Директива о представителях в ЕС»)[31] и «Предложение относительно принятия Регламента Парламента ЕС и Совета о Европейских предписаниях о предоставлении данных (*European Production Orders*) и хранении данных (*Preservation Orders*) в отношении электронных доказательств по уголовным делам» (далее – «Регламент о предписаниях ЕС»)[32]. Принятие этих предложений, конечно, будет иметь «общеправовой эффект» и в предметном значении для уголовного права и уголовного процесса ЕС, и в оптимизации взаимодействия правоохранительных и судебных органов ЕС[33].

Директива о представителях в ЕС, применительно к режиму защиты персональных данных, связана с уголовно-процессуальным аспектом, а Регламент о предписаниях ЕС – с уголовным (материально-правовым). Оба названных документа призваны гармонизировать на уровне ЕС порядок доступа к персональным данным, специфицированный к контексту взаимодействия правоохранительных и судебных органов по уголовным делам в уголовном процессе. Ввиду ограниченности формата статьи, отметим лишь два момента.

«Единство» правового режима персональных данных обеспечивается функционированием общего и специального институционального механизма, охватывающего и уровень ЕС, и национальный уровень. GDPR в контексте правового режима персональных данных определяет параметры деятельности органов ЕС общей компетенции, в частности, закреплены полномочия Еврокомиссии по принятию актов в порядке делегированного законодательства по применению GDPR; обозначена компетенция Парламента ЕС и Совета: эти органы рассматривают, во-первых, отчёт, предоставляемый Еврокомиссией об оценке и анализе применения GDPR (отчёт передаётся начиная с 25 мая 2020 года и каждые последующие четыре года), во-вторых, ежегодные отчёты Европейского совета по защите данных (*EDPB*). Применение GDPR непосредственно связано и с деятельностью Суда ЕС как общего органа институциональной структуры ЕС, формирующего правоприменительную (прецедентную) практику.

Первый. Директива о представителях в ЕС коррелирует с соответствующими нормативными положениями GDPR и иными актами ЕС, предусматривающими назначение законного представителя[34]. В общем плане принятие этой Директивы направлено на регулирование вопросов юрисдикции; применимого права в ситуациях, осложнённых

иностранным элементом («*cross-border situations*»); обеспечение согласованного подхода к порядку вручения предписания поставщику услуг (законному представителю поставщика) и т.д.

Второй. Регламент о предписаниях ЕС, так же, как и GDPR[35], устанавливает категоризацию данных, закрепляя, разграничивая и содержательно определяя следующие категории данных: данные абонента (*subscriber data*); данные доступа (*access data*); транзакционные данные (*transactional data*); а также данные контента (*content data*). Поскольку все названные категории данных содержат «персональные данные» (в их общепонятийном значении), соответственно, Регламент о предписаниях ЕС исходит из того, что режим всех этих категорий данных подпадает под действие общих гарантий в рамках ЕС (*EU data protection acquis*)[36] по защите данных. Существенное значение имеет то, что Регламент о предписаниях ЕС не только определяет порядок трансграничного сбора электронных доказательств по уголовным делам и трансграничного доступа к данным, но и предусматривает соответствующие проформы предписаний, и исходит из механизма взаимного признания предписаний.

Влияние Регламента GDPR на регулирование персональных данных в странах, не входящих в ЕС (на примере США)

Регламент GDPR так или иначе окажет влияние на развитие регулирования персональных данных в правопорядках многих государств, не входящих в ЕС. Это объясняется как параметрами функционирования собственно самой системы права ЕС, так и разграничением территориального и юрисдикционного действия GDPR[37], продиктованным необходимостью обеспечения защиты персональных данных физических лиц в ЕС и странах-членах ЕС. Влияние GDPR очевидным образом прослеживается в динамике развития регулирования рассматриваемой сферы отношений в праве США, относящейся к системе «общего права» (*Common Law*). Кратко, в порядке тезисов отметим следующее.

В праве США понятие «личная информация» (*Personal Information*) является основным, это понятие закреплено и терминологически используется в нормативно-правовых актах федерального уровня и уровня штатов. При этом подчеркнём, что содержание и объем этого понятия в настоящее время однозначно не относится исключительно к физическим лицам (к примеру, как в праве ЕС) и может применяться также к данным различных организаций (являющихся юридическими лицами и не являющихся таковыми). В силу разграничения сфер компетенции Федерации и штатов, использование и защита личной информации в правопорядке США регулируется системой актов федерального уровня и уровня штатов[38]. Специфика системы действующих актов заключается в их «отраслевом» характере, в том, что они принимались в разное время (и это определяет разность их содержательного объёма, применяемых методов регулирования и т.д.), а также в том, что они исходят из обеспечения конституционных мер защиты прав частных лиц[39]. При этом, в праве США не принят единый, всеобъемлющий акт, регулирующий сферу личной информации[40]. С этой точки зрения обратим внимание на два законодательных акта, принятых в США после вступления в силу GDPR и в связи сего действием.

Во-первых, после вступления в силу GDPR, в феврале 2018 года Конгресс США внёс поправки в Титул 18 Кодекса США, «пополнив» тем самым законодательный массив права США федеральным кодификационным актом. Речь идёт о «Законе о совершенствовании правоприменительной деятельности по доступу к данным, хранящимся за рубежом, а также в иных целях»[41]. Этот закон (далее – «CLOUD Act») закрепляет механизмы взаимодействия на уровне правительств в отношении трансграничного доступа, обязательные условия для такого доступа, порядок раскрытия (*disclosure*) данных; регулирует порядок предоставления доступа, хранения, раскрытия и т.д. данных поставщиками коммуникационных услуг, а также предусматривает меры процедурно-процессуального порядка и т.д.[42].

CLOUD Act, в отличие от GDPR, не оперирует, в частности, понятием «субъект данных», а использует понятия «потребитель» (*customer*), «абонент» (*subscriber*), «резидент Соединённых Штатов» (*United States person*). Понятие «резидент США» означает гражданина или жителя США, допущенного на законном основании к постоянному проживанию; некорпоративную ассоциацию (*unincorporated association*) (т.е. объединение без прав юридического лица), значительное число членов которой являются гражданами США или допущены на законном основании к постоянному проживанию; а также корпорацию (*corporation*), инкорпорированную (т.е. зарегистрированную) в США.

Во-вторых, практически через месяц после начала применения GDPR, 28 июня 2018 года в штате Калифорния был одобрен «Закон о конфиденциальности потребителей», который начнёт действовать с 1 января 2020 года (далее – «CCPA Калифорния»)[43]. Помимо того, что предметная сфера и содержание CCPA Калифорния явно связаны с GDPR, в нем закреплён целый ряд схожих нормативных положений: предусмотрен комплекс субъективных прав (право на забвение, право на переносимость данных, право на доступ к данным и др.), предусмотрена обязанность «целевого» сбора информации, установлена ответственность за утечку данных и возмещение убытков и т.д.[44].

Регулирование в CCPA Калифорния, по сравнению с GDPR, отличается детализацией категориально-понятийного аппарата, субъектного состава, категоризацией прав и обязанностей вовлеченных лиц и т.д. Так, закрепляя и содержательно раскрывая понятие «личная информация», CCPA Калифорния предусматривает, что правом защиты личной информации обладает «потребитель» (*consumer*), т.е. физическое лицо, являющееся резидентом штата Калифорния. «Личная информация, связанная с потребителем» (*personal information relating to consumer*), означает информацию, которая идентифицирует, относится, описывает, может быть связана или может быть обоснованно связана, прямо или косвенно, с конкретным потребителем или семьей (*household*). Личная информация охватывает (но не ограничивается):

- идентификаторы (настоящее имя, псевдоним, почтовый адрес, уникальный персональный идентификатор, сетевой идентификатор, адрес интернет-протокола, адрес электронной почты, имя учетной записи, номер социального страхования, номер водительского удостоверения, номер паспорта или другие аналогичные идентификаторы);

- коммерческую информацию, включая записи о личной собственности, товарах/услугах, приобретенных, полученных или предполагаемых к приобретению;

- биометрические данные;

- информацию о действиях в Интернете или иных электронных сетях, включая в т.ч. историю просмотров, поиска, а также информацию о взаимодействии потребителя с веб-сайтами, приложениями или рекламой в Интернете; данные о геолокации;

- информацию о занятости;

- любую информацию, связанную с созданием профиля потребителя, отражающего предпочтения, характеристики, психологические тенденции, предрасположенности, поведение, отношение, интеллект, способности и склонности потребителя и т.д.

Примечательно, что «личная информация», согласно CCPA Калифорния, не включает «общедоступную информацию», содержание которой также раскрывается в этом акте.

Категориальный аппарат CCPA Калифорния использует также понятие «лицо» (*person*), понимаемое в «широком» содержательном значении: физическое лицо, единоличное предприятие, фирма, партнёрство, совместное предприятие, объединение, коммерческий паевой траст, компания, корпорация, общество с ограниченной ответственностью, ассоциация, коллегиальный орган и иные организации или группы лиц, осуществляющие совместную деятельность. Соответственно, субъективные права, согласно CCPA Калифорния, принадлежат потребителю. Именно потребитель вправе требовать раскрытия категорий (конкретных частей) личной информации, которую компания собирает о потребителе, категории источников, из которых эта информация собирается, цели сбора и передачи личной информации, а также категории третьих лиц, которым она передаётся.

Упоминание CCPA Калифорния, т.е. ещё не принятого акта, важно не только с точки зрения хронологии, его предметной сферы, явной содержательной связанности регулирования с GDPR и т.д., но и в силу того, что множество американских компаний, в т.ч. непосредственно поддерживающие и обеспечивающие функционирование критической инфраструктуры Интернета, являются юридическими лицами, созданными в соответствии с правом штата Калифорния, а именно: Корпорация по управлению доменными именами и IP-адресами (*Internet Corporation for Assigned Names and Numbers*, далее – «ICANN»), Корпорация «Технические идентификаторы общего пользования» (*Public Technical Identifiers*, *PTI*), Институт информатики при Университете Южной Калифорнии (*USC Information Sciences Institute*, *ISI*) и др.

Нельзя не сказать о специфике правопорядка США, заключающейся в том, что саморегулирование и сорегулирование[45] выступают (изначально выступали) важным инструментом регламентации использования собственно самого Интернета, а также сфер, связанных с его применением, в т.ч. использованием и защитой личной информации. Соответственно, арсенал регулирования, наряду с нормативным правовым, охватывает и нормативный «неправовой инструментарий»: руководящие принципы, разработанные регулирующими органами и учреждениями, лучшие практики коммерческих, технологических и промышленных групп и т.д.[46]. В этой связи следует обратить внимание на документы ICANN[47], принятые в связи с GDPR.

ICANN инициировала ряд запросов новому органу ЕС – Европейскому совету по защите данных (*European Data Protection Board*, *EDPB*) - по применению GDPR, итогом которых стали следующие документы ICANN. Во-первых, в соответствии с материалами и рекомендациями Европейского совета по защите данных (*EDPB*) в мае 2018 года правление ICANN приняло «Временные требования регистрационных данных общих доменов верхнего уровня»[48]. Названный документ предусматривает меры, позволяющие операторам реестров ICANN и данных общих доменов верхнего уровня (*gTLD*), а также регистраторам соблюдать требования, вытекающие из действующих договоров ICANN, а также политики в отношении регистрационных данных общих доменов верхнего уровня, включая *WHOIS*. Кроме того, документ регулирует порядок сбора регистрационных данных (в т.ч. владельца регистрации, административную и техническую контактную информацию и т.д.), ограничивая большинство персональных данных «многоуровневым», «целевым» доступом к ним. Во-вторых, в июне 2018 года ICANN представила к обсуждению «Проект рамок для Единой модели доступа к непубличным данным *WHOIS*»[49]. Предлагаемая Единая модель доступа (*Unified Access Model*) направлена на создание правовой определённости для ICANN в контексте ее роли в качестве регулирующего и координирующего органа системы *WHOIS*, для соблюдения нормативных требований Регламента GDPR.

Регламент GDPR и дальнейшее развитие международно-правового сотрудничества

В июле 2016 года, т.е. практически через месяц после вступления в силу GDPR (май 2016), между США и ЕС было заключено соглашение, закрепившее новый формат трансграничного обмена персональными данными в коммерческих целях, именуемое «Щит конфиденциальности ЕС-США» (*EU-U.S. Privacy Shield*)[50]. Заключению названного соглашения (далее – «Соглашение Privacy Shield») предшествовало решение Европейского суда от 6 октября 2015 года,[51] отменившее «формат» Соглашения Safe Harbor (принятого в связи с Директивой 95/46/ЕС, о чем говорилось ранее). Соглашение Privacy Shield с 1 августа 2016 года стало действующим правовым механизмом при трансграничной передаче данных в коммерческих целях, «соответствующим требованиям «стандарта GDPR»[52].

В декабре 2016 года между США и ЕС было заключено «Соглашение о защите личной информации, связанной с предупреждением, расследованием, обнаружением и привлечением к ответственности за уголовные преступления»[53]. Соглашение, именуемое «Зонтичным Соглашением», предусматривает комплекс мер защиты личных данных при их обмене между правоохранительными органами и органами уголовного правосудия[54].

И последнее. Нельзя не отметить, что в настоящее время единственным действующим юридически обязательным международным договором в сфере персональных данных, защиты неприкосновенности частной жизни при использовании информационных и коммуникационных технологий и т.д. является упомянутая ранее Конвенция ETS 108. В силу значения Конвенции ETS 108, в Регламенте GDPR прямо предусмотрено, что при оценке уровня защиты персональных данных следует исходить из ее положений, в т.ч. касающихся регулирования трансграничных потоков данных (преамбула (105) GDPR), и иных действующих международно-правовых механизмов.

Примечательно, что после начала применения GDPR, 10 октября 2018 года, Конвенция ETS 108 была «модернизирована» принятием Протокола о внесении соответствующих поправок, которые закрепили новые многосторонние международно-правовые рамки сотрудничества и подходы к защите физических лиц при обработке персональных данных[55]. Содержание нормативных положений названного Протокола коррелирует с положениями GDPR, в частности, некоторые новеллы Протокола предусматривают закрепление строгих требований соблюдения принципов соразмерности, минимизации данных и правомерности обработки; расширение типов конфиденциальных данных (в т.ч. генетические и биометрические данные, членство в профсоюзах и этническое происхождение); обязательства сообщать об утечках данных и обеспечивать прозрачность обработки данных; закрепление подотчётности операторов данных; определение режима трансграничных потоков данных и т.д.

***

Подходы Российской Федерации в сфере регулирования использования персональных данных (сбор, обработка, хранение, доступ к данным правоохранительных органов и т.д.) отличаются, а нередко диаметрально противоположны тем, что действуют и динамично развиваются в ЕС, странах-членах ЕС, США и других странах. Увы, в популистских целях часто делается ссылка на право ЕС и США, якобы закрепляющие подходы, аналогичные тем, которые в настоящее время существуют в российском праве и используются в российской правоприменительной практике. В этой связи изложенное поможет получить адекватную информацию относительно параметров регулирования персональных данных в праве Евросоюза.

Ссылки

1. См.: Архипов В. В. Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория // Закон. 2018. N 2. С. 66.

2. Достаточно назвать Стратегию Единого цифрового рынка Евросоюза (*EU Digital Single Market strategy*). *6 May 2015*. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 (Дата обращения: 09.09.2018); Программу «Цифровая экономика Российской Федерации» 2017 г. (утверждена распоряжением правительства РФ от 28.07.2017 № 1632-р). СПС «Консультант Плюс».

3. К примеру, персональные данные рассматриваются в числе нематериальных активов, составляющих более 84% рыночной стоимости компаний, включенных в индекс корпорации Standard&Poor (S&P 500). См., например, S&P 500. – URL: https://www.finanz.ru/indeksi/rynochnaya-kapitalizatsiya/s&p_500 (Дата обращения 18.08.2018).

4. См., например, *The DAC Beachcroft LLP Personal Data: the new oil and its toxic legacy under the General Data Protection Regulation. DAC Beachcroft LLP. DAC Beachcroft 2017*. – URL: https://www.luther-lawfirm.com/fileadmin/user_upload/PDF/Broschueren/Studien/DACB_GDPR_Liability_Study_-_Luther.pdf (Дата обращения 18.08.2018).

5. См. также проект социального эксперимента, предпринятый компанией «Лаборатория Касперского» с «долларом данных» (*Data Dollar*), который переведен на русский язык как «инфодоллар» (логотип – «ɘ»). – URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-launches-infodollar-a-new-currency-based-on-personal-information (Дата обращения 18.08.2018).

6. Grossman J. *Data Is Currency, Don't Abuse It*. URL: https://www.forbes.com/sites/forbesagencycouncil/2018/07/09/data-is-currency-dont-abuse-it/#7cc6305243d6 (Дата обращения 18.08.2018).

7. Об этом, например, *Summaries of EU Legislation*. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14534 (Дата обращения: 09.09.2018).

8. Ст. 16 Римского договора TFEU (бывшая ст. 16 B); ст. 8 Хартии Европейского Союза об основных правах. К примеру, ст. 39 Маастрихтского договора ЕС (бывшая ст. 25 bis) предусматривает следующее: «Европейский Парламент и Совет, в соответствии с обычной законодательной процедурой, устанавливают правила о защите физических лиц в отношении обработки персональных данных институтами, органами и учреждениями Союза, а также государствами-членами при осуществлении деятельности, которая входит в сферу применения права Союза». СПС «Консультант Плюс». См. также «Декларацию в отношении статьи 16 «B» Договора о функционировании Европейского Союза» (Декларация № 20) и «Декларацию о защите персональных данных в области судебного сотрудничества по уголовным делам и полицейского сотрудничества» (Декларация № 21). СПС «Консультант Плюс».

9. См. об этом ст. 289 (бывшая статья 249 A), ст. 294 Римского договора TFEU. СПС «Консультант Плюс».

10. Ст. 288 Римского договора TFEU предусматривает следующее: «Регламент имеет общее действие. Он является обязательным в полном объеме и подлежит прямому применению во всех государствах-членах». Официальный журнал Европейского Союза – OJ C 326, 26.10.2012, P. 0001 – 0350.

11. К источникам «вторичного права» ЕС относится *решение* – нормативный акт Европейского Парламента и/или Совета Евросоюза индивидуального характера, прямого действия, адресатом которого являются как страны-члены, так и лица. Юридическая сила *решения* отличается и от регламента, и от директивы: в отличие от регламента, *решение* принимается в отношении конкретного государства-члена или лица/группы лиц; в отличие от директивы, *решение* обладает прямым действием в отношении лиц, указанных в нем. См., к примеру, Решение Европейской Комиссии относительно компании *Google* (17/06/2017). – URL: http://ec.europaeu/competition/elojade/isef/case_details.cfm?proc_code=1_39740, а также – URL: http://europa.eu/rapid/press-release_IP-17-1784_en.htm (Дата обращения 18.09.2018).

12. В настоящее время ЕС участвует в качестве самостоятельного участника в более 50 международных соглашениях, заключенных в рамках ООН, ВТО и др. *McGoldrick D. The International Legal Personality of the European Community and the EU* // 50 Years of the European Treaties. Looking Back and Thinking Forward / Eds. by M. Dougan, S. Currie. Oxford, 2009. P. 189.

13. В настоящее время в экономической и валютной сфере Евросоюза Европейский Центральный банк также участвует в различных формах в законодательной деятельности.

14. Этот принцип закреплен, к примеру, в нормативных положениях ст. 5 Маастрихтского договора. СПС «Консультант Плюс».

15. О компетенции и порядке принятия актов делегированного законодательства Европейской Комиссией см., например, ст. 290 Римского договора TFEU. СПС «Консультант Плюс». К примеру, конкретный законодательный акт Парламента ЕС и Совета может предусматривать принятие Еврокомиссией актов общего действия, в порядке делегированного законодательства, уточняющие, изменяющие, дополняющие отдельные положения этого акта. В правовой доктрине акты, принятые в порядке «делегированного

законодательства» (т.е. «незаконодательные» акты общего действия) именуются «актами третичного права», в которых определяются цели, сфера их действия, указание на их принятие в рамках делегирования полномочий и т.д.

16. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (Директива №95/46/ЕС принята в 1995 г., с изм. и доп. от 29.09.2003 г.). Официальный журнал Европейского Союза № L 281, 23.11.1995, p. 31.

17. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбург 28.01.1981) действует с поправками 1999 г. в редакции Дополнительного протокола ETS 181. Конвенция вступала в силу для разных стран в разное время, к примеру, для Российской Федерации – в 2013 г. СПС «Консультант Плюс».

18. The amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108), allowing the European Communities to accede, were adopted by the Committee of Ministers on 15 June 1999, in Strasbourg. – URL: https://www.coe.int/en/web/data-protection/convention108/amendments/ (Дата обращения 18.09.2018).

19. *U.S.-E.U. Safe Harbor Agreement.* – URL: https://2016.export.gov/safeharbor/eu/; а также, например, – URL: https://www.edq.com/uk/glossary/safe-harbour-agreement/ (Дата обращения 18.09.2018).

20. Регламент вступает в силу на двадцатый день после его опубликования в Официальном журнале ЕС. Финлейнсон-Браун Д. (*Jane Finlayson-Brown*), Пеммелаар В. (*Wanne Pemmalaar*) Общий Регламент ЕС по защите персональных данных. // «Интернет изнутри», 2017, № 6 (май), с. 26-30.

21. См, например, Савельев А. И. Направления регулирования больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. N 5. С. 122 – 144; Финлейнсон-Браун Д. (*Jane Finlayson-Brown*), Пеммелаар В. (*Wanne Pemmalaar*) Общий Регламент ЕС по защите персональных данных. // «Интернет изнутри», 2017, № 6 (май), с. 26-30 и др.

22. Baker&Mckenzie о GDPR. URL: https://www.bakermckenzie.com/en/insight/publications/2018/06/the-impact-eu-gdpr-on-ma (Дата обращения 18.08.2018); White&Case о GDPR. URL: https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation. (Дата обращения 18.08.2018); Allen&Overy о GDPR. URL: http://www.allenovery.com/publications/en-gb/data-protection/Pages/default.aspx (Дата обращения 18.08.2018).

23. Этот комплекс прав охватывает в том числе право на исправление данных; право на забвение; право на ограничение обработки; право на переносимость данных; право на возражение; право на доступ к данным; право на получение информации об утечке данных; право подавать жалобу в надзорный орган; право на эффективные средства судебной защиты против надзорного органа; право на эффективные средства судебной защиты в отношении контролера или обработчика; право действовать через представителя; право на получение компенсации от контролера или обработчика за полученный ущерб.

24. **См. п. 1 статьи 3 Федерального закона №152-ФЗ «О персональных данных» 2006 г. (в ред. от 31.12.2017). СПС «Консультант Плюс».**

25. Показательными являются следующие примеры расхождений применения штрафных санкций, связанные с защитой персональных данных в государствах-членах ЕС к моменту применения Общего Регламента *GDPR*: в Германии компания LIDL была оштрафована на €1 460 000 (2008 г.); в Италии компания *Google* оштрафована на €1 000 000 (2013 г.); в Великобритании компания *TalkTalk* оштрафована на £400 000 (2016 г.); в Испании компания *Facebook* оштрафована на €1 200 000 (2017 г.). Отметим, что в большинстве стран-членов Евросоюза размеры штрафов значительно меньше, например, в Латвии – €4248; в Словакии – €8000; в Польше – €47 000.

26. Европейский совет по защите данных (EDPB) заменил с 25 мая 2018 г. Группу *WP29*, которая была создана в соответствии со ст. 29 Директивы 95/46/ЕС и действовала до 25 мая 2018 г., т.е. до момента применения в полном объеме Регламента GDPR. – URL: https://edpb.europa.eu (Дата обращения 18.08.2018). Примечательно, что 11 апреля 2018, т.е. до срока окончания своей деятельности, Группа *WP29* приняла решение создать Рабочую группу по социальным сетям (*Social Media Working Group*), которая наряду с EDPB призвана содействовать согласованному применению *GDRP* после 25 мая 2018 г.

27. Европейский инспектор по защите данных (*EDPS*). – URL: https://edps.europa.eu (Дата обращения 18.08.2018).

28. *GDPR Data Protection Supervisory Authority Listing.* URL: https://blog.varonis.com/gdpr-data-protection-authority-supervisory-listing/ (Дата обращения 18.08.2018).

29. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG (Дата обращения 18.08.2018). В силу «опосредованного» применения, Директива

2016/680 должна была быть имплементирована/транспонирована в национальное право стран-членов к маю 2018 г., и страны-члены должны были уведомить Еврокомиссию о принятии соответствующих национальных мер.

30. К таким актам, к примеру, относятся следующие: Рамочное решение Совета 2009/948/JHA 2009 г. о предотвращении и урегулировании конфликтов осуществления юрисдикции в уголовном процессе; Директива 2010/64/ЕС 2010 г. относительно права толкования и перевода в уголовном процессе; Директива 2012/13/ЕС 2012 г. о праве на информацию в уголовном процессе; Директива 2013/48/ЕС 2013 г. о праве доступа к адвокату в рамках уголовного процесса и Европейского ордера на арест (*European arrest warrant*), а также о праве информирования третьего лица в случае лишения свободы и общения с третьими лицами и с консульскими властями во время лишения свободы; Директива 2016/343 2016 г. по укреплению некоторых аспектов презумпции невиновности и права присутствовать на судебном процессе по уголовному делу и др.

31. *Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM/2018/226 final - 2018/0107 (COD).*– URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN (Дата обращения 18.08.2018).

32. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (COM (2018) 225).* – URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:225:FIN (Дата обращения 18.08.2018).

33. Предложения, скорее всего, будут приняты в ближайшей перспективе. – URL: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vkos7fgq52yj (Дата обращения 18.08.2018).

34. См., например, Регламент GDPR (преамбула (80), ст. 27 GDPR). Назначить законного представителя в т.ч обязаны поставщики услуг, не учрежденные в ЕС, но предлагающие услуги в ЕС, и такие требования закреплены, в частности, в Директиве 2016/1148 2016 г., касающейся мер по обеспечению высокого общего уровня безопасности сети и информационных систем в рамках всего Союза; Директиве 2000/31 о некоторых правовых аспектах услуг информационного общества, в частности, электронной торговли на внутреннем рынке (*e-Commerce Directive*); в Предложении для Парламента ЕС и Совета по Регламенту относительно уважения частной жизни и защиты персональных данных в электронных сообщениях и отмены Директивы 2002/58 / ЕС (*ePrivacy Regulation*) 2017 г. и др.

35. В Регламенте GDPR категоризация персональных данных, к примеру, специфицирована к «особым категориям персональных данных» – «*sensitive data*» (преамбула (11) GDPR).

36. В ЕС категория (принцип/концепция) «*EU's acquis*» (сокращенное от оригин. «*acquis communautaire*») представляет собой ключевой комплекс общих прав и обязательств, являющихся императивными для всех стран-членов ЕС. «*EU's acquis*» находится в постоянном развитии и включает в себя содержание, принципы и политические цели договоров; все законодательство, принятое во исполнение договоров ЕС, а также прецедентное право Суда ЕС; декларации и резолюции, принятые ЕС; меры, касающиеся общей внешней политики и политики безопасности; меры правосудия и внутренних дел; международные соглашения, заключаемые ЕС и заключаемые странами ЕС между собой в сфере деятельности ЕС. Условием присоединения к ЕС для стран-кандидатов является принятие «*EU's acquis*» в полном объеме. Отступление от «*EU's acquis*» предоставляется только в исключительных случаях и ограничено сферой применения. «*EU's acquis*» должен быть инкорпорирован странами-заявителями в их национальное право к дате их вступления в ЕС, и применимы с этой даты.

37. См. ст. 2 и ст. 3 Регламента GDPR.

38. В качестве примера можно назвать: *US Stored Communications Act, SCA* (18 U.S.Code § 2701 et seq.), об этом подробнее: *Lackey M. E., Pottinger O. D.* Stored Communications Act: Practical Consideration. – URL: https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2018/06/22/stored-communications-act-practical-considerations.aspx (Дата обращения 09.09.2018); *US Electronic Communication Privacy Act, ECPA* (18 U.S. Code § 2510 et seq.), об этом: Electronic Communication Privacy Act (ECPA). – URL: https://epic.org/privacy/ecpa/ (Дата обращения 09.09.2018); *Children's Online Privacy Protection Rule, COPPA* (U.S. Code §§6501-6506) – URL: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule/ (Дата обращения 09.09.2018) и др.

39. См. об этом, например: *Right to Privacy: Constitutional Rights & Privacy Laws.* – URL: https://www.livescience.com/37398-right-to-privacy.html (Дата обращения 09.09.2018) и др.

40. Такой «единый» законодательный акт, к примеру, принят в Канаде, как и США имеющей федеративное устройство, право которой в целом также относится к системе «общего права». См. *Canada Personal Information Protection and Electronic Documents Act, PIPEDA.* – URL: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ (Дата обращения 09.09.2018). «Личная информация» (*Personal Information*) является основным понятием, закрепленным в праве Канады.

41. *To amend title 18, United States Code, to improve law*

enforcement access to data stored across borders, and for other purposes – «Clarifying Lawful Overseas Use of Data Act», CLOUD Act. 2-я Сессия 115-й Конгресса США (2018 г.). – URL: https://www.congress.gov/bill/115th-congress/house-bill/4943 (Дата обращения 09.09.2018).

42. CLOUD Act достаточно критично оценивается, в частности, технологическими компаниями и правоведами США, а также европейскими юристами-международниками, поскольку он «несет ряд рисков», среди которых компрометация цифрового суверенитета других стран, коллидирование с защитой конфиденциальности в контексте применимых положений Регламента GDPR и др. Об этом: Ruiz D. *Microsoft Clears the Air About Fighting CLOUD Act* Abuses. – URL: https://www.eff.org/ru/deeplinks/2018/09/microsoft-clears-air-about-fighting-cloud-act-abuses (Дата обращения 09.09.2018); Nojeim G. *Cloud Act Implementation Issues.* – URL: https://www.lawfareblog.com/cloud-act-implementation-issues (Дата обращения 09.09.2018); Christakis T. Lost in the Cloud? Law-enforcement Cross-border Access to Data after the «***Clarifying Lawful Overseas Use of Data***» (*CLOUD*) Act and E-Evidence. – URL: https://observatoire-fic.com/en/lost-in-the-cloud-law-enforcement-cross-border-access-to-data-after-the-clarifying-lawful-overseas-use-of-data-cloud-act-and-e-evidence/ (Дата обращения 09.09.2018).

43. *California Consumer Privacy Act, CCPA.* – URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121/ (Дата обращения 09.09.2018).

44. California Consumer Privacy Act: The Challenge Ahead – Consumer Litigation and the CCPA: What to Expect – URL: https://www.hldataprotection.com/2018/09/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-consumer-litigation-and-the-ccpa-what-to-expect/ (Дата обращения 09.09.2018).

45. См., например, *Dennis D. Hirsch.* The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? 34 Seattle Uuniversity Law Review. 439. 2011. – URL: http://digitalcommons.law.seattleu.edu/sulr/vol34/iss2/3/ (Дата обращения 09.09.2018); *Monroe Edwin Price and Stefaan G. Verhulst.* Self-Regulation and the Internet. Kluver Law International. 2005. P. 14-18 и др.

46. См., например, *Jolly I.* Data protection in the United States: overview. – URL: https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1 (Дата обращения 09.09.2018).

47. См. также Micrisoft.

48. *ICANN Temporary Specification for gTLD Registration Data.* – URL: https://www.icann.org/en/system/files/files/advisory-statement-gtld-registration-dataspecs-17may18-en.pdf (Дата обращения 18.08.2018).

49. *Draft Framework for a Possible Unified Access Model to Full WHOIS Data.* – URL: https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf (Дата обращения 18.08.2018). Непубличные данные *WHOIS* (*Non-public WHOIS data*) охватывают персональные данные, включенные в элементы регистрационных данных. В частности, предполагается, что непубличные данные *WHOIS* должны быть удалены из общедоступных данных в *WHOIS*, в т.ч. имя и адрес электронной почты владельца регистрации.

50. *EU-US Privacy Shield Framework* – опубликовано в Федеральном реестре США (*Federal Register*), являющемся эквивалентом Официального журнала ЕС. – URL: https://www.privacyshield.gov/EU-US-Framework (Дата обращения 18.08.2018).

51. Решение Европейского суда о признании «недействительным» решения Еврокомиссии 2000/520/ЕС от 26 июля 2000 г. (*European Commission's Decision 2000/520/EC of 26 July 2000*). *Judgement of the Court (Grand Chamber) 6 October 2015.* – URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031 (Дата обращения 18.08.2018).

52. Martin A. Weiss M. A., Archick K. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. – URL: https://fas.org/sgp/crs/misc/R44257.pdf (Дата обращения 18.08.2018).

53. *Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences. Council Decision (EU) 2016/2220 (OJ L 336/1-2), 2 December 2016.* – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.336.01.0003.01.ENG (Дата обращения 18.08.2018).

54. *U.S.-EU «umbrella» Data Privacy and Protection Agreement, DPPA.* – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8 (Дата обращения 18.08.2018).

55. *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (*Strasbourg, 10/10/2018*). – URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223 (Дата обращения 18.08.2018). См. также Решение Еврокомиссии 2018/0237 (NLE) от 05.06.2018. – URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0449:FIN (Дата обращения 18.08.2018).

Угрозы доверия(ю)

Павел Храмцов

Основной тренд современного развития технологий – потеря доверия участников взаимодействия друг к другу. И это принципиальный момент, т.к. большинство современных технологий базируются именно на доверии. Собственно, весь Интернет – это, изначально, одно сплошное доверие.

Еще один важный момент в развитии современных коммуникационных технологий – это защита адресов и контактов.

Разберем несколько примеров, которые подтверждают приведенные выше тезисы. Как это ни выглядит парадоксальным, но и мир off-line, и мир on-line здесь во многом похожи.

Спекуляции – это плохо, или За что боролись, на то и напоролись!

В начале 2018 года были опубликованы и широко обсуждались аппаратные уязвимости современных микропроцессоров, используемые в Spectre[1] и Meldown[2].

Не вдаваясь глубоко в суть проблемы, можно констатировать, что ускорение производительности современных процессоров за счет спекулятивных вычислений привело к появлению аппаратной уязвимости, которая не может быть устранена без снижения производительности.

Но для начала разберемся с термином «спекулятивные вычисления». В 1974 году в журнале *EEE Journal of Solid State Circuits* группа авторов во главе с Робертом Деннардом (Robert H. Dennard) опубликовала статью «Design of Ion-Implanted MOSFET's with Very Small Physical Dimensions»[3]. Из статьи следовало, что миниатюризация элементной базы приводит к повышению быстродействия и снижению электропотребления. Данный закон получил название закона Деннарда.

Этот закон дал физическое обоснование другому закону – закону Мура. Фактически, работа Деннарда и его коллег задала направление развития вычислительной техники на 30 лет вперед.

Однако в 2005-2007 годах закон Деннарда перестал работать. Миниатюризация уперлась в физические ограничения. «Разогнать» обычный одноядерный процессор быстрее 4ГГц не удавалось. Быстродействие не росло, и появились архитектуры со многими ядрами.

Но еще до появления многоядерных архитектур была реализована возможность параллельных вычислений на аппаратном уровне, собственно закон Деннарда и позволял это сделать. Среди способов аппаратной реализации параллельных вычислений можно выделить внеочередное исполнение команд и спекулятивные вычисления.

При внеочередном исполнении команд команды исполняются в момент, когда имеется возможность их выполнить, а не по порядку, установленному в программе. Это означает, что процессор может выполнить некоторые команды, результаты которых могут и не понадобиться в будущем. Но если результат понадобится, то он уже будет готов к этому моменту.

Спекулятивное исполнение – это исполнение команд, результаты которых могут потребоваться в будущем с высокой вероятностью.

И в первом, и во втором случае происходят множественные обращения к страницам памяти. Для ускорения операций отображения виртуальной памяти в физическую существует специальный механизм кэширования такого соответствия. Уязвимости, которые эксплуатируют Spectre и Metdown, связаны с эксплуатацией особенности работы этого механизма.

Но собственно существование этого механизма и обеспечивает повышение быстродействия. Отказ от него (механизма) приводит к снижению скорости вычислений.

Это все прекрасно понимали, когда проектировали процессоры с возможностями измененного порядка выполнения команд и спекулятивным вычислениями. Теоретически уязвимость могла быть использована еще лет десять тому назад. Но попробовать реализовать уязвимость решили только 2017 году.

О чем это говорит? Разделение и защита образов процессов — это давно установленное правило. **Защита области ядра – это тоже давно установленное правило.** Все это принято называть безопасностью. Но безопасность бывает разная. Одно дело защита от непреднамеренных ошибок **— safety—** и другое дело — защита от преднамеренного воздействия — **security**.

Большинство современных компьютерных технологий разрабатывалось в эпоху действия парадигмы SAFETY. Анализ аппаратных платформ на предмет фундаментальных уязвимостей переводит нас в эпоху SECURITY.

И еще одно: и Meltdown, и Spectre эксплуатируют уязвимость, основанную на чтении адреса. Возможно, это совпадение, но ниже мы убедимся, что современный тренд безопасности – это защита адресов и контактов.

Феномен Telegram

13 апреля 2018 года Таганский суд Москвы вынес решение по иску Роскомнадзора о немедленной блокировке мессенджера Telegram[4]. С этого момента началась эпопея по обходу ограничения «доступа к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» и функционирование которых обеспечивается Telegram Messenger Limited Liability Partnership».

В результате выполнения решения суда по установке ограничений доступа со стороны Роскомнадзора в «черные списки» попали десятки миллионов IP-адресов. В том числе, например, адреса облачных сервисов Amazon и Digital Ocean.

Формально решение суда, чтобы ни говорила сетевая общественность, Роскомнадзор выполнил. Ограничение доступа, если подходить формально к букве постановления суда, было реализовано и действует до сих пор. Однако самым любопытным во всей этой истории является совсем не это.

Суд мотивировал свое решение отказом Telegram предоставить ключи для чтения контента. А противоборство между надзорным ведомством и Telegram развернулось вокруг маскирования адресной информации, т.е. адресов серверов Telegram.

Среди множества технологий такого маскирования следует выделить технологию репликации Telegram proxy-серверов (MTProto Proxy[5]). Собственно, сами серверы Telegram никуда не переезжают. Авария в голландских электросетях только подтвердила этот факт[6]. Разработчики Telegram предложили пользователям мессенджера специализированное программное обеспечение, которое может быть установлено в сети любого ISP.

Таким образом, учитывая формулировку суда, установка MTProto Proxy провоцирует блокировку сетей любого провайдера. Именно по этой причине под ограничения доступа и попали Amazon с Digital Ocean.

Фактически, Telegram запустил процесс построения добровольного «ботнета». В этой связи борьба за ключи шифрования перешла в плоскость борьбы за реальные адреса, которые использует сервис. Telegram защищает/маскирует свои адреса и тем самым сохраняет работоспособность сервиса.

Это странное слово – «GDPR»

Теперь от адресов программ перейдем к данным, которые позволяют однозначно идентифицировать персону, то бишь обычных людей. К защите персональных данных, в том числе и персональных контактов.

С 25 мая 2018 года в силу вступила директива Европейского союза по защите данных (General Data Protection Regulation[7]). В основном она касается правил обработки персональных данных граждан Европейского Союза.

Особое значение этой директиве придают следующие особенности: она носит экстерриториальный характер, она предполагает право на забвение и она предполагает огромные штрафы (до 20 000 000 евро или 4% годового оборота) для любой компании в мире, которая будет замечена в нарушении Директивы.

Дилемма, которая возникает при реализации GDPR, – это противоречие между требованиями правоохранителей различных стран мира по поводу свободного доступа к персональным данным физических лиц с целью противодействия деяниям, угрожающим общественной безопасности, и защитой этих самых персональных данных от доступа к ним неограниченного круга лиц.

На самом деле, национальных законов, защищающих персональные данные граждан, почти столько же, сколько стран. В рамках этих законов доступ к данным так или иначе отрегулирован.

Например, для сервиса WHOIS в домене .ru данные физического лица скрыты фразой «Private person»:

domain:	TRAVELN.RU
nserver:	ns1.expired.reg.ru.
nserver:	ns2.expired.reg.ru.
state:	REGISTERED, DELEGATED, VERIFIED
person:	Private Person
registrar:	REGRU-RU
admin-contact:	http://www.reg.ru/whois/admin_contact
created:	2017-06-26T07:14:10Z
paid-till:	2018-06-26T07:14:10Z
free-date:	2018-07-27
source:	TCI

Получить персональные данные администратора домена в .ru можно, например, либо по решению суда, либо в соответствии с законом об «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ.

Для того, чтобы оценить влияние GDPR на управление пространством доменных имен, достаточно сказать, что половина заседаний секции очередной конференции ICANN[8] была посвящена одному вопросу – как жить в этих условиях дальше. Однако, по порядку.

Семь лет назад организация NORC at the University of Chicago по контракту с ICANN провела анализ достоверности данных WHOIS[9]. Исследовалась возможность получения обратной связи от администратора домена, а также досто-

верность предоставляемой информации администратором домена для хранения в реестре.

Исследовались в основном домены верхнего уровня общего назначения .com, .net, .org, .biz, .info (суммарно чуть более 98% от общего числа доменов в выборке). Было установлено, что корректно данные администратора домена были указаны только в 23,9% случаях. Абсолютная невозможность связаться с администратором домена была выявлена только в 7,8% случаев. Для понимания общей картины эти цифры требуют разъяснения.

Регистрация в доменах, которые исследовала NORC, носит уведомительный характер, собственно, так же, как и в российских национальных доменах .ru и .рф. Это значит, что необходимым условием регистрации и обслуживания домена является возможность контакта регистратора и администратора домена.

Остальные параметры, хоть и являются важными, и прописаны в договоре между регистратором и администратором домена, являются опционными, т.е. обслуживание клиента на том основании, что эти параметры отсутствуют, не прекращается.

Невозможность контакта была оценена исследователями в величину, равную менее 8% от общего количества исследованных доменов, что является по любым меркам довольно малой величиной.

Тем не менее, точность данных WHOIS была признана катастрофически недостаточной. Данных не хватало для идентификации администраторов доменов, т.е. для надежного установления адреса администратора.

Понятно, что это нужно только для поддержки «безопасности и стабильности» работы системы, т.е. прямого отношения к технологии DNS не имеет. О чем и было замечено в отчете Комитета советников ICANN по безопасности и стабильности (SAC058) от 27 марта 2013 года[10].

С момента появления этого отчета в IETF была начата разработка нового протокола Registration Data Access Protocol (RDAP)[11], который должен был заменить старый протокол WHOIS. Новый протокол обеспечивал также структуризацию данных и простоту автоматической обработки запросов.

В марте 2015 года он был утвержден в качестве стандарта. Его отличие от традиционного WHOIS в формате запросов и ответов (это RESTFul протокол) и детализации персональных данных администраторов доменов.

После опубликования протокола обязательное требование поддержки RDAP появляется в перезаключаемых контрактах gTLD и в программе new gTLD[12].

Все аккредитованные в ICANN регистраторы теперь обязаны поддерживать этот протокол и обеспечивать полноту данных, которые передаются в реестры. Эти же данные попадают в резервные файлы data escrow.

Кроме того, все эти данные могут быть доступны в публично в сервисах реестра (Registration Data Directory Services). Никакого ограничения или особых условий доступа в контрактах прописано не было.

Параллельно с этой историей в ICANN задумались об аккредитации privacy и proxy-сервисов[13], которые могут использоваться для сокрытия контактов администраторов доменов. Данный пункт предполагалось включить во все контракты регистраторов. При обсуждениях этой политики в рабочих группах все уперлось в раскрытие информации по запросам правоохранительных органов.

Кроме того, с 1 мая 2018 года предполагалось начать новые регистрации в формат «толстого» реестра для доменов .com, .net и .job. Это тоже важно для понимания значения GDPR.

Все дело в том, что реестры доменов до настоящего времени в зависимости от объема и типа хранящихся в них данных делят на «толстые» и «тонкие».

«Тонкий реестр хранит только техническую информацию о домене (домен, регистратор, даты начала и окончания регистрации и серверы, на которых домен делегирован). Данных об администраторе домена в «тонком» реестре не хранится. В этом случае все данные об администраторе домена хранятся у регистратора.

«Толстый» реестр хранит не только технические данные домена, но и данные его администратора.

Перевод реестров из формата «тонкого» реестра в формат «толстого» реестра предполагает, что все данные администраторов домена регистратор передаст третьей стороне – реестру, а также оператору резервной копии реестра (data escrow).

И еще. В январе 2018 года ICANN в очередной раз вернулся к вопросу применения правил трансляции и транслитерации контактной информации для сервиса RDDS и протокола RDAP.

Таким образом, можно констатировать, что с одной стороны ICANN стремилась к повышению точности контактной информации в реестрах, а с другой, доступ к этой информации никаким общим документом не описывался.

Появление GDPR привело к тому, что 17 мая 2018 года ICANN вынуждена была выпустить «Временную спецификацию для регистрационных данных gTLD»[14], которая вступила в силу с 25 мая 2018 года (начало действия GDPR).

Издание этого документа не принесло каких-либо открытий. Например, многие рекомендации Временной спецификации в части отображения персональных данных в WHOIS практически дословно повторяют правила регистрации в доменах .ru и .рф. Также для целей анонимизации данных предлагается процедура хеширования персональных данных, которая во многом похожа на ту, что используется в проекте «Нетоскоп» Координационного Центра национального домена сети Интернет[15].

Данная история – это демонстрация двух основных тенденций развития Интернета. С одной стороны, защита частной жизни, а с другой - защита общественной безопасности. И ключевую роль в этом конфликте играют адреса и контакты, а точнее, их защита и правила раскрытия.

Ссылки

1. https://spectreattack.com/spectre.pdf

2. https://meltdownattack.com/meltdown.pdf

3. https://www.ece.ucsb.edu/courses/ECE225/225_W07Banerjee/reference/Dennard.pdf

4. https://www.mos-gorsud.ru/rs/taganskij/services/cases/civil/details/2cc72aea-39e7-4f8e-adc9-37d170966efa?caseNumber=02-1779/2018

5. https://hub.docker.com/r/telegrammessenger/proxy/

6. https://twitter.com/durov/status/990371212877549568

7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

8. https://62.schedule.icann.org/

9. https://www.icann.org/en/system/files/newsletters/whois-accuracy-study-17jan10-en.pdf

10. https://www.icann.org/en/system/files/files/sac-058-en.pdf

11. https://www.rfc-editor.org/search/rfc_search_detail.php?title=RDAP&pubstatus%5B%5D=Any&pub_date_type=any

12. https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf (Specification 4)

13. https://gnso.icann.org/sites/default/files/file/field-file-attach/pdp-update-20feb18-en.pdf

14. https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-ru.pdf

15. https://netoscope.ru/ru/about/

Безопасность и современные тренды

Павел Храмцов

В последнее время популяризация технологических новаций Интернета превратилась в популяризацию страхов и угроз.

Создается впечатление, что практически каждый из известных протоколов Интернета либо уже обзавелся своей защищенной версией, либо прямо сейчас эту версию активно обсуждают в одной или нескольких рабочих группах IETF.

Кроме того, если раньше из-за ошибки программирования мог разбиться о поверхность Марса спутник[1] или взорваться ракета «Ариан-5»[2], то сейчас ошибки такого рода начинают затрагивать миллионы «гражданских».

Как защищаются от «подглядывания» и ошибок в современных технологиях; как берегут персональные и не только данные; как противостоят не только софтверным, но и аппаратным атакам? Рассмотрим эти вопросы подробнее на нескольких примерах.

Монополизация DNS: браузеры и лидеры рынка атакуют

В середине октября 2018 года в Амстердаме прошел очередной семинар сообщества DNS-OARC[3]. Как обычно, темы семинара были актуальны и интересны, но одну из тем, тему инкапсуляции протоколов DNS в TLS (DNS over TLS – DoT)[4] и HTTPS(DNS over HTTPS – DoH)[5], хотелось бы выделить отдельно. Но прежде обратимся к классическому сервису DNS.

DNS - это сервис сопоставления легко запоминаемого имени и трудно запоминаемого адреса. В этом суть. С переходом на IPv6 роль трансляции имени в адрес и наоборот стала еще более важной.

Внешне, скажем, в вебе, это выглядит так: пользователь в адресной строке вводит доменное имя и за доли секунды получает необходимый контент.

Вся «кухня» отображения имени в адрес от пользователя скрыта. А процедура эта непростая, и как в любой непростой технологии, в ней возможны ошибки и преднамеренное искажение соответствия.

Эти «тонкости» могут привести к тому, что конечный пользователь может оказаться в «параллельной реальности», т.е. получить совсем не тот контент, который он предполагал получить.

Таким образом, решение проблемы состоит в том, чтобы удостоверить источник DNS-информации.

С этой целью в систему DNS было имплементировано расширение, которое известно под названием «DNSSEC»[6]. Казалось бы, все в порядке – сторонние злоумышленники не смогут обмануть доверчивых пользователей.

Проблема возникла совершенно с противоположной стороны. В эпоху тотальной защиты персональных данных (чего стоит только директива GDRP[7]) встал вопрос защиты самого DNS-трафика от посторонних глаз.

В первую очередь речь идет о защите DNS-запросов на пути от конечного пользователя к резолверу, который выполняет поиск IP-адреса в системе DNS. Обычно это тот самый DNS-сервер, адрес которого присылается по протоколу DHCP[8] при подключении компьютера к сети.

Но в последнее время стало модно отказываться от DNS-резолвинга своего собственного провайдера и прописывать в качестве резолвера DNS-серверы Yandex (77.88.8.8), Google (8.8.8.8), CloudFlare (1.1.1.1). Все они предлагают дополнительные возможности по управлению резолвингом, но при этом запросы пользователя «уходят в плавание» по Интернету.

Для защиты от «подсматривания» DNS-провайдеры предлагают различные технологии шифрования. Yandex, например, DNSCRYPT (Cisco – OpenDNS), в то время, как Google и CloudFlare стараются опереться на предлагаемые в RFC более общие стандарты DoT и DoH.

В обоих случаях при обработке запросов используется транспорт TCP. Об UDP речи не идет вообще. В случае DoT используется порт 853, а в случае DoH - стандартный 443 порт.

Различия подходов прекрасно описаны Джефом Хюстоном в блоге APNIC[9]. В первом случае DNS просто «заворачивается» в защищенное TCP-соединение. Второй случай гораздо интереснее, так как сам запрос и ответ могут быть представлены в виде традиционных сообщений HTTP.

На рисунке 1 приведен пример резолвинга с использованием протокола DoH и JSON-форматом запросов и ответов.

Рис. 1. Пример резолвинга с использованием протокола DoH и JSON-форматом запросов и ответов.

```
curl -s -H 'accept: application/dns+json' 'https://dns.google.com/resolve?name=kremlin.ru&type=A' | jq
> GET /resolve?name=kremlin.ru&type=A HTTP/2
> Host: dns.google.com
> User-Agent: curl/7.54.0
> accept: application/dns+json
>
* Connection state changed (MAX_CONCURRENT_STREAMS updated)!
< HTTP/2 200
< strict-transport-security: max-age=31536000; includeSubDomains; preload
< date: Mon, 15 Oct 2018 12:11:26 GMT
< expires: Mon, 15 Oct 2018 12:11:26 GMT
< cache-control: private, max-age=59
< content-type: application/x-javascript; charset=UTF-8
< server: HTTP server (unknown)
< x-xss-protection: 1; mode=block
< x-frame-options: SAMEORIGIN
< alt-svc: quic=":443"; ma=2592000; v="44,43,39,35"
< accept-ranges: none
< vary: Accept-Encoding
<
{ [379 bytes data]
* Connection #0 to host dns.google.com left intact
{
  "Status": 0,
  "TC": false,
  "RD": true,
  "RA": true,
  "AD": false,
  "CD": false,
  "Question": [
    {
      "name": "kremlin.ru.",
      "type": 1
    }
  ],
  "Answer": [
    {
      "name": "kremlin.ru.",
      "type": 1,
      "TTL": 59,
      "data": "95.173.136.70"
    },
    {
      "name": "kremlin.ru.",
      "type": 1,
      "TTL": 59,
      "data": "95.173.136.72"
    },
    {
      "name": "kremlin.ru.",
      "type": 1,
      "TTL": 59,
      "data": "95.173.136.71"
    }
  ],
  "Comment": "Response from 194.226.127.212."
}
```

Собственно, в последнем случае мы уже не имеем традиционного DNS-сервиса. Все может быть «упаковано» в пользовательское приложение (браузер или мобильное приложение). Специализированные средства DNS на компьютере конечного пользователя не нужны.

Собственно, именно этот момент и стал предметом обсуждения доклада Сары Дикенсон (Sara Dickinson)[10] на семинаре DNS-OARC.

Во-первых, браузер или приложение могут сами отправлять и принимать запросы по встроенным адресам резолверов.

Во-вторых, использование стандартного 443 порта существенно затруднит блокировку именно DNS-запросов. Во всяком случае, потребуется анализ TCP-пакетов.

В-третьих, число DNS-провайдеров может сократиться в разы. В-четвертых, схема с корневыми удостоверяющими центрами начинает работать и для DNS.

На самом деле мы видим уплощение стека сервисов, который стремительно превращается в браузер/почтовый клиент/клиент системы мгновенных сообщений и т.п. – одним словом, в приложение. По сути, в пределе «прости-прощай», концепция открытой системы.

С защитой персональных данных связан еще один вопрос, который не столь бурно обсуждается инженерным сообществом, – это необходимость передавать исходный запрос конечного клиента по всей цепочке рекурсивного поиска.

Еще в 2016 году Стефан Бортцмаер (Stephane Bortzmeyer)[11] поднимал вопрос об отсутствии необходимости передавать полный DNS-запрос от рекурсивного резолвера всем авторитетным серверам вплоть до серверов, которые поддерживают root (корень системы DNS).

Суть вопроса в том, что соответствие полного доменного имени и IP-адреса знает только авторитетный сервер той зоны, в которой установлено это соответствие. Все остальные серверы присылают только ссылки на следующий за ними сервер в рекурсивной цепочке.

Встает резонный вопрос – для чего им знать, какой конкретный домен интересует конечного пользователя.

Для того, чтобы прислать адрес авторитетного сервера соответствующей зоны, нужно знать только часть полного доменного имени. Например, возьмем имя:

Dns.example.ru

Авторитетным серверам корня нужно знать только то, что пользователи ищут что-то в зоне .ru. Передавать им полный запрос совершенно нет никакой необходимости. Но сейчас запрос передается целиком.

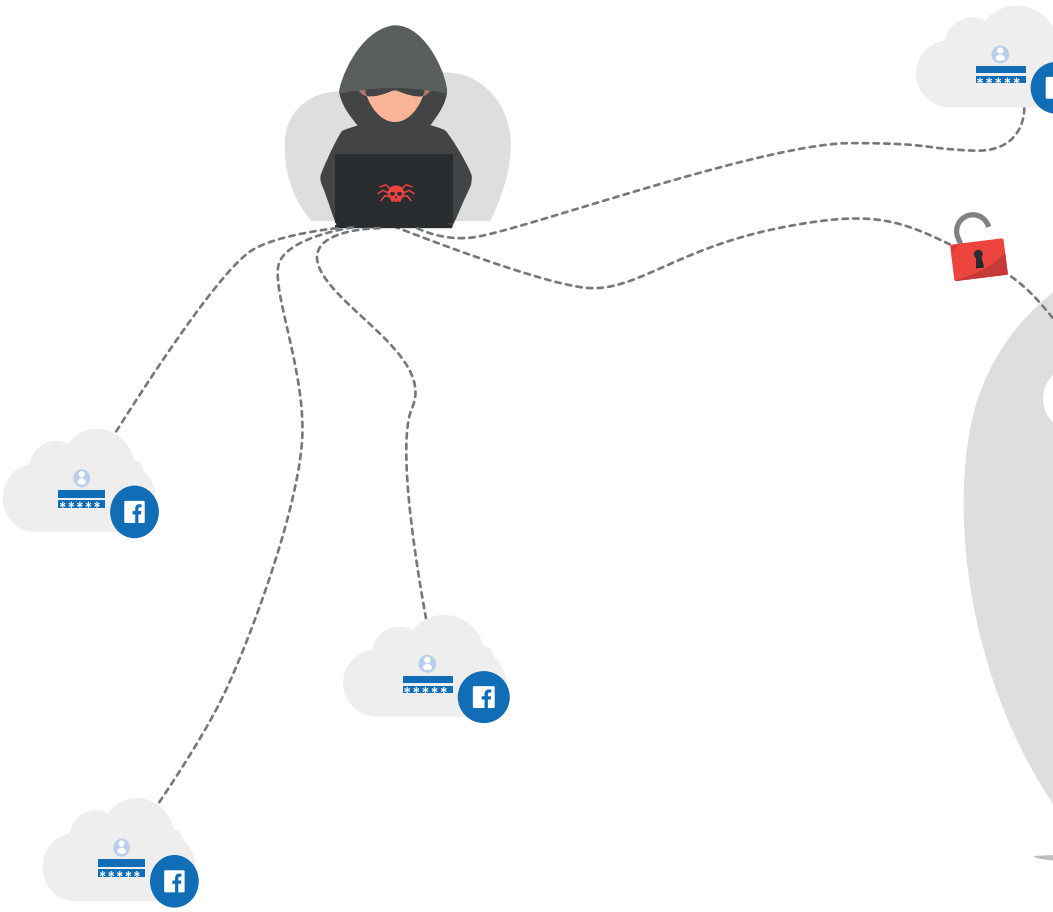
Клуб операторов корневых серверов невелик. Правил, как войти в него, нет. Статистика запросов, которые получают авторитетные серверы, по понятным причинам является чрезвычайно ценной. Видимо, по этой же причине документ Бортцмаера широкой поддержки до сих пор не нашел, в отличие от усилий DNS-провайдинга резолвинга (Google и CloudFlare).

Facebook и скомпрометированные аккаунты

Персональные данные могут «утекать» не только в виде «БигДаты», как это рассмотрено выше в случае с DNS. Все может быть гораздо прозаичнее.

Например, 28 сентября 2018 года соцсеть Facebook объявила[12] о том, что в результате уязвимости в режиме просмотра «View As» пострадало около 50 миллионов аккаунтов пользователей.

Согласно отчету Facebook, уязвимость стала результатом совокупности трех ошибок:



Во-первых, «View As» должен быть реализован только в виде интерфейса просмотра. Однако в одном из режимов просмотра была реализована посылка видео с поздравлением ко дню рождения.

Во-вторых, в версии загрузчика изображений для мобильных устройств был реализован режим с получением токена доступа, который используется вместо ввода логина и пароля при доступе к аккаунту.

В-третьих, в режиме просмотра «View As» для загрузчика изображений генерировался токен доступа от лица владельца стороннего аккаунта, а не от лица владельца аккаунта, который использует режим «View As».

Сам токен можно было получить, просмотрев HTML-страницу. Это позволяло зайти на чужую страницу и проделать все операции по получению нового токена заново. В итоге аккаунты посторонних лиц, их друзей, друзей этих друзей и т.п. оказались взломаны.

Типичное проявление «горя от ума» - нужно было попасть в чужое окружение, в котором оказался доступен и токен доступа.

В настоящее время возможность «View As» отключена. Кроме 50 миллионов пострадавших аккаунтов, Facebook переустановила токены еще 40 миллионам пользователей, которые, возможно, применяли режим «View As».

Вопрос с утечкой персональных данных Facebook гораздо интереснее, чем может показаться на первый взгляд. В настоящее время мы являемся современниками процесса отказа от традиционной парадигмы идентификации по логину и паролю.

Вместо них предлагается использовать двухфакторную идентификацию с возможностями биометрии. Аргументы просты: пароли вечно забывают, их надо регулярно менять и они не обладают достаточной стойкостью ко взлому.

Случай Facebook показывает, что проблема глубже. Полученные с помощью современной идентификации токены тоже нужно менять, а из системы время от времени нужно выходить. Но если эта парадигма на настольных компьютерах еще как-то работает, то в мобильных приложениях это не столь очевидно и удобно. Да и биометрия не является панацеей.

Встык с «утечкой» из Facebook оказалось еще одно событие – поломка сервиса Yale[13]. Здесь речь уже идет не об утере персональных данных. Все гораздо интереснее.

Мы имеем дело с мобильным приложением, которое управляет охраной жилища и «умными» ключами. Ключами в смысле отпирания замков, а не криптографии.

Вообще, британские любители продвинутых технологий в «умных» домах оказались в сложной ситуации. Безусловно, «умные» устройства можно было открыть и закрыть при помощи предлагавшихся к ним пультов, но кто же в «умных» технологиях помнит дополнительные пин-коды.

Собственно, и случай с Facebook, и случай с Yale заставляют нас помнить, что живем мы в офлайновом мире, где информация из онлайна может быть использована отнюдь не виртуально.

К слову, директива GDPR уже действует. Будет ли она применена к Facebook? Вот что интересно.

Китайцы и их чипы

И уж совсем не виртуально выглядят миниатюрные микросхемы, о которых 4 октября 2018 Блумберг[14] опубликовал большую статью.

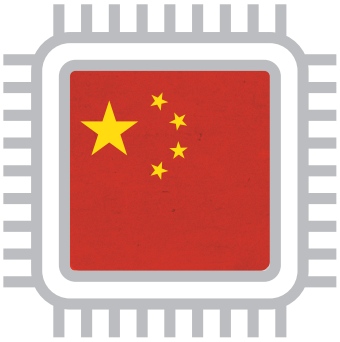
Дело в том, что в аппаратуре Super Micro Computer Inc. были найдены чипы-закладки, которые поместили туда специально обученные китайцы.

Согласно информации агентства, все началось еще весной 2015 года, когда компания Amazon в рамках использования ее платформы AWS в целях национальной безопасности отправила несколько серверов на исследование в Канаду.

Исследователи обнаружили сторонние микрочипы в серверах для министерства обороны, в аппаратуре для ЦРУ и в оборудовании для корабельных сетей ВМФ.

Чипы позволяли реализовать «бэкдор» и были установлены в оборудование на заводах, а заводы эти были китайские.

Китайцы собирают комплектующие для 70% всех мобильных устройств и 90% всех персональных компьютеров. Было бы странным, если бы они не воспользовались этим своим уникальным положением в деликатных целях.



По данным Блумберг, пострадало почти 30 американских компаний, включая банки, правительственные учреждения, компании-мейджоры, например, такие, как Apple и Amazon.

Установить источник атаки в случае аппаратной закладки в некотором смысле проще, чем в случае с программным обеспечением. Оборудование поставляется по накладным с определённых предприятий. Всю цепочку поставок можно проследить.

Любопытно, что согласно утверждениям американских экспертов, в США существует программа контроля цепочек поставки для чувствительных областей: обороны и национальной безопасности[15]. При этом проблема надежных поставщиков существовала всегда. И всегда экономика побеждала сомнения в надежности и безопасности поставщика.

Что же мы имеем в сухом остатке в этой истории

Во-первых, проблема импортозамещения, оказывается, актуальна не только для нас. Во-вторых, во избежание неожиданностей министерство обороны США запретило использовать сотовые телефоны производства ZTE и Huawey на американских военных объектах.

В-третьих, министерство торговли США чуть было не запретило на семь лет импорт продукции ZTE в Штаты.

Специалисты утверждают, что ни один частный предприниматель, а тем более частное лицо от действий китайцев не пострадали, т.к. Китай рассчитывал на отложенный эффект внедрения своих чипов. Всем остается только на это надеяться – Supermicro является крупнейшим поставщиков материнских плат в мире. Все их разом не заменишь.

Ссылки

1. http://exploration.esa.int/mars/47852-entry-descent-and-landing-demonstrator-module/

2. http://esamultimedia.esa.int/docs/esa-x-1819eng.pdf

3. https://indico.dns-oarc.net/event/29/contributions/speakers

4. https://tools.ietf.org/html/rfc7858

5. https://tools.ietf.org/html/draft-ietf-doh-dns-over-https-14

6. https://tools.ietf.org/html/rfc4033

7. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

8. https://www.ietf.org/rfc/rfc2131.txt

9. https://blog.apnic.net/2018/10/12/doh-dns-over-https-explained/

10. https://indico.dns-oarc.net/event/29/contributions/649/attachments/637/1024/OARC29_Encrypted_DNS.pdf

11. https://tools.ietf.org/html/rfc7816

12. https://newsroom.fb.com/news/2018/09/security-update/

13. https://twitter.com/YaleSecurity/status/1050048180161789952

14. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2

15. https://krebsonsecurity.com

Новости Доменной индустрии

Важные события 2018

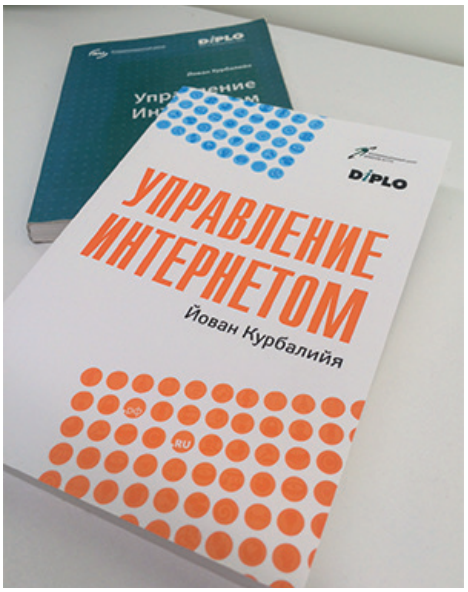
Безопасность

«ДОКТОР ВЕБ» СТАЛ НОВОЙ КОМПЕТЕНТНОЙ ОРГАНИЗАЦИЕЙ ПРИ КООРДИНАЦИОННОМ ЦЕНТРЕ ДОМЕНОВ .RU/.РФ

20.07.2018

Координационный центр доменов .ru/.рф и компания «Доктор Веб» подписали соглашение, в соответствии с которым «Доктор Веб» как признанный эксперт в области информационной безопасности становится одной из компетентных организаций при Координационном центре.

Институт компетентных организаций при Координационном центре занимается сбором и анализом информации об интернет-ресурсах, которые используются для распространения вредоносного ПО, фишинга, управления бот-сетями и других видов противоправной деятельности. В том случае, если компетентная организация обнаруживает такой ресурс самостоятельно или на основании обращения конечного пользователя, она направляет аккредитованному в доменах .ru/.рф регистратору запрос о снятии домена с делегирования, для прекращения, таким образом, использования доменного имени в противоправных целях.



КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ ПЕРЕИЗДАЕТ КНИГУ «УПРАВЛЕНИЕ ИНТЕРНЕТОМ»

19.09.2018

Книга Йована Курбалийи «Управление Интернетом» была впервые издана на русском языке в 2010 году, инициатором, спонсором и популяризатором выхода книги стал Координационный центр национального домена сети Интернет. Выпуск книги был приурочен к проведению Первого российского форума по управлению Интернетом (RIGF 2010). Тогда было переведено третье издание книги, причем тираж дважды допечатывался – настолько она оказалась популярной среди самых разных групп интернет-пользователей.

В 2018 году Координационный центр доменов .ru/.рф принял решение о переиздании книги, сделав новый перевод уже седьмого издания бестселлера Diplo. Объем книги за прошедшие восемь лет вырос почти в два раза, в книге отражены самые современные тенденции в управлении Интернетом, описываются предметы и явления, о которых в 2010 году еще никто даже не задумывался. Онлайн-версия книги уже доступна всем интернет-пользователям на сайте Координационного центра. Бумажное издание книги выйдет в ноябре 2018 года и будет распространяться на различных отраслевых конференциях и форумах интернет-сообщества.

НА TLDCON 2018 ПРЕДСТАВЛЕНЫ НАПРАВЛЕНИЯ РАБОТЫ КООРДИНАЦИОННОГО ЦЕНТРА ДОМЕНОВ .RU/.РФ НА 2019-2021 ГОДЫ

12.09.2018

В Юрмале (Латвия) 12 сентября открылась 11-я Международная конференция администраторов и регистраторов национальных доменов верхнего уровня стран СНГ, Центральной и Восточной Европы (TLDCON 2018), организованная Координационным центром доменов .ru/.рф при поддержке Технического центра Интернет, ICANN и NIC.LV. В конференции приняли участие более 120 специалистов доменной индустрии из России, Латвии, США, Канады, Ирландии, Чехии, Армении, Белоруссии, Казахстана, Украины, Сербии и других стран. Главные темы 2018 года – безопасность доменного пространства, взаимоотношения между доменной индустрией и правообладателями, развитие национальных доменов, DNS и новые технологии.

Продолжается формализация отношений Координационного центра с Техническим центром Интернет. «Новый Технический центр Интернет входит в Группу компаний «Ростелеком», и, естественно, у нас выстраиваются несколько другие отношения. На сегодняшний день между министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, ПАО «Ростелеком» и АНО «Координационный центр национального домена сети Интернет» подписан меморандум, который регулирует взаимоотношения в области построения и развития инфраструктуры российских доменов», – рассказал глава КЦ Андрей Воробьев.

Большое внимание в своем выступлении директор Координационного центра уделил работе с компетентными организациями. Он представил всех участников и рассказал, какова специализация каждой из компаний в области обеспечения кибербезопасности. Воробьев отметил, что институт компетентных организаций делает саморегулирование отрасли эффективным и оперативным.

Не осталась без внимания и тема прошлогоднего повышения цен на регистрацию и продление доменных имен, которое, как считают эксперты, повлияло на снижение темпов роста российских доменных зон .ru и .рф. «Есть и другие причины для снижения числа регистраций – малый и средний бизнес отказывается от того, что не используется в работе в данный момент, в том числе и от доменных имен, зарегистрированных «про запас». Но в целом тенденции на рынке положительные, и начало делового сезона показывает осторожный рост регистраций», – отметил Воробьев.

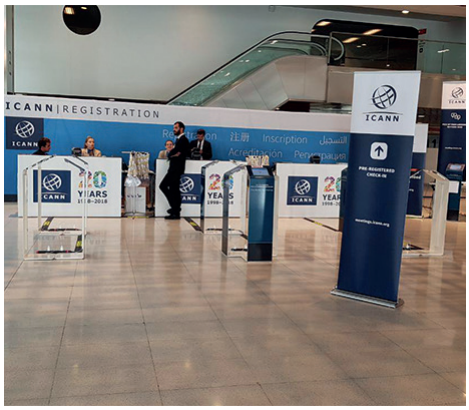
Топвизор

Новый регистратор

АККРЕДИТОВАН НОВЫЙ РЕГИСТРАТОР ИЗ САНКТ-ПЕТЕРБУРГА

04.10.2018

Координационный центр доменов .ru/.рф подписал соглашение об аккредитации с ООО «Топвизор» из Санкт-Петербурга. Статус аккредитованного регистратора предоставлен компании 6 сентября 2018 года. ООО «Топвизор» стало 46-м регистратором, аккредитованным в доменах верхнего уровня .ru и .рф, и седьмым регистратором в Санкт-Петербурге.



В ЦЕНТРЕ ВНИМАНИЯ ICANN 63 – БЕЗОПАСНОСТЬ, NEW GTLD, ПОЧТОВЫЕ СЕРВИСЫ ДЛЯ IDN

30.10.2018

Завершилась 63-я встреча ICANN, походившая на прошлой неделе в Барселоне. Во время мероприятия обсуждались многие актуальные вопросы развития мирового доменного пространства. Делегация Координационного центра доменов .ru/.рф активно участвовала в обсуждениях и дискуссиях на полях встречи, российские эксперты обменялись опытом и лучшими практиками с зарубежными коллегами.

Важное обсуждение, вызвавшее бурю эмоций у некоторых национальных делегаций, проходило на заседании Правительственного консультативного комитета (GAC). В центре внимания оказалась возможная отмена процедуры уведомления национальных правительств о регистрации двухбуквенных доменов, совпадающих с обозначениями стран, на втором уровне в новых доменных зонах. Против отмены процедуры уведомления на нынешнем заседании GAC резко выступили делегации Китая и ОАЭ, обсуждение будет продолжено.

На секции ISPCP, организованной рабочей группой ICANN по взаимодействию с интернет-операторами и точками обмена трафиком, представитель Канады рассказал, что одна из главных проблем страны в этой области – локализация трафика. На встрече Комитета по стабильности работы корневых серверов RSSAC обсуждался вопрос с дополнительным финансированием программы размещения управляемых ICANN L-серверов. По заявлению технического директора ICANN Дэвида Конрада, атаки на серверы растут практически экспоненциально, и проблема больше не может решаться старыми методами. По мнению Конрада, сегодня добиться положительных результатов, просто увеличив количество серверов и расширив полосу пропускания к ним, невозможно. Сейчас активно обсуждается вопрос о возможном выделении денег также и другим операторам корневых серверов для этих же целей.

Также на ICANN 63 было сообщено, что инициатива по открытым данным (Open data initiative) прошла тестовый период и сейчас превращается в рабочий Open data project. При помощи этого механизма ICANN будет давать расширенную статистику по новым и старым общим доменам верхнего уровня, в том числе данные, которые стали доступны в результате работы проекта DAAR (Domain Abuse Activity Report), исследующего использование доменных имен для зловредных целей. Данные будут обезличенными, в виде обобщенной статистики.

Наконец, на секции, посвященной интернационализированным доменам и программе Universal Acceptance, участникам рассказали, что компания Microsoft реализовала поддержку интернационализированных имен в своем самом популярном почтовом продукте – Outlook.

«На ICANN 63 были подняты вопросы, важные для российских интернет-пользователей. Например, полноценная поддержка программой Outlook почты на нелатинских доменах, несомненно, окажет положительное влияние на рост и развитие российского кириллического домена .рф. Не менее чувствительны для нас вопросы безопасности доменного пространства, которыми сейчас занимаются многие страны, и мы также готовы внести свой вклад в общее дело. В целом очередная встреча ICANN прошла очень насыщенно и продуктивно», - рассказал директор Координационного центра доменов .ru/.рф Андрей Воробьев.

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

.RU и .РФ

ДЛЯ ВЗАИМОДЕЙСТВИЯ РЕГИСТРАТОРОВ И КОМПЕТЕНТНЫХ ОРГАНИЗАЦИЙ СОЗДАНА ИНФОРМАЦИОННАЯ СИСТЕМА

01.11.2018

30 октября в бизнес-пространстве Deworkacy прошла рабочая встреча аккредитованных регистраторов с компетентными организациями, сотрудничающими с Координационным центром доменов .ru/.рф. Главной темой обсуждения стала информационная система, созданная Координационным центром для автоматизации взаимодействия компетентных организаций и регистраторов. Участники обсудили первые итоги работы с системой и высказали предложения по ее доработке и расширению функционала.

По словам руководителя специальных проектов Координационного центра Евгения Панкова, новая система уже помогла повысить эффективность взаимодействия компетентных организаций с регистраторами: «Система работает 3,5 месяца, за это время в системе было обработана более 2300 обращений, и у нас была возможность убедиться в том, что она существенно ускоряет и облегчает работу. Она позволяет собирать заявки в едином формате, благодаря чему обработка идет существенно быстрее».

СТАРТОВАЛ VII ВСЕРОССИЙСКИЙ ОНЛАЙН-ЧЕМПИОНАТ «ИЗУЧИ ИНТЕРНЕТ – УПРАВЛЯЙ ИМ»

07.11.2018

Координационный центр доменов .ru/.рф и «Ростелеком» сообщают о начале VII Всероссийского онлайн-чемпионата «Изучи Интернет – управляй им». Для участия в нем зарегистрировались больше 11 тысяч ребят, при этом 2800 из них объединились в 440 школьных команд со всей страны.

Участникам Чемпионата предстоит за 60 минут выполнить задания разного уровня сложности. Главная тема этого года – технологии будущего: робототехника, искусственный интеллект, интернет вещей, блокчейн, виртуальная и дополненная реальность, телемедицина и кибербезопасность.

Турнирный модуль чемпионата открыт для зарегистрированных участников до 30 ноября 2018 года на официальном сайте проекта.

По итогам соревнований три лучших участника в индивидуальном зачете и три сильнейших школьных команды получат заслуженные награды.

Календарь событий: 2018 - 2019 год

Международные события

15 января 2019
UKNOF42,
Лондон, Великобритания

Изначально созданная как встреча сетевых операторов Великобритании, UKNOF (United Kingdom Network Operators' Forum) выросла в международную конференцию, хотя и не утратила национальной специфики. Основные темы конференции типичны для глобальных операторских встреч - передовые практики, новые технологии и, конечно, вопросы безопасности. Эта однодневная встреча в этот раз проходит в Лондоне. https://indico.uknof.org.uk/event/44/

18-28 февраля 2019
APRICOT,
Тэджон, Южная Корея

APRICOT - крупнейшая ежегодная конференция по интернет-технологиям, собирающая более 800 участников Азиатского региона и Океании. Здесь обсуждаются вопросы внедрения и использования интернет-технологий, технического администрирования сетей и инфраструктурных услуг Интернета. Особое внимание уделяется образовательной деятельности – конференция начинается неделей «мастерских» по администрированию различных компонентов инфраструктуры Интернета. Совместно с APRICOT проводится встреча APNIC, организуемая региональной интернет-регистратурой, отвечающей за этот регион. Здесь помимо технических вопросов обсуждаются политики администрирования адресного пространства. https://2019.apricot.net/

18-20 февраля 2019
NANOG 75,
Сан-Франциско, США

Североамериканская группа сетевых операторов (The North American Network Operators Group, NANOG) является одной из самых активных профессиональных ассоциаций в области сетевой архитектуры, конфигурации и технического администрирования сетей в Интернете. Основной фокус NANOG - на технологиях и системах, обеспечивающих работу Интернета: системе глобальной маршрутизации, DNS, пиринге и связности. NANOG имеет активный список рассылки и проводит конференции три раза в год. Поскольку инженерные вопросы NANOG имеют глобальный характер, участие в списке рассылки и конференциях может быть полезно широкому кругу технических специалистов в области сетевых технологий Интернета.
Подача заявок на доклады заканчивается 3 декабря 2018 г.
https://nanog.org/meetings/nanog75/home

19-14 марта 2019
ICANN 64,
Кобэ, Япония

Встречи ICANN проводятся три раза в год в различных регионах земного шара для того, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. Участие во встречах ICANN бесплатно.
https://meetings.icann.org/en/calendar

23-29 марта 2019
IETF 104,
Прага, Чехия

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов в области Интернета. В основном работа в IETF проходит в многочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100). Три раза в год IETF проводит недельные совещания, на которые приезжают разработчики протоколов, инженеры и операторы со всего мира (в среднем около 1200 участников из более 50 стран мира). Совещания IETF – это хорошая возможность познакомиться с новейшими тенденциями в области сетевых технологий и принять участие в их разработке. https://www.ietf.org/how/meetings/104/

31 марта - 2 апреля 2019
Euro-IX Forum 34,
Тулуза, Франция

Euro-IX является ассоциацией точек обмена трафиком (IXP), координирующей различную коллективную деятельность между участниками и предоставляющей информационные услуги, такие как база данных IXP по всему миру. Два раза в год Euro-IX организует встречу участников и всех, кому интересны вопросы обмена трафиком, создания и обслуживания IXP. Это прекрасная возможность обменяться опытом, расширить свою профессиональную сеть и установить новые деловые отношения.
https://www.euro-ix.net/en/events/fora/34th-euro-ix-forum/

В России

21 февраля 2019, Санкт-Петербург

Smart City & Region

Бизнес-форум «Smart City & Region: Цифровые технологии на пути к «умной стране» будет посвящен вопросам построения цифровой информационной инфраструктуры для создания «умного города» и продолжит традиции ежегодной конференции «Телеком российских столиц», которая собирала владельцев цифровой инфраструктуры и представителей органов власти различных регионов страны.
https://www.comnews-conferences.ru/ru/conference/smartspb2019

В Москве

23 ноября 2018

XIV Пиринговый форум MSK-IX

Крупнейшая ежегодная встреча участников интернет- и телеком-рынка, организованная MSK-IX. **Главные темы XIV Пирингового форума**: измерения в сети, аналитика и исследования сетевой связности, доступа пользователей, распределения сетевых ресурсов; медиалогистика; иностранцы в России – опыт деплоя в РФ от зарубежных компаний; что не так с BGP и есть ли возможность это исправить?; региональный пиринговый ландшафт и другие актуальные вопросы развития сети и обмена трафиком.
https://peering-forum.ru/

4 декабря 2018

Broadband Russia Forum

VIII Международный форум «Broadband Russia Forum: Цифровые сервисы поверх сетей доступа». Это крупнейшее событие рынка ШПД в России, которое традиционно собирает на своей площадке более 200 участников рынка широкополосного доступа, более 30 докладчиков – операторов, регуляторов и поставщиков оборудования и сервисов, более 20 экспонентов.
https://www.comnews-conferences.ru/ru/conference/bb2018

4-5 декабря 2018

EE DNS FORUM 2018

III Восточноевропейский DNS-форум, организованный международной корпорацией ICANN при поддержке Координационного центра доменов .ru/.рф. В фокусе форума — интернет-безопасность, юридические аспекты регистрации доменов, злоупотребление DNS, новые технологии идентификации, региональные тренды и многое другое с участием ведущих экспертов доменной отрасли. Первый день форума будет посвящен вопросам технологий и техническим аспектам, а второй – разработке политик регулирования взаимодействий между участниками доменного рынка.
https://eednsforum.org/ru/

29-31 января 2019

CSTB Telecom & Media 2019

21-я Международная выставка и форум – главное событие индустрии телевидения и телекоммуникаций в России и странах СНГ, с которого вот уже более 20 лет ежегодно открывается деловой сезон. В 2019 году проект пройдет под эгидой цифровой трансформации телеком- и медиаиндустрии.
https://www.cstb.ru/

31 января - 1 февраля 2019

Инфофорум-2019

21-й Большой национальный Инфофорум – важнейшее мероприятие в сфере информационной безопасности в Российской Федерации, которое проводится с 2001 года и ежегодно собирает более 1,5 тысяч специалистов из всех регионов России и дружественных стран. https://infoforum.ru/

4 февраля 2019

PgConf.Russia 2019

Международная техническая конференция по открытой СУБД PostgreSQL, ежегодно собирающая более 500 разработчиков, администраторов баз данных и IT-менеджеров для обмена опытом и профессионального общения. В программе – мастер-классы ведущих мировых экспертов, доклады в три тематических потока, примеры лучшего опыта и разбор ошибок, гостиная разработчиков и блиц-доклады из зала. https://pgconf.ru/2019

21-22 марта 2019

Transport Networks Russia & CIS 2019

Ключевыми темами X Международной конференции «Transport Networks Russia & CIS: Развитие телекоммуникационных транспортных сетей в России и СНГ» станут глобальный рынок магистральных транспортных сетей; новые возможности трансграничных переходов и стыков магистральных сетей; оптимизация инфраструктуры и новые технологии в строительстве магистральных линий; контент-провайдеры и операторы связи на российском рынке; роль точек обмена трафиком на магистральном рынке и другие темы. https://www.comnews-conferences.ru/ru/conference/tn2019

MSK IX

10
ГОРОДОВ

500+
УЧАСТНИКОВ

42
ПЛОЩАДКИ

21
УЗЛЕЛ DNS-СЕТИ

ПОДКЛЮЧЕНИЯ ДО
100G

ТРАФИК
2,8Тбит/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

Интернет изнутри

2018