SAC132

Система доменных имен работает на бесплатном и открытом программном обеспечении (FOSS)

Отчет Консультативного комитета по безопасности и стабильности (SSAC) ICANN
25 сентября 2025 года

Предисловие

Это отчет Консультативного комитета по безопасности и стабильности ICANN (SSAC) Правлению ICANN, корпорации ICANN, сообществу ICANN и, в целом, интернет-сообществу о том, каким образом работа системы доменных имен (DNS) зависит от бесплатного и открытого программного обеспечения (FOSS).

В центре внимания SSAC находятся вопросы, связанные с безопасностью и целостностью систем распределения имен и адресов Интернета. К ним относятся рабочие вопросы (например, относящиеся к правильной и надежной работе системы публикации корневых зон), технические административные вопросы (например, относящиеся к распределению интернет-адресов и присвоению номеров) и регистрационные вопросы (например, связанные с услугами регистратур и регистраторов). SSAC занимается постоянной оценкой угроз и анализом рисков для служб распределения имен и интернет-адресов с целью определения источников основных угроз стабильности и безопасности и дает соответствующие рекомендации сообществу ICANN. SSAC не обладает полномочиями регламентировать, обеспечивать соблюдение или выносить решения. Эти функции исполняют другие органы, и содержащиеся в настоящем документе рекомендации следует рассматривать по существу. Члены SSAC участвуют как индивидуальные лица, а не как представители своих работодателей или других организаций. Консенсус SSAC по документу достигается, когда перечисленные авторы соглашаются с содержанием и рекомендациями при отсутствии окончательных возражений со стороны остальных членов SSAC, за исключением отказов от участия, указанных в конце документа.

Содержание

Список рисунков

Список таблиц

Основные положения

Система доменных имен (DNS) — это глобально распределенная, иерархическая и децентрализованная система, информация которой лежит в основе практически каждого взаимодействия в интернете. Основная цель — сопоставить друг с другом удобные для чтения пользователем доменные имена с удобными для обработки компьютером IP-адресами, необходимыми для нахождения ресурсов в сети. Будь то просмотр страниц, отправка электронной почты или использование мобильного приложения, все соединения в интернете зависят от информации, которая исходит от системы DNS и структурируется ею.

Основной вывод этого отчета заключается в том, что система DNS построена и работает на основе бесплатного и открытого программного обеспечения (FOSS). Это не узкоспециализированная практика, а общепринятая реальность. Использование FOSS является нормой для самых фундаментальных компонентов инфраструктуры DNS. Например, по крайней мере девять из 12 независимых организаций, которые управляют системой корневых серверов интернета (RSS), используют исключительно реализации FOSS. Кроме того, девять из 10 крупнейших провайдеров услуг для доменов верхнего уровня (TLD) используют FOSS. Такое доминирование обусловлено сильными сторонами, присущими модели разработки FOSS, которая сочетает в себе экономическую эффективность и простоту внедрения с транспарентностью, безопасностью за счет сотрудничества и эксплуатационной отказоустойчивостью, необходимыми для критической инфраструктуры.

Хотя модель разработки FOSS принципиально отличается от модели разработки программного обеспечения с закрытым исходным кодом, FOSS не является заведомо совершенно безопасным. Безопасность любого программного проекта определяется качеством процессов его разработки и сопровождения, а не доступностью его исходного кода для всех. В отличие от коммерческого программного обеспечения, FOSS представляет собой открытый глобальный проект, основанный на четырех основных свободах: свободе использования, изучения, распространения и изменения. Эта экосистема зависит от глобальной сети лиц, оказывающих услуги по сопровождению проекта, и участников проекта, которые часто являются волонтерами, не получающими платы за свою работу. Хотя многие из этих волонтеров работают не за денежное вознаграждение, сфера DNS уникальна тем, что полагается также на несколько давно существующих организаций технической поддержки. Это создает модель, основанную на сотрудничестве сообщества, а не на коммерческих контрактах, которые определяют традиционную цепочку поставок программного обеспечения, что влечет за собой особые риски, связанные с финансовой устойчивостью организаций, оказывающих услуги по сопровождению проекта, и выгоранием волонтеров, предоставляющих поддержку проекту.

Эти уникальные особенности означают, что нормативные рамки, разработанные для коммерческого программного обеспечения, могут не подходить для FOSS и,

следовательно, могут иметь серьезные непредвиденные последствия для стабильности критической инфраструктуры интернета. Чтобы преодолеть эти сложности и создать безопасную цифровую экосистему, Консультативный комитет по безопасности и стабильности (SSAC) предоставляет следующие рекомендации для организаций, формирующих политику:

- **Признать важную роль FOSS:** Организации, формирующие политику, должны открыто признать в любом соответствующем законодательстве или нормативных актах, что критическая инфраструктура интернета зависит от бесплатного и открытого программного обеспечения (FOSS) и что его использование является преимуществом, которое необходимо сохранить.
- **Прислушиваться к мнению сообщества FOSS:** При разработке законодательства и нормативных актов необходимо учитывать мнения всех участников экосистемы FOSS: от отдельных лиц, оказывающих услуги по сопровождению проекта, до некоммерческих организаций и корпораций.
- **Использовать современные подходы регулирования FOSS:** Организации, формирующие политику, могут ссылаться на недавние тематические исследования в отчете о современных подходах, включающих уникальные характеристики модели развития FOSS.
- **Стимулировать устойчивое развитие FOSS:** Поощрять вклад государственного и частного секторов в критически важные проекты FOSS как форму инвестиций в общественное благо для всех.
- **Коллективно устранять системные риски:** Развивать и финансировать совместные решения в масштабах всей экосистемы, чтобы снизить риски, связанные с общими взаимозависимыми элементами, а не обременять отдельных лиц, оказывающих услуги по сопровождению проекта.

1 Введение

Этот отчет подготовлен в связи с возросшим вовлечением организаций, формирующих политику, в усилия отрасли по снижению числа уязвимостей программного обеспечения в цифровой инфраструктуре. Поскольку правительства и регулирующие органы по всему миру стремятся обезопасить цепочку поставок программного обеспечения, крайне важно, чтобы эти усилия основывались на четком понимании того, как на самом деле создаются и поддерживаются основополагающие системы интернета. Недавние примеры (предлагаемого) вмешательства регулирующих органов с целью снижения уязвимости программного обеспечения в цифровой инфраструктуре включают:

- Добровольный кодекс правил по безопасности программного обеспечения для поставщиков программного обеспечения в Великобритании.[1]
- Внутренняя аттестация отрасли по безопасности методов разработки программного обеспечения для использования правительством США.[2]
- Требования к выходу на рынок («Закон о киберустойчивости (CRA)») для цифровых продуктов (включая программное обеспечение) в ЕС.[3]
- Обязательства по управлению рисками и отчетности для провайдеров цифровой инфраструктуры в ЕС («NIS2 IA»).[4]
- Сообщества открытого программного обеспечения названы одной из целей развития пятилетнего плана Китая в области ИТ.[5,6]

[1] «Кодекс правил по безопасности программного обеспечения». Министерство науки, инноваций и технологий Великобритании, 7 мая 2025 года. https://www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice.

[2] «Форма аттестации безопасной разработки программного обеспечения». Агентство кибербезопасности и безопасности инфраструктуры США, https://www.cisa.gov/secure-software-attestation-form.

[3] «Закон о киберустойчивости». Депутаты Европарламента приняли планы по повышению безопасности цифровых продуктов», пресс-релиз Европейского парламента от 12 марта 2024 года, https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products

[4] «Закон о киберустойчивости». Депутаты Европарламента приняли планы по повышению безопасности цифровых продуктов». Пресс-релиз. Европейский парламент, 12 марта 2024 года. https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products.

[5] «14-й пятилетний план для индустрии программного обеспечения и услуг информационных технологий». Государственный совет Китайской Народной Республики, Министерство промышленности и информационных технологий, декабрь 2021 года. https://www.gov.cn/zhengce/zhengceku/2021-12/01/5655205/files/a44b507d67c74591ad4f5e55b98c4518.pdf.

[6] «Перевод: 14-й пятилетний план национальной информатизации». Проект DigiChina, Стэнфордский университет, 24 января 2022 года. https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

Хотя бесплатное и открытое программное обеспечение (FOSS) сегодня является доминирующей практикой в разработке программного обеспечения, его особые характеристики часто упускаются из виду в дискуссиях о политике. Если организации, формирующие политику, вводят регулирующие меры, не понимая уникальной модели разработки и поставок FOSS, они рискуют поставить под угрозу безопасность и стабильность критической инфраструктуры, которая от него зависит, включая домены и системы маршрутизации интернета. Целью настоящего отчета является предоставление необходимого контекста.

В отличие от того, что принято в других секторах, большая часть программного обеспечения, обеспечивающего работу интернета, доступна по лицензиям на авторские права FOSS. Эти лицензии в первую очередь касаются не стоимости, а свободы. В частности, лицензии FOSS предоставляют операторам инфраструктуры четыре основные свободы: использовать, изучать, изменять и делиться программным обеспечением — модифицированным или нет — со всеми. Это модель разработки, а не просто «бесплатное» программное обеспечение, [7] и это основа совместных глобальных усилий, которые создают и поддерживают большую часть критической инфраструктуры интернета.

Этот отчет структурирован таким образом, чтобы предоставить организациям, формирующим политику, всестороннее понимание роли FOSS в системе доменных имен (DNS) и экосистеме регистрации доменных имен.

- Раздел 2 содержит введение в DNS без технических подробностей, в котором объясняются ключевые компоненты и функции этой критической инфраструктуры.
- В Разделе 3 подробно описывается модель FOSS, объясняются ее основные характеристики, присущие ей сильные стороны и уникальные риски по сравнению с коммерческим программным обеспечением.
- В Разделе 4 представлены основные исследования Консультативного комитета по безопасности и стабильности (SSAC) по распространенности FOSS, демонстрирующие его доминирование в наиболее важных частях DNS.

[7] FOSS может использоваться в любых целях и не имеет ограничений, таких как истечение срока действия лицензии или географические ограничения. Его код может изучить любой желающий без соглашений о неразглашении или аналогичных ограничений. Его можно копировать и распространять практически бесплатно. Кроме того, FOSS может быть изменено любым человеком, и эти улучшения могут быть опубликованы. Отсутствие или ослабление хотя бы одной из этих свобод означает, что приложение является коммерческим, то есть программным обеспечением с закрытым исходным кодом. Эти четыре свободы предоставляются лицензией на программное обеспечение. Лицензии на программное обеспечение определяют условия, при которых программа может единожды или многократно использоваться. Чтобы программное обеспечение считалось свободным, текст лицензии должен содержать как минимум четыре свободы. Фонд свободного программного обеспечения (https://www.gnu.org/licenses/license-list.html), Инициатива открытого исходного кода (https://opensource.org/licenses) и Проект Debian (https://wiki.debian.org/DFSGLicenses) ведут списки рассмотренных и одобренных лицензий. Приложение обычно не может считаться FOSS, если его лицензия не указана ни в одном из этих списков.

- В Разделе 5 рассматриваются несколько современных случаев из США, Великобритании и Европейского Союза, которые иллюстрируют, как организации, формирующие политику, адаптируют правила кибербезопасности к уникальным реалиям экосистемы FOSS.
- Раздел 6 объединяет основной анализ отчета в ряд выводов, которые формируют обоснование руководящих принципов, изложенных в Разделе 7.
- Раздел 7 содержит прямые и действенные рекомендации для организаций, формирующих политику.

2 Введение в DNS

Когда вы отправляете электронное письмо, просматриваете страницу, общаетесь с друзьями и т. д., ваше устройство (например, компьютер, телефон или планшет) отправляет и получает тысячи единиц информации. Это можно представить как цифровую открытку с адресом отправителя, адресом получателя и содержимым. Каждое устройство, подключенное к интернету, имеет как минимум один уникальный IP-адрес. Людям легче запоминать имена, чем числа. DNS — это своего рода адресная книга интернета. Она связывает IP-адрес с доменным именем, чтобы каждый мог легче пользоваться интернетом.[8,9] DNS — это критически важная система, которая необходима для стабильной, безопасной и функционально совместимой глобальной сети интернет.

DNS обеспечивает сопоставление удобных для пользователя доменных имен (например, icann.org) с удобными для компьютера числовыми IP-адресами (например, 192.0.43.7 или 2001:db8::1). Эти сопоставления в совокупности составляют глобальное пространство имен. Чтобы иметь сайт или учетную запись электронной почты, доступ к которым возможен через доменное имя, владелец домена должен опубликовать схемы сопоставления для этой услуги. Такая публикация в DNS делает связь между доменным именем и IP-адресом сервиса доступной любому пользователю интернета.

Как показано на рисунке 1, экосистема DNS состоит из трех основных частей:

- Регистрация доменного имени (светло-голубое поле): Это административная и договорная основа приобретения доменных имен.
- Инфраструктура DNS (зеленый квадрат): Это технические системы, которые обеспечивают работу доменных имен в интернете, преобразуя их в IP-адреса.
- Услуги для конечного пользователя и контента (оранжевые и темно-синие поля): Это те услуги, которыми в конечном итоге пользуются люди, например сайты и электронная почта.

[8] ICANN. «Система доменных имен», 13 сентября 2022 года. https://www.icann.org/resources/pages/dns-2022-09-13-en.

[9] Cloudflare. «Что такое DNS? | Как работает DNS», https://www.cloudflare.com/learning/dns/what-is-dns/.

Основное внимание в этом отчете уделяется регистрации доменных имен и инфраструктуре DNS, которые вместе образуют уровень критической инфраструктуры интернета. Поиск информации в глобальном пространстве доменных имен в основном не монетизируется и предоставляется клиентам «бесплатно», без взимания платы. Инфраструктура, которая позволяет использовать эту глобальную распределенную службу как «общественное благо, не предполагающее эксплуатацию», в данном отчете называется «инфраструктурой DNS». Система широко распространена в интернете и состоит из множества компонентов, которыми управляют многие независимые организации, выполняющие различные конкретные функции в этой системе. Эти системы функционально совместимы, поскольку необходимые технические детали их интерфейсов и коммуникаций стандартизированы Инженерной проектной группой Интернета (IETF).

Эта критическая инфраструктура существует отдельно от контента, который передается по ней. Регистрация доменного имени — это не то же самое, что создание сайта. Публикация доменного имени в DNS для возможности его поиска — это не то же самое, что публикация контента сайта. В этом отчете рассматривается базовое программное обеспечение, обеспечивающее работу адресной книги, а не информация, записанная на страницах этой книги.

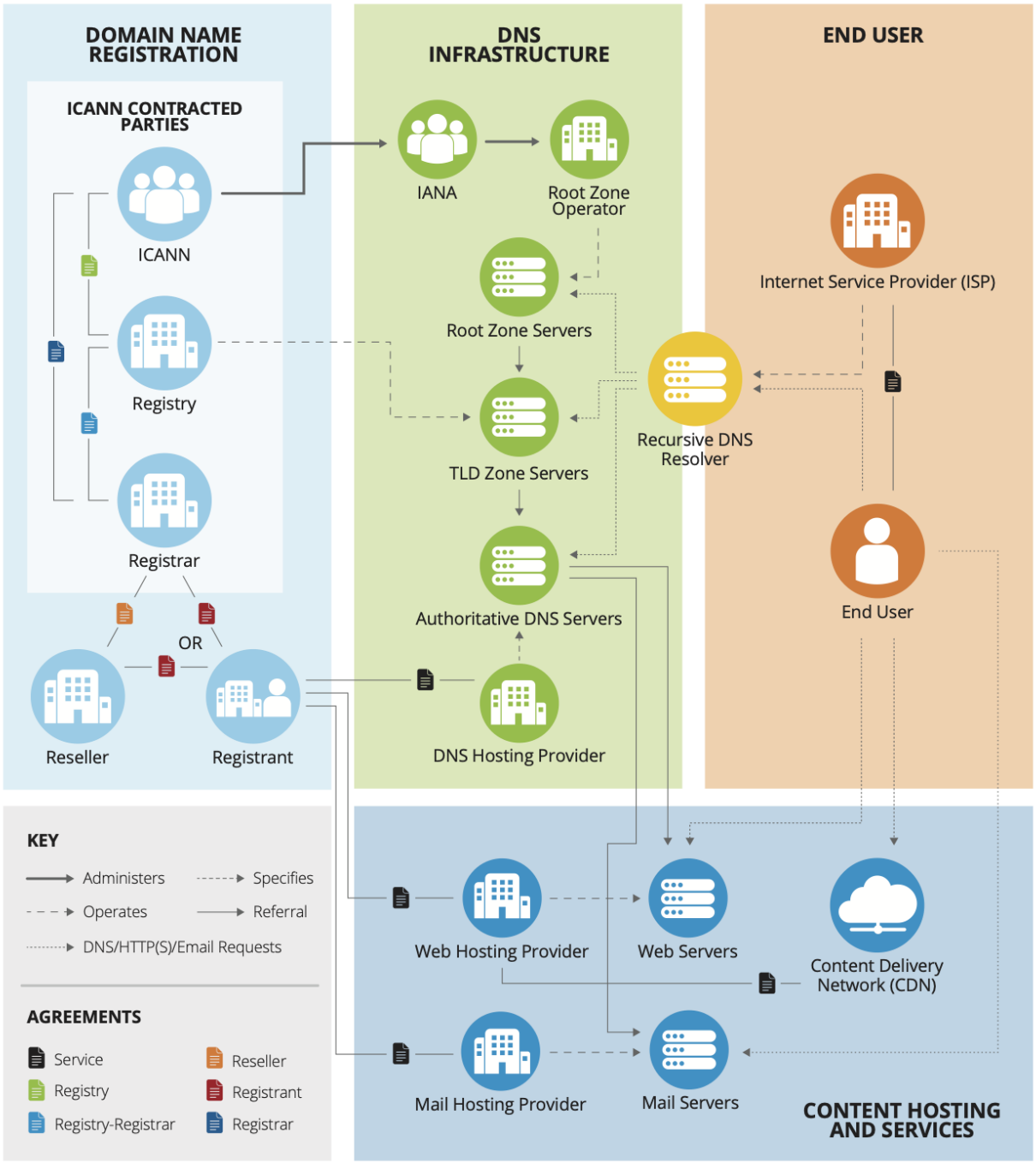

Рис. 1. *Экосистема интернета.* Кит Дразек (Keith Drazek). «Безопасность DNS: продолжающаяся работа сообщества по снижению угроз безопасности системы доменных имен (DNS)». Блог Verisign, 7 декабря 2021 года. https://blog.verisign.com/domain-names/ongoing-community-work-to-mitigate-domain-name-system-security-threats/.

2.1 Иерархия DNS

DNS — это глобально распределенная, иерархическая и децентрализованная система. Эта система, показанная на рисунке 1 как «Инфраструктура DNS», спроектирована с расчетом на отказоустойчивость, обеспечивая отсутствие единой точки отказа в глобальном интернете.

На рисунке 2 показана иерархия пространства имен DNS.

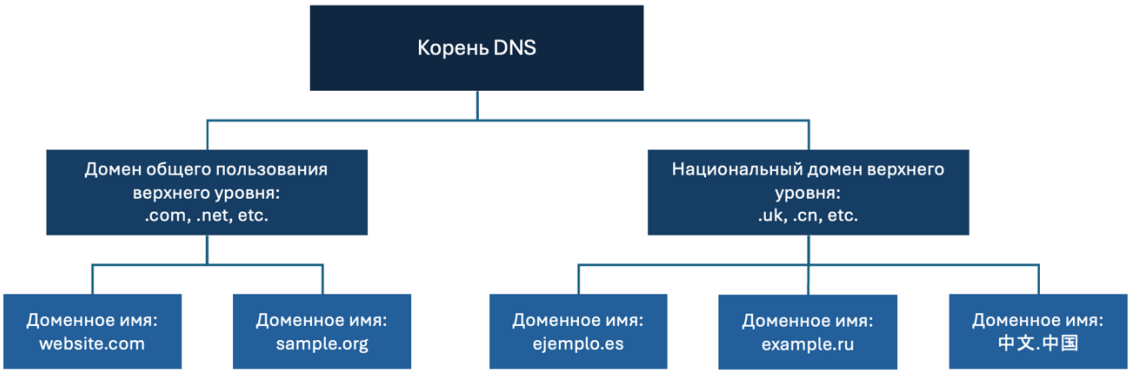

Рис. 2. *Иерархия DNS*

На самом верху иерархии находится корень DNS (.), который обслуживается системой корневых серверов (RSS).[10] Корень указывает на авторитативные серверы для различных доменов верхнего уровня (TLD). Домены верхнего уровня (TLD) — это окончания доменных имен, которые можно разделить на два типа:

- Домены общего пользования (верхнего уровня) (gTLD): Это домены общего назначения, такие как .com, .org, .xyz и .shop.[11]
- Национальные домены верхнего уровня (ccTLD): Они зарезервированы для использования странами, территориями и географическими локациями, указанными в списке кодов стран ISO 3166-1.[12] Названия ccTLD могут основываться на двухбуквенных кодах стран, определенных стандартом ISO 3166-1 (например, .jp для Японии, .fr для Франции, .ke для Кении), или они могут представлять название страны или территории в алфавите, отличном от символов

[10] Система корневых серверов состоит из распределенных по всему миру серверов, которыми управляют 12 независимых организаций. Дополнительную информацию об операторах корневых серверов см. в документе «RSSAC023v2: история системы корневых серверов». Консультативный комитет системы корневых серверов ICANN (RSSAC), 17 июня 2020 года. https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf.

[11] ICANN. «Аббревиатуры и терминология, домен общего пользования (верхнего уровня) (gTLD)», https://www.icann.org/ru/icann-acronyms-and-terms/generic-top-level-domain-ru.

[12] Международная организация по стандартизации. «ISO 3166 — Коды стран», https://www.iso.org/iso-3166-country-codes.html.

ASCII.[13] Это получило название интернационализированные доменные имена (IDN) — концепция, реализуемая ICANN с 2009 года.

Ниже TLD находятся отдельные доменные имена. Доменное имя состоит из двух или более текстовых сегментов, разделенных точками. Как показано на рисунке 3, доменное имя формируется справа налево, начиная с TLD. Например, в icann.org домен верхнего уровня — .org, а домен второго уровня — icann. Вместе они образуют уникальное доменное имя. Во втором примере, bbc.co.uk, TLD — .uk, а домен второго уровня — .co. Эта иерархическая и децентрализованная система обеспечивает надежность и устойчивость глобального интернета.

Доменное имя — это уникальное имя, которое составляет основу унифицированных адресов ресурсов (URL), используемых людьми для поиска ресурсов в интернете. Доменное имя само по себе идентифицирует конкретный адрес в интернете, принадлежащий субъекту, например компании, организации, учреждению или частному лицу.[14]

[13] ICANN. «Аббревиатуры и терминология, национальный домен верхнего уровня (ccTLD)», https://www.icann.org/ru/icann-acronyms-and-terms/country-code-top-level-domain-ru.

[14] ICANN. «Аббревиатуры и терминология, доменное имя», https://www.icann.org/ru/icann-acronyms-and-terms/domain-name-ru.

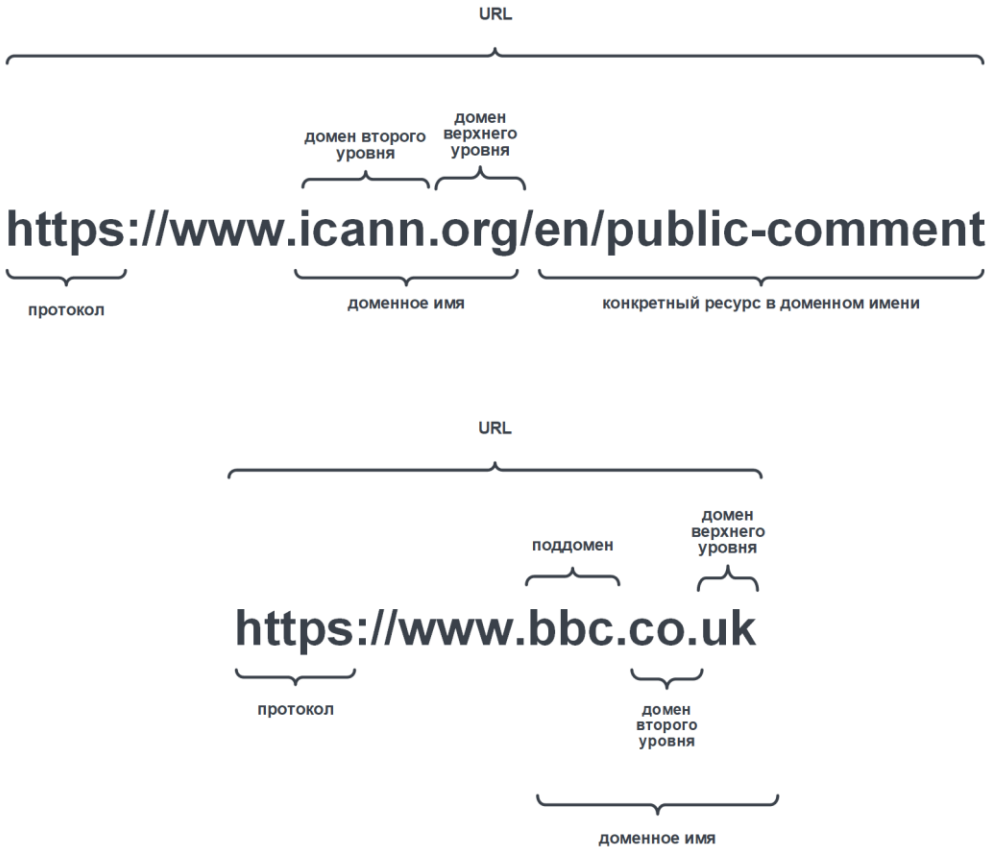

Рис. 3. *Компоненты унифицированного адреса ресурса (URL) и доменного имени*

2.2 Регистрация и публикация доменного имени

Инфраструктура регистрации доменных имен относится к системам, которые облегчают получение уникального доменного имени. Этот процесс, проиллюстрированный в разделе «Регистрация доменного имени» на рисунке 1, включает в себя несколько ключевых участников и два отдельных процесса: регистрацию и публикацию.

Регистрация — это процесс резервирования доменного имени. Владелец домена — это физическое или юридическое лицо, которое регистрирует определенное доменное имя и владеет правами на него. Чтобы зарегистрировать доменное имя в определенном домене верхнего уровня, владелец домена должен воспользоваться услугами регистратора. Регистратор — это публичная организация, которая действует как розничный продавец доменных имен. Регистраторы фактически являются каналами распространения регистраций, управления платежами, продлением и другой административной информации. Затем регистратор взаимодействует с регистратурой. Регистратура является авторитетной основной базой данных всех доменных имен в пределах данного TLD. Организация, которая ведет эту базу данных, называется оператором регистратуры. Для автоматизации миллионов транзакций между собой регистраторы и регистратуры

используют Протокол EPP — стандартизированный протокол для регистрации, продления и передачи доменных имен.

Результатом успешной регистрации является публикация DNS-записей домена на авторитативных серверах, входящих в инфраструктуру DNS, что делает домен доступным в интернете. Публикация — это технический процесс, делающий записи DNS домена доступными на авторитативных серверах имен. Эти серверы содержат списки удобных для пользователя доменных имен с соответствующими им пригодными для компьютера IP-адресами, что имеет решающее значение для обнаружения и проверки подлинности сайтов, почтовых серверов и других интернет-ресурсов.

2.3 Разрешение DNS

При вводе доменное имя, например www.example.com, в браузер, начинается процесс, называемый «разрешение DNS». Этот процесс основан на двух типах компонентов инфраструктуры DNS, которые работают вместе: рекурсивных резолверах и авторитативных серверах (см. рисунок 4).

Рис. 4. *Традиционное разрешение DNS*

Авторитативные серверы — это компоненты, которые публикуют информацию о домене. Они хранят окончательную официальную запись по конкретному домену и делают ее доступной для поиска. Авторитативные серверы имен обслуживаются физическими лицами, предприятиями, университетами, провайдерами услуг и государственными органами. Например, серверы имен TLD публикуют технические данные для всех отдельных доменов в своей регистратуре. Во многих организациях имеются локальные службы DNS, которые предоставляют только информацию, относящуюся к их внутренней организации, например, для поиска сайтов отделов во внутренней сети. Это большая часть DNS, которая не видна из открытого интернета.

Некоторые конечные пользователи и предприниматели малого бизнеса полагаются на авторитетные DNS-серверы регистраторов доменных имен или компаний хостинга для публикации информации о своих доменах, но компании, правительства и организации часто используют свои авторитативные серверы отдельно, либо внутри компании, либо на

аутсорсинге. Основными проблемами являются надежность и резервирование данных; в связи с этим администраторы «зонной» информации, опубликованной в домене, часто приобретают «вторичные авторитативные DNS-сервера» у внешних провайдеров. Эти провайдеры публикуют те же данные, что и основные авторитативные DNS-серверы. Многие из организаций, предлагающих такие услуги, являются теми же, что предоставляют авторитативные DNS-сервера для доменов верхнего уровня.

Резолверы облегчают поиск информации DNS. Они действуют от имени устройства пользователя («клиента», например, вашего смартфона), чтобы найти правильный IP-адрес. Чтобы делать это эффективно, резолверы поддерживают постоянно обновляемую базу данных последних поисков, называемую кэшем. На практике резолверы часто отвечают на 90% запросов из своего локального кэша, что намного быстрее, чем отправка запросов серверам через интернет. Для ответов, которых нет в кэше, им приходится обращаться к авторитативным серверам. Резолверы обычно представляют собой очень активные, сильно загруженные системы, отчасти потому, что постоянно высокий уровень трафика обуславливает непрерывное обновление кэша.

По всему миру существуют миллионы резолверов. Резолвер может работать в локальной сети, в сети пользователя или сети провайдера доступа, либо в облаке, как отдельная служба, размещенная в интернете, или в сочетании с другими облачными сервисами. Независимо от того, как организован сервис, важно, чтобы отправлять запросы к нему могли только те пользователи, для которых он предназначен. Если сервис открыт для любого пользователя интернета, он может быть использована не по назначению, например, для проведения атак типа «отказ в обслуживании» (DDoS). Предпочтительный провайдер обычно определяется настройками устройства пользователя. Многие университеты, предприятия и интернет-провайдеры (ISP) предоставляют локальные резолверы для пользователей своих сетей, а также существуют популярные облачные сервисы, такие как Google (8.8.8.8), Quad9 (9.9.9.9) и Cloudflare (1.1.1.1). Ключевые факторы при принятии решения о том, резолвер какого провайдера использовать, включают организационную политику, политики фильтрации или блок-листа резолвера, а также доступность зашифрованной передачи данных DNS. Процесс разрешения доменного имени (рисунок 4) показывает, как эти компоненты работают вместе, следуя иерархии DNS.

3 Модель FOSS: ключевые характеристики и нюансы

В предыдущем разделе были представлены основные сведения об инфраструктуре DNS и регистрации доменных имен — основополагающих системах, которые позволяют пользователям ориентироваться в интернете. В этом разделе объясняется, как создается и поддерживается эта критическая инфраструктура. Программное обеспечение, лежащее в основе большей части этой инфраструктуры, — это бесплатное и открытое программное обеспечение (FOSS), которое работает на основе принципиально иной модели разработки

и экономики, чем традиционное коммерческое программное обеспечение. Обсуждение обоснованной политики требует понимания этих уникальных характеристик.

3.1 Ключевые роли в экосистеме FOSS

В отличие от традиционного программного обеспечения с закрытым исходным кодом, разработка которого осуществляется внутри одного юридического лица, модель FOSS является открытой и распределенной. Роли не являются взаимоисключающими и могут исполняться кем угодно и откуда угодно. Для целей настоящего отчета будут использоваться следующие термины:

- **Лицо, оказывающее услуги по сопровождению проекта:** Индивидуальное лицо или группа, ответственные за общее руководство проектом FOSS. Лица, оказывающее услуги по сопровождению проекта, имеют право принимать или отклонять дополнения к официальной версии программного обеспечения, обеспечивая качество и согласованность. Они являются координаторами проекта.
- **Участник:** Индивидуальное лицо или организация, предлагающие улучшения для проекта, например, путем предоставления кода, документации или отчетов об ошибках. Такие улучшения проверяются лицами, оказывающими услуги по сопровождению проекта, перед добавлением в официальный проект.
- **Пользователь или оператор:** Индивидуальное лицо или организация, которые внедряют и используют программное обеспечение. В контексте DNS «оператор» — это организация, которая управляет компонентами инфраструктуры DNS, такими как авторитативные серверы или резолверы. Пользователи и операторы являются важнейшей частью экосистемы, обеспечивая обратную связь и придавая смысл проекту.

Во избежание двусмысленности в данном отчете используются конкретные термины «лицо, оказывающее услуги по сопровождению проекта» и «участник» вместо более общего термина «разработчик», поскольку индивидуальное лицо может разрабатывать код в качестве сопровождающего, участника или независимо.

3.2 Основные принципы модели разработки FOSS

Модель FOSS определяется правами, предоставляемыми ее лицензиями на авторские права. Чтобы программа считалась FOSS, ее лицензия должна предоставлять пользователям четыре основные свободы:[15,16]

[15] Операционная система GNU. «Что такое бесплатное программное обеспечение?», https://www.gnu.org/philosophy/free-sw.html.

[16] Альтернативное и популярное определение того, что представляет собой лицензия FOSS, — это «Определение открытого исходного кода» от Open Source Initiative. https://opensource.org/osd.

- Свобода ***использовать*** программное обеспечение в любых целях без ограничений, таких как истечение срока действия лицензии или географические ограничения.
- Свобода ***изучения*** того, как работает программа, требующая доступа к исходному коду без соглашений о неразглашении.
- Свобода ***распространения*** программного обеспечения, то есть его можно распространять и копировать практически бесплатно.
- Свобода ***вносить изменения*** в программу и открыто публиковать эти улучшения.

Отсутствие или ослабление любой из этих свобод означает, что программное обеспечение является коммерческим, а не FOSS. Эти свободы являются основой общих характеристик FOSS, которые существенно отличаются от коммерческого программного обеспечения. Такие организации, как Free Software Foundation,[17] Open Source Initiative[18] и Debian Project,[19] ведут списки лицензий на программное обеспечение, которые были рассмотрены и одобрены как соответствующие этим критериям.

Эти четыре свободы — не просто абстрактные принципы; они являются основой уникальной модели разработки и экономических характеристик FOSS, которые описаны в следующих подразделах.

3.2.1 Модель FOSS обеспечивает возможность разработки в рамках глобального сотрудничества

Поскольку лицензии FOSS предоставляют всем свободу изучать код, вносить в него изменения и распространять его, они обеспечивают возможность открытого глобального сотрудничества в разработке программного обеспечения. Не существует произвольного набора предварительных условий, применяемых к участникам разработки FOSS, что позволяет любому индивидуальному лицу вносить вклад в его разработку. Вклад может поступать от самых разных лиц и организаций, иногда в рамках корпоративной разработки продукта, иногда на волонтерской индивидуальной основе.

Полученный продукт свободно предоставляется любому лицу не только для любого использования (включая коммерческое), но и для дальнейшей разработки. Это снижает сложность разработки программного обеспечения, особенно в случаях, когда изменения интегрируются обратно в программный продукт, способствуя ускорению разработки функций, а также устранению ошибок программного обеспечения и проблем безопасности. Основанная на сотрудничестве разработка FOSS способствует транспарентности и быстрому внедрению инноваций. Более того, сами вклады участников

[17] Операционная система GNU. «Различные лицензии и комментарии о них», https://www.gnu.org/licenses/license-list.html.

[18] Инициатива открытого исходного кода. «Лицензии, одобренные OSI», https://opensource.org/licenses.

[19] Debian Wiki. «DFSGLicenses», https://wiki.debian.org/DFSGLicenses.

обычно также являются открытыми, что позволяет другим изучать предлагаемые вклады и высказывать свои замечания относительно их целесообразности и преимуществ интеграции в программный продукт.

Таким образом, редко бывает так, чтобы все подобные вклады принимались без определенной степени проверки и одобрения. Подобные проверки направлены на снижение риска компрометации программного обеспечения за счет включения непоследовательного, неверного или вредоносного кода. Существуют некоторые общие условия принятия вкладов, включая необходимость сохранения авторских прав и прав интеллектуальной собственности. Распространенная практика FOSS заключается в том, что никакие вклады участников сотрудничества не могут налагать дополнительные ограничения на использование программного обеспечения сверх условий, уже связанных с программным обеспечением, а также не могут налагать дополнительные ограничения на авторские права или интеллектуальную собственность на существующую базу программного обеспечения.

В качестве альтернативы участию, лицензии FOSS также позволяют участникам создавать собственные производные версии (ответвления проекта) вместо работы с исходным проектом (основная ветка проекта). Беспрепятственный форкинг (ответвление) проекта обеспечивает быстрое внедрение инноваций. Некоторые ответвления стали более популярными, чем то программное обеспечение, от которого они произошли. Но они также могут создавать путаницу, разделяя имеющиеся возможности проверки для выявления ошибок или вредоносных изменений.

Программное обеспечение может быть самостоятельным или может полагаться на другие программные библиотеки для создания необходимой функциональности. Такие библиотеки, по сути являющиеся внешними компонентами кода, могут изменяться способами, менее заметными для разработчиков кода, и эта ситуация может приводить к непредвиденным последствиям. FOSS имеет очень низкий барьер для использования в качестве компонента в другом (в том числе коммерческом) программном обеспечении, что делает наблюдаемую частоту возникновения такого риска выше, хотя он не является уникальным для FOSS.

3.2.2 Модель FOSS функционирует без договорных обязательств

Одним из основных отличий модели поставок FOSS является то, что стороны обычно не имеют договорных отношений. Это контрастирует с цепочкой поставок физических товаров, где производители и дистрибьюторы имеют контракты, которые можно использовать для закрепления политики или передачи обязательств по соблюдению требований. Так или иначе, в модели поставки FOSS операторы получают программное обеспечение несколькими путями. Хотя лица, оказывающие услуги по сопровождению проекта, предоставляют программное обеспечение в виде исходного кода для публичной загрузки, чаще всего оно распространяется через посредников, которые предоставляют устанавливаемые пакеты (например, «проект Debian»), продукты или услуги. Помимо

условий открытой лицензии лиц, оказывающих услуги по сопровождению проекта, оператор редко имеет договор с таким посредником. Только малая часть из них имеют контракт с лицами, оказывающими услуги по сопровождению проекта. Если и существуют договорные отношения, то они обычно касаются технической поддержки, а не самого FOSS.

3.2.3 Модель FOSS отделяет финансирование от использования

В отличие от физических товаров, программное обеспечение представляет собой всего лишь информацию и не имеет неотъемлемой материальной стоимости за каждую дополнительную произведенную единицу. Свобода использования и распространения FOSS означает, что лицензии предоставляют права, не требуя обмена на деньги. Пользователи, включая операторов интернет-инфраструктуры, могут финансировать разработку и поддержку FOSS, если захотят, но лицензия не обязывает их делать это, поэтому финансирование разработчиков не привязано к использованию их программного обеспечения.

3.2.4 FOSS часто не имеет единого ответственного юридического лица

В мире физических товаров довольно распространено предположение о существовании единого ответственного юридического лица, которое, в свою очередь, может быть субъектом политики или нести ответственность за соблюдение требований. В отличие от физических товаров, распространение программного обеспечения по всему миру часто осуществляется через интернет по очень низкой или нулевой стоимости. Это позволяет физическим лицам или группам лиц разрабатывать и распространять программное обеспечение без оплаты и без создания юридического лица. Проект Debian — яркий пример проекта[20] с открытым исходным кодом, не имеющего связанного с ним юридического лица. Программное обеспечение Debian используется в таких областях, как атомная энергетика, железнодорожный транспорт, промышленная автоматизация и медицинское оборудование. Хотя некоторые проекты FOSS имеют юридическое лицо, обеспечивающее управление, спонсорскую поддержку или даже трудоустройство, у большинства такого нет. Позже мы увидим, что DNS в этом отношении необычен: четыре небольшие организации профессионально поддерживают FOSS.

3.3 Закрытые проприетарные системы зависят от FOSS

Характеристики FOSS оказываются подходящими и для систем, которые сами по себе являются коммерческими (не FOSS). Это связано с тем, что современные коммерческие системы часто полагаются на FOSS для своего функционирования. Инструменты и библиотеки FOSS широко используются при разработке и развертывании коммерческого программного обеспечения. Например, большая часть программного обеспечения не

[20] Debian. «Наша философия: почему мы это делаем и как мы это делаем», https://www.debian.org/intro/philosophy.

создается без компиляторов или сред выполнения; программное обеспечение не может хранить объекты или структурированные данные без хранилищ объектов или баз данных; программное обеспечение не может взаимодействовать с другими компонентами без средства передачи сообщений. Эти внутренние функции обычно предоставляются FOSS.

В конкретном случае DNS полезным примером служит Cloudflare. Cloudflare управляет широко используемой публичным сервисом DNS, известной как резолвер «1.1.1.1». Первоначально сервис успешно работал с помощью Knot Resolver, представляющего собой FOSS; однако позднее его заменили проприетарным программным обеспечением, разработанным внутри компании.[21] Коммерческое программное обеспечение, лежащее в основе 1.1.1.1, написано на языке программирования Rust, а спецификации, эталонная реализация и его компилятор предоставляются некоммерческим фондом как FOSS.[22] Также используется tokio[23] — асинхронная среда выполнения, которая также является FOSS. Она работает на базе Linux, операционной системы FOSS, и окружена значительным набором других компонентов FOSS, которые обеспечивают мониторинг и другие эксплуатационные потребности.[24] Проприетарное программное обеспечение Cloudflare, лежащее в основе резолвера 1.1.1.1, работает в необходимом масштабе благодаря FOSS, а не вопреки ему.

3.4 Неотъемлемые преимущества FOSS в экосистеме DNS

Модель FOSS — это не просто теоретическая конструкция; ее принципы воплощаются в ощутимые преимущества, которые сделали ее доминирующей парадигмой для программного обеспечения инфраструктуры DNS. Свобода изучать, распространять и совершенствовать программное обеспечение в целом создает среду, способствующую транспарентности, устойчивости и инновациям. Это не случайные побочные продукты, а, скорее, неотъемлемые сильные стороны модели FOSS, которые оказались особенно подходящими для требований создания и обслуживания критически важной инфраструктуры интернета. В следующих разделах подробно описаны эти сильные стороны.

3.4.1 Транспарентность и безопасность за счет сотрудничества

Реализации DNS с открытым исходным кодом выигрывают от транспарентности. Доступность исходного кода для реализаций FOSS позволила мировому сообществу

[21] Анбанг Вен и Марек Вавруша. «Как Rust и Wasm обеспечивают работу Cloudflare 1.1.1.1». Блог Cloudflare, 28 февраля 2023 года. https://blog.cloudflare.com/big-pineapple-intro/.

[22] Фонд Rust. «О нас — миссия, руководство, совет директоров», https://rustfoundation.org/about/.

[23] Tokio. «Руководство», https://tokio.rs/tokio/tutorial.

[24] Джон Грэм-Камминг. «CloudFlare и программное обеспечение с открытым исходным кодом: улица с двусторонним движением». Блог Cloudflare, 7 октября 2013 года. https://blog.cloudflare.com/open source-two-way-street/.

разработчиков, исследователей и операторов выявлять и устранять уязвимости, зачастую быстрее, чем в коммерческих системах. Они уже несколько десятилетий[25] являются предметом активного изучения со стороны сектора науки и образования и специалистов по безопасности, что приводит к сообщениям об уязвимости как в протоколе DNS, так и в реализациях с открытым исходным кодом.[26]

В случае выявления уязвимостей тесные связи между этими тремя группами позволяют своевременно решать любые серьезные проблемы и координировать раскрытие информации и выпуск исправлений, обеспечивая полную защиту критически важных DNS-серверов (например, корневых) до того, как информация станет общедоступной, а также оперативное обновление всех остальных серверов.

В ходе опроса операторов инфраструктуры DNS (см. Приложение C) респонденты указали, что они ценят транспарентность своей цепочки поставок как мощную характеристику, позволяющую им ускорить устранение уязвимостей во взаимозависимых элементах программного обеспечения службы DNS, которую они используют. Например, смотрите следующие ответы:[27]

> Открытый исходный код БЫСТРО выявляет любые недостатки (как связанные с безопасностью, так и иные), исправляя их и распространяя гораздо быстрее, чем любая коммерческая организация.
>
> Крупные коммерческие организации, такие как [вымарано], [вымарано] и [вымарано], часто в течение многих лет выпускали исправления безопасности спустя долгое время ПОСЛЕ факта обнаружения уязвимости.
>
> Мы всегда отстаиваем ту точку зрения, что использование FOSS отвечает интересам всех: как пользователей, так и потребителей наших услуг. Это позволяет им удостовериться, что мы используем надежные программные компоненты. В редких случаях, когда в используемом нами программном обеспечении обнаруживается проблема безопасности, она открыто обсуждается и оперативно устраняется — в отличие от того, что мы наблюдаем в случае с коммерческим программным обеспечением.

---

[25] Например, см. статью Пола Викси «Проблемы безопасности DNS и BIND» в *материалах пятого симпозиума по безопасности USENIX UNIX*, Солт-Лейк-Сити, штат Юта, 1995 год. https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/vixie.pdf.

[26] Чтобы проиллюстрировать понятие «активный предмет исследования», см., например, резюме результатов 23 исследовательских работ, опубликованных в 2024 году по безопасности DNS, представленное Чаои Лу в «Обзоре научных работ по DNS и безопасности, опубликованных в 2024 году» (презентация, ICANN82, Сиэтл, штат Вашингтон, 12 марта 2025 год), https://static.sched.com/hosted_files/icann82/7b/1.1%20chaoyi-dnspapers2024-0304.pdf.

[27] Консультативный комитет по безопасности и стабильности ICANN, «Опрос ICANN SSAC о предполагаемом влиянии регулирования ПО с открытым исходным кодом на инфраструктуру DNS», личное сообщение, февраль 2025 года.

> Существует множество примеров коммерческого программного обеспечения с проблемами безопасности и плохой историей транспарентности или исправлений. Сообщество FOSS справляется с работой лучше большинства поставщиков в обоих направлениях.

Использование и управление бесплатным и открытым программным обеспечением DNS активно и открыто обсуждается операторами публично. Каждая из ведущих систем программного обеспечения DNS имеет публичный лист[28] рассылки для пользователей и общедоступную базу данных ошибок и проблем, доступную для всеобщего просмотра.[29] Сообщество DNS сотрудничает в своей деятельности и исследованиях через отраслевую организацию Центр исследований и анализа работы DNS (DNS-OARC).[30] Такая культура открытого общения способствует более быстрому и широкому информированию о проблемах с работой, ошибках программного обеспечения, несовместимости между реализациями и ошибками операторов, которые влияют на другие части системы.

3.4.2 Стабильность и долгосрочная поддержка

В целом FOSS широко полагается на поддержку со стороны волонтеров, часто одного человека. В случае DNS четыре ведущих решения с открытым исходным кодом разработаны четырьмя различными организациями (тремя некоммерческими учреждениями и одной коммерческой компанией) из разных стран и территорий Северной Америки и Европы.[31] Все четыре компании были созданы на заре массового внедрения интернета и достигли стабильности в источниках дохода и внутренней организации. Каждая из этих организаций руководит разработкой своего программного обеспечения, посредством написания нового кода, а также просматривая и проверяя предоставляемый код от активных сообществ, разбросанных по всему миру. Долгосрочные обязательства этих организаций-спонсоров и централизованный технический контроль изменений программного обеспечения помогают снизить проблемы качества, безопасности и надежности, характерные для проектов FOSS, разрабатываемых без строгого технического контроля. Культура технического сообщества DNS с открытым исходным

[28] Например, см. публичные листы рассылки CZnic (https://lists.nic.cz/postorius/lists/knot-resolver-users.lists.nic.cz/), NLnet Labs (https://www.nlnetlabs.nl/support/mailing-lists/), и PowerDNS (https://mailman.powerdns.com/mailman/listinfo/).

[29] Например, см. отслеживание проблем для CoreDNS (https://github.com/coredns/coredns/issues) и BIND 9 (https://gitlab.isc.org/isc-projects/bind9/-/issues/).

[30] Центр исследований и анализа работы DNS. «Введение в DNS-OARC», 3 июля 2008 года. https://www.dns-oarc.net/oarc/info.

[31] В алфавитном порядке: CZNIC — ассоциация чешских интернет-провайдеров («ISP»), основанная в 1998 году; Internet Systems Consortium, Inc. («ISC») — американская некоммерческая корпорация, созданная в 1994 году специально для поддержки программного обеспечения с открытым исходным кодом и систем для инфраструктуры интернета; NLnet Labs — нидерландская некоммерческая организация, основанная в 1999 году для разработки открытых стандартов и программного обеспечения с открытым исходным кодом для DNS и междоменной маршрутизации; и PowerDNS — нидерландская компания, основанная в 1999 году для поддержки разработки специализированного программного обеспечения DNS для интернет-провайдеров.

кодом такова, что злоумышленнику потребуются длительные и последовательные усилия, чтобы выстроить связи и репутацию, необходимые для того, чтобы занять роль, требующую доверия.

3.4.3 Операционная отказоустойчивость за счет многообразия

Высокая доступность, требуемая от служб DNS, подразумевает необходимость резервного дублирования и предотвращения единых точек отказа. Для многих операторов это подразумевает использование нескольких независимых реализаций DNS в программном обеспечении. Операторы, использующие аутсорсинг, также могут использовать стратегию привлечения нескольких провайдеров. Это создает внутреннюю потребность в существовании нескольких решений, чтобы операторы высоконадежных служб могли запускать два или более решений параллельно и избегать зависимости от какого-либо отдельного разработчика программного обеспечения или полной уязвимости к проблемам в каком-либо одном продукте. Доступность FOSS DNS снижает барьеры для организаций, желающих эксплуатировать собственную инфраструктуру, предоставляя возможность избежать рыночной концентрации и централизации рынка.[32]

3.4.4 Вспомогательный механизм экономического роста и инноваций

Известно, что бесплатное и открытое программное обеспечение — движущая сила прогресса.[33,34] Как мы увидели, множество продуктов с открытым исходным кодом легко и бесплатно доступны любому человеку, нуждающемуся в программном обеспечении DNS, в любой точке мира. Система ориентирована на интернет-провайдеров, регистратуры, регистраторов и интернет-пользователей. Физические лица, некоммерческие организации, стартапы и эксперты в предметной области, которые не могут позволить себе стоимость лицензий на коммерческое программное обеспечение, могут получить необходимое им программное обеспечение бесплатно. Как заявил респондент опроса операторов DNS (см. Приложение C): «Сегодня меня больше всего

[32] Марк Ноттингем. «RFC 9518: централизация, децентрализация и стандарты интернета». Запрос комментариев Инженерная проектная группа интернета, 18 декабря 2023 года. https://datatracker.ietf.org/doc/rfc9518/.

[33] «В анализе содержится оценка соотношения затрат и прибыли более чем 1:4 и прогнозируется, что увеличение вкладов в программное обеспечение с открытым исходным кодом на 10% ежегодно будет генерировать дополнительные 0,4–0,6% ВВП, а также более 600 новых стартапов в сфере информационных и коммуникационных технологий в ЕС. Практические исследования показывают, что, приобретая ПО с открытым исходным кодом вместо коммерческого, государственный сектор может снизить общую стоимость владения, избежать привязки к поставщику и, таким образом, повысить свою цифровую автономность». От Европейской Комиссии. Генеральный директорат по коммуникационным сетям, контенту и технологиям. *Влияние открытого программного обеспечения и аппаратного обеспечения на технологическую независимость, конкурентоспособность и инновации в экономике ЕС: итоговый отчет исследования*. Люксембург: издательство ЕС, 2021 год. https://data.europa.eu/doi/10.2759/430161.

[34] Райт, Наталия Лэнгбурд, Фрэнк Нэгл и Шейн Гринштейн. «Открытое программное обеспечение и глобальное предпринимательство». *Research Policy* 52, № 9 (2023): 104846. https://doi.org/10.1016/j.respol.2023.104846.

волнует то, что мы используем так много компонентов с открытым исходным кодом в некритических частях нашего стека, на которые у нас нет контрактов на поддержку, что в целом мы не смогли бы позволить себе лицензирование, даже если бы оно предлагалось».[35]

Существование множества решений FOSS для DNS оказывает положительное влияние на техническое и коммерческое развитие использования интернета, а также программного обеспечения для него и услуг в целом, как с открытым исходным кодом, так и коммерческого. Многие коммерческие системы и размещенные сервисы в значительной степени зависят от компонентов с открытым исходным кодом для обеспечения критически важных функций; многие коммерческие платформы для облачных и интернет-служб используют в качестве компонента один из продуктов FOSS для DNS.[36] В то же время значительная часть инфраструктуры DNS зависит от криптографических библиотек бесплатного и открытого программного обеспечения, таких как OpenSSL. Аналогичным образом Linux, операционная система с открытым исходным кодом, служит основой для значительной части облачной инфраструктуры, серверных сред и устройств интернета вещей (IoT). Эта основополагающая роль подчеркивает глубокое влияние FOSS на технологические инновации. Проприетарное программное обеспечение часто включает в себя эти платформы FOSS при создании приложений с закрытым исходным кодом или функций в дополнение к ним, что создает симбиотическую связь между двумя моделями.[37]

3.4.5 Вклад в цифровую автономию

Поскольку использование FOSS, как правило, не требует оплаты лицензий или компенсаций, размер капитала, необходимого для запуска новых цифровых предприятий, может быть ниже, чем при использовании коммерческого программного обеспечения. Более того, свобода изучать, изменять и распространять код, предоставляемый FOSS, способствует развитию локальных знаний и навыков, что приводит к новым исследовательским и бизнес-проектам. Локальная адаптация или дальнейшие разработки не требуют какого-либо разрешения или согласия со стороны первоначальных авторов. Любой сервис, основанный на FOSS, не может быть заблокирован иностранными

[35] Консультативный комитет по безопасности и стабильности ICANN, «Опрос SSAC ICANN о предполагаемом влиянии регулирования ПО с открытым исходным кодом на инфраструктуру DNS».

[36] В настоящее время не существует единственного независимого источника, подтверждающего это утверждение. Однако на основании исследования, проведенного коллективно авторами данной статьи, мы можем с уверенностью утверждать, что это действительно так. Существуют проблемы с конфиденциальностью, связанные с публичным раскрытием информации о том, какая именно платформа использует тот или иной сервис, и поэтому это вполне обоснованное заявление без надлежащей документации.

[37] Гортмейкер, Джефф. «Политика в области открытого программного обеспечения в условиях отраслевого равновесия» Рабочий документ, технический отчет, 2024 год. https://jeffgortmaker.com/files/Open_Source_Software_Policy_in_Industry_Equilibrium.pdf.

правообладателями, поскольку лицензии на него не могут быть отозваны. Даже в случае торговых конфликтов и эмбарго, код останется доступным.

3.5 Риски, присущие модели FOSS

Хотя модель FOSS обладает значительными преимуществами, ее уникальные характеристики также несут в себе особый набор рисков, которые отличаются от рисков традиционного коммерческого программного обеспечения. Это не недостатки самой модели, а скорее присущие ей компромиссы, которые следует понимать и которыми необходимо управлять, особенно когда программное обеспечение используется в критической инфраструктуре. Экономическая модель, распределенный характер разработки и отсутствие традиционных договорных отношений оказывают влияние на долгосрочную устойчивость и операционную безопасность. В следующих разделах эти неотъемлемые риски описываются подробно.

3.5.1 Финансовая устойчивость и выгорание лиц, оказывающих услуги по сопровождению проекта

Одной из основных угроз для DNS является общая проблема финансовой устойчивости FOSS. Модель отделяет финансирование от использования (Раздел 3.2.3), что обеспечивает широкое внедрение, но также допускает бесплатное использование,[38] когда весь мир может зависеть от программного обеспечения, финансируемого немногими.[39,40]

Как отмечается в отчете Консультативной группы по технологиям широкополосного интернета (BITAG):

> Существует разрыв между покупкой сетевого оборудования с дорогостоящими контрактами на поддержку и отсутствием финансирования программного обеспечения с открытым исходным кодом, от которого во многих случаях зависит это самое оборудование. Зачастую технический персонал сетевых операторов готов поддерживать разработку, но их корпоративная структура не позволяет этого,

[38] Джастин Паппас Джонсон. «Очерки микроэкономической теории». Диссертация, Массачусетский технологический институт, 1999 год. http://hdl.handle.net/1721.1/9518.

[39] Джон Кристофф, Александр Бэнд, Онджей Филип и Джефф Осборн. *Панельная дискуссия: Core Systems OSS*. NANOG 84, 2022 год. https://www.youtube.com/watch?v=vWiW-3jMw7w.

[40] Например, в одном из отчетов подчеркивается дисбаланс между использованием необходимого программного обеспечения для маршрутизации и финансовыми вкладами в его разработку: «Мы иллюстрируем актуальность этого дисбаланса между финансированием и использованием... на двух примерах. По оценкам, из 2000 установок программного обеспечения Routinator RP и 1400 сетей, использующих программное обеспечение делегированного CA Krill, менее десяти финансируют свою разработку. Большинство операторов рассчитывают на стабильность, непрерывность существования и будущее развитие программного обеспечения, но не способствуют достижению этой цели». Техническая рабочая группа Технической консультативной группы по широкополосному интернету (BITAG), «Безопасность инфраструктуры маршрутизации интернета», 2 ноября 2022 года, 26, https://www.bitag.org/documents/BITAG_Routing_Security.pdf.

> поскольку такое программное обеспечение нельзя купить в запечатанной коробке с контрактом на поддержку. Спонсирование разработки какой-либо функции может быть проблематичным, поскольку юридические отделы по умолчанию исходят из того, что разработка программного обеспечения приводит к тому, что спонсор [на эксклюзивной основе] владеет интеллектуальной собственностью, что несовместимо с моделью бесплатного и открытого программного обеспечения.[41]

Хотя четыре ведущие реализации DNS с открытым исходным кодом сопровождаются организациями, добившимися устойчивой финансовой и организационной стабильности, все они являются небольшими организациями. Любая из них может быть дестабилизирована, если их источник финансирования окажется под угрозой или если регулирование наложит на них бремя, превышающее их способность покрыть сопутствующие расходы. Если одна из ведущих систем с открытым исходным кодом потеряет поддержку сопровождающих или станет полностью недоступной, это может оказать существенное влияние на DNS.

Это особенно актуально для основополагающих инструментов, которые требуют постоянного обслуживания, но оторваны от основных бизнес-процессов своих пользователей. Четыре наиболее популярные реализации DNS с открытым исходным кодом поддерживаются группами разработчиков, состоящими не более чем из дюжины инженеров, поэтому добавление требований к проекту, которые могли бы потребовать, например, эквивалента полной занятости персонала, стало бы существенной проблемой.

Финансирование коммерческих лиц, оказывающих услуги по сопровождению проекта, осуществляется разными способами, некоторые из которых могут оказаться неожиданными. Помимо приема пожертвований и предоставления частной технической поддержки, некоторые проекты предлагают финансовым спонсорам ранний доступ к исправлениям ошибок, поддержку веток, выведенных из поддержки, приоритетную разработку функций, доступ к предварительно скомпилированным пакетам и дополнительным службам безопасности.[42,43,44,45] Регулирующим органам следует

---

[41] Техническая рабочая группа BITAG, «Безопасность инфраструктуры маршрутизации интернета», 26.

[42] Например, Консорциум интернет-систем предлагает услугу раннего оповещения об уязвимостях. См. Консорциум интернет-систем, «Раннее уведомление об уязвимостях (EVN)», https://www.isc.org/evn/.

[43] NLnet Labs предоставляет услуги по обучению, консультированию, технической поддержке и разработке программного обеспечения через свою дочернюю компанию Open NetLabs. См. NLnet Labs, «Услуги Open Netlabs — консультации», https://nlnetlabs.nl/services/consultancy/.

[44] PowerDNS предлагает множество услуг и продуктов, включая PowerDNS Protect — службу безопасности, включающую защитные блок-листы. См. «PowerDNS Protect», https://www.powerdns.com/powerdns-protect.

[45] Обзор различных видов организационных моделей с открытым исходным кодом см. в статье «Архетипы открытого исходного кода: рамочная модель для осмысленного Open-Source», Open Tech Strategies, Mozilla Corporation, 28 октября 2019 года, https://blog.mozilla.org/wp-content/uploads/2018/05/MZOTS_OS_Archetypes_report_ext_scr.pdf.

проявлять осторожность, чтобы случайно не запретить какие-либо из этих возможных путей финансирования деятельности тех, кто поддерживает FOSS.

FOSS для DNS является исключением в том смысле, что здесь вообще существуют долгоживущие организации, которые нанимают коммерческих лиц, оказывающих услуги по сопровождению проекта. Главный риск для их дальнейшего существования — *финансовая устойчивость*. Но в общем и в целом риск мотивирует. Сопровождение подавляющего большинства проектов FOSS осуществляется одним человеком в свободное время.[46] Примером является программное обеспечение DNS, которое чаще всего встроено в небольшие недорогие маршрутизаторы, используемые дома и на малых предприятиях, а именно Dnsmasq. Большую часть времени его сопровождение осуществляется одним волонтером, работающим преимущественно бесплатно.[47] Аналогично, сопровождение нескольких программных библиотек высокого уровня для программирования DNS фактически осуществляется одним человеком в свободное время.[48] Другая популярная реализация DNS, CoreDNS и лежащая в её основе библиотека Go DNS, поддерживаются усилиями сообщества и одним волонтером, оказывающим услуги по сопровождению проекта. Эти примеры подчеркивают определяющую характеристику экосистемы программного обеспечения: небольшая организация или отдельный разработчик могут играть решающую роль в написании программного обеспечения для всемирной цифровой инфраструктуры, при этом будучи полностью отделенными от капитальных или операционных расходов на ее использование. В отношении этих независимых волонтеров, оказывающих услуги по сопровождению проекта, если их работа не будет финансироваться как основная, постоянная работа, риск заключается не в финансовой устойчивости, а в выгорании. Регулирующие органы должны быть осторожны и не налагать дополнительную нагрузку, выходящую за рамки возможностей и желания лиц, оказывающих услуги по сопровождению проекта, вкладывать свободное время в поддержание проектов, которые по сути являются хобби-проектами. Это область активных исследований, и политикам стоит принять во внимание рекомендации ученых.[49]

3.5.2 Риск для цепочки поставок из-за общих взаимозависимых элементов

Значительная часть критически важного программного обеспечения, включая как FOSS, так и коммерческое программное обеспечение, использует некоторые из одних и тех же

[46] Джош Брессерс. «Открытый исходный код — это один человек». Безопасность открытого исходного кода, 28 августа 2025 года. https://opensourcesecurity.io/2025/08-oss-one-person/.

[47] «Dnsmasq — сетевые службы для небольших сетей», https://thekelleys.org.uk/dnsmasq/doc.html.

[48] В качестве примеров можно привести *Net::DNS* для языка программирования Perl и *miekg/dns*, библиотеку Go DNS, используемую в Kubernetes, Docker и центре сертификации Let’s Encrypt. Больше примеров библиотек можно найти в Таблице 7.

[49] Надия Эгбал. «Маршрутизаторы и сетевые мосты: невидимый труд, стоящий за нашей цифровой инфраструктурой». Фонд Форда, 14 июля 2016 года. https://www.fordfoundation.org/work/learning/research-reports/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure/.

компонентов FOSS. Серьезная ошибка в популярной криптографической библиотеке FOSS[50] может повлиять на все реализации DNS.[51] Существуют и другие, менее заметные, но часто повторно используемые компоненты. Это существенная потенциальная уязвимость не только для DNS, не только для бесплатного и открытого программного обеспечения, но и для всего программного обеспечения в целом.[52] Риски для устойчивости, обсуждавшиеся выше в разделе 3.5.1, относятся и к этим общим компонентам, что усугубляет угрозу.

Этот риск усугубляется тем фактом, что разработчики FOSS со злым умыслом могут незаметно внедрить вредоносный код в проекты с открытым исходным кодом или их компоненты. Он может быть внедрен посредством вмешательства в репозитории пакетов или в качестве вклада в проекты. Необходимо проявлять бдительность при проверке и мониторинге взаимозависимых элементов кода, чтобы не допустить внедрения вредоносного кода в программные проекты.

3.5.3 FOSS не предоставляет никаких гарантий и не гарантирует поддержку

Бесплатное программное обеспечение является привлекательным выбором, поскольку оно предоставляется бесплатно и обычно не требует никаких дополнительных усилий, кроме загрузки пакета. Но поскольку на него не распространяется никакая гарантия и оно не обещает никакой поддержки, его использование также сопряжено с рисками. По умолчанию не существует никакого другого договора, кроме лицензионного соглашения FOSS между провайдером такого продукта и пользователем.[53] Если пользователь не заключит собственные соглашения об обслуживании с лицами, оказывающими услуги по сопровождению проекта, у него нет гарантии активного обслуживания или поддержки.

---

[50] OpenSSL — классический пример широко распространенной криптографической библиотеки. Чтобы проиллюстрировать масштаб этой зависимости, на момент обнаружения уязвимости «Heartbleed» в OpenSSL примерно 17% серверов интернета, сертифицированных доверенными органами, считались уязвимыми для атак. Netcraft, «Полмиллиона пользующихся большим доверием сайтов уязвимы для Heartbleed», Netcraft News, 8 апреля 2014 года, https://web.archive.org/web/20141119102520/http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html.

[51] Как и программное обеспечение DNS, разработка криптографического программного обеспечения — это работа для специалистов. Хотя существуют некоторые старые криптографические алгоритмы FOSS, их разнообразие и качество представляют проблему.

[52] Пример одной из попыток обратить внимание на общие взаимозависимые элементы см. «Перепись бесплатного и открытого программного обеспечения III», *The Linux Foundation*, декабрь 2024 года: https://www.linuxfoundation.org/research/census-iii

[53] Наличие договорных отношений между лицами, оказывающими услуги по сопровождению проекта, и операторами является распространенным заблуждением, которое рассматривается в разделе 3.2.2.

Если в продукте обнаружены уязвимости безопасности, будь то случайно внесенные, как в случае с ошибкой OpenSSL Heartbleed,[54] или злонамеренные, как в случае с обходом системы защиты в xz Utils,[55] никто не обязан предоставлять исправления. Хотя технически любой человек, включая пользователя, может взять копию исходного кода и исправить проблему вручную, такое «ответвление» требует значительных знаний в области разработки программного обеспечения и операционных ресурсов, так что в большинстве случаев пользователь фактически не имеет никакого контроля над доступностью исправлений. Эта проблема особенно серьезна в пакетах, которые, как OpenSSL и xz, настолько широко используются, что для них нет легкодоступных заменителей. Риски монокультуры не ограничиваются открытым исходным кодом, но это может быть причиной того, почему эти общие риски применимы и к FOSS.

Снижение интереса сообщества к предоставлению услуг по обслуживанию FOSS может рассматриваться как стимул для появления организаций, предлагающих обслуживание по контракту. Однако изменения в кодовой базе, вносимые этими организациями поддержки, обычно передаются обратно в проект FOSS, чтобы минимизировать нагрузку по сопровождению отдельной базы кода. В свою очередь, это позволяет другим получать выгоду от этого обслуживания, не платя за него самим. Это приводит к проблеме бесплатного использования: когда провайдер услуг использует FOSS, но не вносит вклад в его поддержку, он может делать это по более низкой цене, чем конкурент, который это делает, тем самым подрывая его позиции.[56]

Отсутствие неотъемлемой гарантии или поддержки можно компенсировать. Операторы могут обучать и удерживать штатных экспертов, финансировать или нанимать лиц, оказывающих услуги по сопровождению проекта[57], или заключать контракты на поддержку, чтобы получить доступ к экспертным знаниям лиц, оказывающих услуги по сопровождению проекта, или опытных участников проекта.[58] Отчет BITAG, цитируемый в

[54] «Ошибка Heartbleed», https://heartbleed.com/.

[55] Дэн Гудин. «Что мы знаем о лазейке в xz Utils, которая чуть не заразила мир». Ars Technica, 1 апреля 2024 года. https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/.

[56] Например, немецкая бизнес-ассоциация разработчиков FOSS указала на эту проблему при его государственных закупках. См. статью рабочей группы по закупкам Open Source Business Alliance, «Критерии отбора для устойчивых закупок программного обеспечения с открытым исходным кодом», Open Source Business Alliance, 11 февраля 2025 года, https://osb-alliance.de/publikationen/veroeffentlichungen/selection-criteria-for-the-sustainable-procurement-of-open source-software.

[57] Филиппо Вальсорда. «Теперь я штатный профессиональный специалист, оказывающий услуги по сопровождению ПО с открытым исходным кодом», 2 февраля 2023 года. https://words.filippo.io/full-time-maintainer/.

[58] Контракты на поддержку доступны для нескольких систем FOSS, рассматриваемых в данном отчете.

разделе 3.5.1, иллюстрирует организационные препятствия, которые мешают операторам делать это.

3.5.4 Операционные риски при развертывании

Распределенный характер FOSS создает операционные проблемы, связанные с аутентичностью программного обеспечения, установкой исправлений и нехваткой квалифицированных операторов.

Проверка подлинности программного обеспечения

Бесплатное и открытое программное обеспечение свободно распространяется через интернет и, следовательно, может быть перехвачено или заменено поддельным кодом. Из-за этого риска FOSS обычно подписывается с использованием надежных криптографических методов лицом, оказывающим услуги по сопровождению проекта. Пользователь может проверить эти подписи, чтобы убедиться в целостности программного обеспечения. Все наиболее популярные реализации FOSS для DNS, используемое в инфраструктуре интернета, имеют такие подписи. Однако пользователи могут не проверять эти подписи или получать программное обеспечение через посредников, которые не проверяют и иным образом не поддерживают целостность программного обеспечения.

Отсутствие информации о развертывании и скорости получения исправлений

Исследователи проявляют большой интерес к поиску уязвимостей в FOSS для DNS и имеют большой опыт их обнаружения и сообщения о них. Каждый из ведущих поставщиков программного обеспечения для DNS следует общепринятым передовым практикам реагирования на уязвимости программного обеспечения, их исправления и раскрытия. Однако нет надежного источника информации о том, обновляют ли пользователи свое программное обеспечение до текущих, улучшенных версий, и если да, то как быстро.

В целом в бесплатном и открытом программном обеспечении имеется ограниченное количество данных, с которыми можно было бы работать при оценке этого риска. Тот факт, что потребители программного обеспечения часто получают его через третью сторону —как пакет для операционной системы или от энтузиаста FOSS, который может скопировать и распространять программное обеспечение, — еще больше затрудняет отслеживание обновлений. Этот риск можно снизить с помощью правил, требующих от операторов предоставления централизованной отчетности по любому программному обеспечению, имеющему решающее значение для их производственных операций.

Аутсорсинг и нехватка навыков

Сложность правильной работы с FOSS является проблемой, поскольку в некоторых частях мира ощущается нехватка квалифицированных операторов. Такое сочетание критичности

и сложности заставляет некоторых лиц, принимающих решения, передавать задачи на аутсорсинг облачным сервисам, что может ослабить разнообразие и распределенный характер системы, потенциально снижая ее отказоустойчивость и безопасность. Например, если все жители региона выбирают популярного поставщика услуг электронной почты, потому что это проще, чем создавать, эксплуатировать и поддерживать собственные почтовые серверы, то доступность электронной почты во всем регионе будет определяться стабильностью работы одного почтового провайдера.

Также наблюдается смена поколений на предприятиях и в компаниях с небольшими объемами работы: сотрудники более молодого возраста все больше полагаются на облачные сервисы и меньше знакомы с работой собственных сетевых служб. Несколько организаций проводят обучающие мероприятия для операторов (APNIC, NSRC, PCH) с целью развития навыков управления DNS и других навыков управления сетями. Проекты FOSS пытаются решить эту проблему с помощью предварительно скомпилированных пакетов и простых в использовании функций, но конкурировать с альтернативами «программное обеспечение как услуга» тем не менее сложно.

4 Распространенность FOSS в инфраструктуре DNS и регистрации доменных имен

FOSS играет решающую и доминирующую роль в технических операциях систем доменных имен и их регистрации в интернете. В наиболее важных частях этой инфраструктуры FOSS является нормой, а коммерческое программное обеспечение — исключением. Исследование, представленное в данном отчете, устанавливает, что глобальная и распределенная инфраструктура DNS зависит от FOSS. По крайней мере девять из 12 операторов системы корневых серверов в интернете используют в DNS исключительно реализации FOSS. Аналогичным образом, девять из десяти крупнейших провайдеров услуг для доменов верхнего уровня используют FOSS. В сфере регистрации доменных имен, хотя многие крупные системы являются коммерческими, они в подавляющем большинстве построены на компонентах FOSS, также, как и основные провайдеры услуг по временному депонированию данных для регистратур и регистраторов. В следующих разделах подробно описывается распространенность FOSS в каждом компоненте этой критической инфраструктуры. Методология описана в Приложении B.

4.1 FOSS в инфраструктуре регистрации доменных имен

Инфраструктура регистрации относится к системам, которые обеспечивают регистрацию отдельных доменных имен и делают зарегистрированные доменные имена доступными в публичной DNS. Хотя точные данные о масштабах использования FOSS отсутствуют, имеющиеся данные свидетельствуют о глубокой зависимости от него как комплексных систем, так и основополагающих компонентов.

Ряд операторов регистратуры поддерживают инфраструктуру регистрации, которая полностью представляет собой FOSS (Таблица 1). Например, известно, что платформа регистратуры FRED используется по меньшей мере 12 регистратурами ccTLD, а платформа Nomulus используется несколькими регистратурами gTLD.

Таблица 1. Системы FOSS, используемые регистратурами

Система программного обеспечения	Лицензия открытого исходного кода	Кем используется
FRED	GPLv3	FRED используется (по крайней мере) в ccTLD Албании, Анголы, Аргентины, Боснии и Герцеговины, Коста-Рики, Чешской Республики, Лесото, Макао, Малави, Северной Македонии, Парагвая и Танзании.
Регистратура интернет- доменов в зоне .ee	MIT	ccTLD для Эстонии (.ee).
Namingo	MIT	Namingo разработан для Программы ICANN New gTLD 2026 года: следующий раунд.
Nomulus	Apache 2.0	Регистратуры Google gTLD, включая .app и т. д.

Таблица 2. Системы регистратур, построенные на компонентах FOSS

Система регистратуры / backend-сервис	Примеры использования компонентов с открытым исходным кодом	Кем используется регистратура
Afnic	Сервер, База данных	20 доменов верхнего уровня, включая .fr
CIRA / SIDN / Hello Registry	База данных, сервер, сервер приложений, отчетность, интерфейс	6 национальных доменов верхнего уровня, 6 доменов общего пользования верхнего уровня, включая .ca, .ie
CoCCA	Сервер, сервер приложений, база данных	56 национальных доменов верхнего уровня
CORE Association	Сервер, база данных, библиотеки Java	1 национальный домен верхнего уровня, 21 домен общего пользования верхнего уровня

Система регистратуры / backend-сервис	Примеры использования компонентов с открытым исходным кодом	Кем используется регистратура
GoDaddy Registry	База данных, серверы приложений, отчетность, мониторинг, ведение журнала, тестирование, интерфейс, DNS	Более 200 доменов верхнего уровня
Identity Digital	База данных	250 gTLD и ccTLD, включая ccTLD .au, .me, .pr
Nominet	База данных, сервер приложений, анализ, ведение журнала, тестирование, интерфейс, сервер имен	Более 85 доменов верхнего уровня, включая .uk
TANGO Registry Services	Сервер, база данных, библиотеки Java	8 доменов общего пользования верхнего уровня
Tucows Registry	База данных, программное обеспечение DNS и вспомогательные инструменты, серверы и почтовые серверы, очереди сообщений, оркестровка и виртуализация инфраструктуры, операционная система	222 «TLD», включая SLD, управляемые как TLD, в том числе .my и com.my
Verisign[59]	(ничего не предоставлено)	.com, .net, .edu и другие домены верхнего уровня

[59] Компания Verisign предоставила следующее заявление для этого отчета: «Verisign использует проприетарную платформу разрешения DNS Advanced Transaction Lookup and Analysis System (ATLAS). Verisign также использует специализированную инфраструктуру регистрации и разрешения, которая использует разнообразный и тщательно подобранный набор коммерческих и открытых программных компонентов для обеспечения избыточности».

Напротив, крупнейшие регистраторы и серверы регистратур часто используют проприетарные системы. Однако такие системы, как правило, не создаются с нуля; зачастую они основаны на проприетарных, оптимизированных расширениях и интегрированных компонентах, таких как базы данных и серверы, которые в основном являются FOSS (Таблица 2).

Такая зависимость от FOSS также характерна и для служб временного депонирования данных, которые надежно хранят копии регистрационных данных доменных имен. Три крупнейших провайдера этих услуг как для регистратур, так и для регистраторов построили свои системы, по крайней мере частично, на компонентах FOSS(Таблица 3).

Таблица 3. FOSS у провайдеров услуг временного депонирования данных

Провайдер услуг временного депонирования данных	Для регистратур	Для регистраторов	Интегрирует ли FOSS в ключевые функции?
Beilong Zedata (Beijing) Data Technology Co., Ltd	✓	✓	Нет
Сетевой информационный центр Китая (CNNIC)	✓	✓	Нет
Центр администрирования IDN Китая (CONAC)	✓	✓	Нет
DENIC Services GmbH & Co. KG	✓	✓	Да, частично
Escrow4All	✓		Да
Акционерное общество «Центр взаимодействия компьютерных сетей «МСК-IX»	✓	✓	Неизвестно
NCC Group	✓		Да, частично
Сетевой информационный центр Тайваня (TWNIC)	✓		Нет

Измерение показателей и обследование инфраструктуры регистраторов для данного отчета не производились. Мы считаем вероятным, что регистраторы регулярно используют проприетарные, оптимизированные расширения и интегрированные компоненты, которые в основном являются FOSS. Например, некоторые регистраторы используют программное обеспечение сервера nginx или Apache для управления своими порталами для владельцев доменов. Они также используют решения FOSS для мониторинга программного обеспечения, анализа данных, управления кодом и других нужд.

4.2 FOSS в инфраструктуре публикации DNS (авторитативные серверы)

Доказательства доминирования FOSS наиболее очевидны в инфраструктуре, публикующей информацию о доменах. На самых высоких уровнях иерархии DNS — корневом и TLD — FOSS встречается практически повсеместно.

Система корневых серверов — это самый верхний уровень иерархии DNS. Из 12 независимых организаций, которые управляют корневыми серверами, по крайней мере девять используют для DNS исключительно реализации FOSS для ответов на запросы (Таблица 4).

Таблица 4. Использование FOSS в системе корневых серверов

Идентификатор корневого сервера	Программное обеспечение	с открытым исходным кодом[60]
A, J	ATLAS (коммерческое) NSD	Частично[61]
B	Knot BIND9	Да.[62,63]
C	BIND9	Да
D	NSD	Да
E	*неизвестно* (FOSS), *внутреннее* (коммерческое)[64]	Частично[65]

[60] Виллем Тороп и др., «Отчет об исследовании внедрения RSSAC028» (отчет, NLnet Labs и Stichting Internet Domeinregistratie Nederland (SIDN), 27 сентября 2023 года), 15, https://www.icann.org/en/system/files/files/rssac028-implementation-study-report-27sep23-en.pdf.

[61] Из заявления Verisign об ожиданиях от корневых серверов в отношении услуг RSSAC001v2: «Verisign использует две различные кодовые базы для услуг корневой зоны DNS: (1) наша проприетарная запатентованная платформа разрешения ATLAS и (2) программное обеспечение с открытым исходным кодом NLnet Labs Name Server Daemon (NSD). «В любой момент времени может использоваться одна, другая или обе реализации», https://a.root-servers.org/aroot-rssac001v2-expectations.pdf.

[62] «Корневой DNS-сервер USC/ISI», https://b.root-servers.org/.

[63] «RSSAC023v2: история системы корневых серверов». Консультативный комитет системы корневых серверов ICANN (RSSAC), 17 июня 2020 года. https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf.

[64] Дэни Грант. «Обслуживание корня DNS». Блог Cloudflare, 10 сентября 2017 года. https://blog.cloudflare.com/f-root/.

[65] Ральф Бишоф. «:Инстанс E-Root в Сан-Франциско возвращает SERVFAIL?», 19 июня 2025 года https://lists.dns-oarc.net/pipermail/dns-operations/2025-June/022899.html.

Идентификатор корневого сервера	Программное обеспечение	с открытым исходным кодом[60]
F	BIND9, *внутреннее* (проприетарное)[66]	Частично
G	BIND9	Да
H	NSD	Да
I	*конфиденциально*	Да[67]
K	BIND9 Knot NSD	Да
L	Knot NSD	Да
M	BIND9	Да[68]

Если говорить о доменах ccTLD и gTLD, то мы обнаруживаем, что девять из десяти ведущих операторов, предоставляющих авторитативные DNS-серверы для регистратур доменов верхнего уровня, используют для этого FOSS.[69]

Ниже корневого уровня и доменов верхнего уровня авторитативные серверы имен обслуживаются широким кругом организаций, включая частных лиц, предприятия, университеты и правительства. Хотя для всей этой разнообразной группы отсутствуют полные данные, известно, что многие из тех же систем FOSS, которые используются в корне и доменах верхнего уровня, также являются наиболее популярным выбором для этих операторов. Многие из организаций, предлагающих вторичный DNS, являются теми же организациями, которые предоставляют авторитативные DNS-серверы для доменов верхнего уровня. В таблицах 5 и 6 перечислены системы FOSS и коммерческие продукты, подходящие для авторитативных реализаций DNS.

Авторитативные серверы имен часто интегрируются с системами предоставления услуг, чтобы упростить обновление информации о зоне и реализовать надлежащую авторизацию и контроль за ведением этих записей. Некоторые из наиболее популярных систем предоставления услуг являются FOSS.[70]

[66] Грант, «Доставка DNS по TLS».
[67] Публикуется с разрешения Netnod в переписке с SSAC от 13 декабря 2024 года

[68] «DNS-сервер M-Root» https://m.root-servers.org/.

[69] Ведущие операторы по количеству обслуживаемых доменов верхнего уровня. Описание использованной методологии см. в Приложении B.
[70] Популярные системы включают VinylDNS (https://www.vinyldns.io/), сопровождение которой осуществляет Comcast, и OctoDNS, сопровождение которой осуществляет Amazon и Oracle. DNS Control —

Значительная часть самого популярного контента в интернете размещается в нескольких крупных сетях размещения контента, таких как YouTube от Google, который использует собственную систему DNS. Хотя ряд крупных операторов авторитативных DNS-серверов второго и более низких уровней иерархии используют бFOSS (например, те, которые также обслуживают корневые или TLD зоны), имеющихся публичных заявлений недостаточно для надежного исследования и составления статистики относительно использования ими FOSS.[71] Дополнительная информация приведена в таблицах ниже. Это заметный пробел в имеющейся у нас информации, поскольку на долю четырех очень крупных провайдеров может приходиться более половины запросов на авторитативные имена, видимые в интернете.[72]

4.3 FOSS в инфраструктуре получения DNS-данных (резолверы)

Доминирование FOSS не ограничивается сферой публикации данных DNS; она столь же значима и в инфраструктуре, которая извлекает эту информацию: разнообразной экосистеме DNS-резолверов. FOSS широко распространено во всей экосистеме резолверов: от локальных сетей до глобальных облачных платформ.

Большинство пользователей обслуживаются локальными резолверами, которыми управляют их интернет-провайдеры, предприятия или образовательные учреждения. По оценкам исследователей, общая доля пользователей, обслуживаемых облачными резолверами, составляет менее 20% во всем мире. Остальные 80% пользователей используют тот или иной локальный резолвер.[73] Многие из наиболее распространенных систем FOSS могут использоваться как для авторитативных функций, так и для резолверов (Таблица 5).

Таблица 5. Широко используемые системы FOSS для приложений DNS-серверов

Система программного обеспечения	Лицензия открытого исходного кода	Приложение — Примеры пользователей

еще одна популярная система конфигурации, которая управляет DNS как на локальных системах, так и в облачных сервисах, включая Cloudflare, сервис Route53 от Amazon и Gandi, регистратора DNS и провайдера хостинга.

[71] Сбор надежных количественных данных о внедрении FOSS представляет собой сложную проблему. Дэниел Стенберг в своей статье «Что мы не можем измерить» приводит несколько причин, почему это так. Daniel://Stenberg:// (блог), 5 июня 2025 года, https://daniel.haxx.se/blog/2025/06/05/what-we-cant-measure/.

[72] Джефф Хьюстон. «Насколько централизована DNS». APNIC Blog (блог), 22 ноября 2022 года. https://blog.apnic.net/2022/11/22/looking-at-centrality-in-the-dns/.

[73] Хьюстон, «Насколько централизована DNS».

BIND9	MPL 2.0	Авторитативные DNS-серверы, резолверы - CIRA, NIC.BR, Visionary Broadband
CoreDNS	Apache 2.0	Kubernetes, Авторитативные DNS-серверы - Meta
dnsdist	GPL 2.0	Балансировка нагрузки DNS
Dnsmasq	GPL 2 или 3	Преимущественно резолверы — популярны во встраиваемых системах, таких как OpenWRT, домашних шлюзах.
Knot DNS	GPL 3.0	Авторитативные DNS-серверы - .cz TLD
Knot Resolver	GPL 3.0	Резолвер - DNS4EU
NSD	BSD 3-пункт	Авторитативные DNS-серверы - Rcode Zero
PowerDNS	GPL 2.0	Авторитативные службы - Rakuten
PowerDNS Recursor	GPL 2.0	Резолвер - British Telecom
Unbound	BSD 3-Clause	Резолверы - Quad9, Let’s Encrypt
YADIFA	BSD 3-Clause	Авторитативные DNS-серверы - .eu TLD

Хотя для этого рынка существует множество коммерческих продуктов, большинство из них включают одно или несколько решений FOSS в качестве основного компонента DNS для предлагаемых ими услуг (Таблица 6).

Глобальные облачные вычислительные платформы, такие как Microsoft Azure, Google Cloud и Amazon AWS, используют обширную инфраструктуру резолверов для поддержки своих служб. По крайней мере четыре крупнейших глобальных оператора используют FOSS для разрешения DNS,[74] в то время как другие создали проприетарные решения на основе библиотек FOSS для DNS (Таблица 7).

Наконец, некоторые конечные пользователи настраивают свои системы так, чтобы обходить резолвер, предоставленный их сетевым оператором, и вместо этого используют открытые публичные резолверы. В то время как два самых популярных публичных сервиса (Google 8.8.8.8 и Cloudflare 1.1.1.1) используют проприетарное программное обеспечение, другие основные публичные резолверы, такие как Quad9 (9.9.9.9) и DNS4EU, построены на FOSS. Более подробная информация доступна в Приложении B.

[74] Подробности скрыты для конфиденциальности.

Таблица 6. Примеры коммерческих DNS-служб, включающих бесплатное и открытое программное обеспечение

Производитель	Продукт	Применение	Включает бесплатное и открытое программное обеспечение
Akamai	Edge DNS	Гибрид облачного резолвера и авторитативного DNS-сервера	Нет
Bluecat Networks	Integrity, Micetro	Авторитативный DNS-сервер, резолвер	Да
Cygna Labs	VitalQIP, DiamondIP	Авторитативный DNS-сервер, резолвер	Да
EfficientIP	SolidServer DDI	Авторитативный DNS-сервер, резолвер, аппаратный и облачный	Да
F5	BIG-IP DNS	Резолвер	Да
IBM	NS1 Connect	Облачный авторитативный DNS-сервер	Неизвестно
InfoBlox	Universal DDI и NIOS DDI	Авторитативный DNS-сервер, резолвер, аппаратный и облачный	Да
Knipp	IronDNS	Авторитативный DNS-сервер	Частично
Microsoft	Windows Server DNS	Авторитативный DNS-сервер, резолвер, используется в корпоративных сетях, интегрируется с Active Directory	Нет
	Azure DNS	Сервис облачного резолвера	Да
Netgate	pfSense	Резолвер	Да
Oracle	OCI DNS	Облачный авторитативный DNS-сервер	Да
TCPWave	DDI Management	Аппаратнаый авторитативный DNS-сервер	Да

Таблица 7. Библиотеки FOSS используемые для приложений инфраструктуры DNS

Система программного обеспечения	Язык программирования	Приложение — примеры пользователей
c-ares	C	libcurl, curl, NodeJS
dnsjava	Java	(Проприетарные) программы для бэкенда регистратур
dnspython	Python	Mailman, Samba, Ansible
domain	Rust	Cascade
miekg/dns	Go	Let's Encrypt, CoreDNS, Docker
ldns	C	Zonemaster, dnstap, (проприетарные) серверы имен
libunbound	C	Open vSwitch, libreswan, opendkim
Net::DNS	Perl	Spamassassin, Mail::DMARC, Mail::DKIM, Mail:SPF

5 Современные примеры нормативного регулирования FOSS

В этом разделе рассматриваются несколько современных случаев из США, Великобритании и Европейского Союза, которые иллюстрируют, как политики адаптируют нормы кибербезопасности к уникальным реалиям экосистемы FOSS. В таблице 8 представлен общий обзор этих подходов, которые демонстрируют схему освобождения волонтеров, оказывающих услуги по сопровождению проектов, от прямой ответственности, при этом основное внимание уделяется обязанностям коммерческих организаций, которые интегрируют или развертывают FOSS. Затем каждый случай рассматривается подробно.

Таблица 8. Обзор современных подходов к регулированию FOSS

Раздел	Основное направление	Пример подхода к регулированию	бесплатного и открытого программного обеспечения
5.1	Распределение ответственности	Стратегия кибербезопасности США 2023 год, Кодекс Великобритании 2025 год.	Освободить от ответственности лиц, оказывающих услуги по сопровождению проекта, сосредоточиться на коммерческих организациях
5.2	Стимулирование сотрудничества	Закон ЕС о киберустойчивости	Ввести дополнительную роль «координатора» для стимулирования поддержки
5.3	Недопущение требований, предполагающих использование проприетарных решений	Акт о реализации ЕС NIS 2	Нет контрактов = нет прямого поставщика, поощрять поддержку
5.4	Предотвращение конфликтных режимов	Директива ЕС NIS 2	Предотвращение дублирующего регулирования для глобальных элементов, таких как корневые серверы.

5.1 Распределение ответственности между заинтересованными сторонами, обладающими наибольшим потенциалом к действию

Национальная стратегия[75] кибербезопасности США 2023 года направлена на перенос ответственности за небезопасные программные продукты и услуги (стратегическая цель 3.3). В ней сформулирована общая концепция, согласно которой «компании, производящие программное обеспечение, должны иметь свободу для инноваций, но они также должны нести ответственность, если не выполняют свои обязанности по обеспечению безопасности потребителей, предприятий или провайдеров критической инфраструктуры». С самого начала стратегия предусматривала более избирательный подход к лицам, оказывающими услуги по сопровождению FOSS: «Ответственность

[75] Президент США. «Национальная стратегия кибербезопасности». Вашингтон, Округ Колумбия: Белый дом, 1 марта 2023 года. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

должна лежать на тех, кто способен принять наиболее эффективные меры для предотвращения негативных последствий, а не на конечных пользователях, которые часто страдают от последствий использования небезопасного ПО, и не на разработчиках компонентов с открытым исходным кодом, интегрированных в коммерческий продукт».

Аналогично, добровольный Кодекс правил по безопасности программного обеспечения[76] Великобритании 2025 года направлен на «поддержку поставщиков программного обеспечения и их клиентов для снижения вероятности и последствий атак на цепочку поставок программного обеспечения и других инцидентов, связанных с устойчивостью программного обеспечения». Он также нацелен на поставщиков коммерческого программного обеспечения: «В отношении программного обеспечения с открытым исходным кодом разработчик / лицо, оказывающее услуги по сопровождению проекта, не несет никаких формальных обязательств по дальнейшей цепочке поставок или по текущему обслуживанию и безопасности своего кода. Любые риски, связанные с открытым исходным кодом, должны контролироваться конечными пользователями или разработчиками, использующими открытый исходный код в своем программном обеспечении».

5.2 Стимулирование межотраслевого сотрудничества в области устойчивого сопровождения

Целью Закона о киберустойчивости ЕС[77] является решение проблемы «низкого уровня кибербезопасности продуктов с цифровыми элементами, что отражается в широком распространении уязвимостей, а также недостаточном и непоследовательном предоставлении обновлений безопасности для их устранения». Аналогичным образом освобождая от ответственности лиц, оказывающих услуги по сопровождению FOSS, которые не монетизируют его, он стимулирует межотраслевое сотрудничество по его устойчивому сопровождению, вводя нового юридического субъекта («координаторы ПО с открытым исходным кодом»), который «оказывает постоянную поддержку разработке» и гарантирует «жизнеспособность этих продуктов». Координаторы — это дополнительная, пока еще не получившая широкого распространения роль для организаций, с которыми могут сотрудничать лица, оказывающие услуги по сопровождению FOSS, в качестве средства направления ресурсов от производителей или операторов важной инфраструктуры, зависящей от него. Хотя объем FOSS, поддерживаемого в настоящее время организацией, выполняющей функции координатора, незначителен, Закон о киберустойчивости может в будущем расширить эту практику, и она, вероятно, применима к некоторым организациям, поддерживающим программное обеспечение DNS. Последним нововведением в сфере регулирования станет будущая возможность

[76] «Кодекс правил по безопасности программного обеспечения».

[77] Регламент (ЕС) 2024/2847 Европейского парламента и Совета от 23 октября 2024 года о требованиях к горизонтальной кибербезопасности для продуктов с цифровыми элементами и о внесении изменений в Регламенты (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директиву (ЕС) 2020/1828 (Закон о киберустойчивости), 2024 O.J. (L 2024/2847) 1, https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

«добровольной аттестации безопасности», которая позволит осуществлять межотраслевое сотрудничество в рамках комплексной проверки.

5.3 Недопущение требований безопасности цепочки поставок, предполагающих использование проприетарного программного обеспечения

Директива ЕС NIS 2 направленана «борьбу с угрозами сетевым и информационным системам, используемым для предоставления основных услуг в ключевых секторах».[78] Она регулирует цифровую инфраструктуру как «сектор высокой критичности», возлагает ответственность за управление кибербезопасностью и предписывает «меры по управлению рисками», подробно описанные в акте о реализации.[79] К ним относится «безопасность цепочки поставок, включая аспекты безопасности, касающиеся отношений между каждым субъектом и его прямыми поставщиками или провайдерами услуг». Приложение, в котором излагаются эти требования, основано на элементах управления стандарта ISO/IEC 27002:2022 и, в отличие от реалий FOSS (см. раздел 3.2.2), предполагает цепочку договорных обязательств вплоть до разработчика программного обеспечения.

В своем техническом руководстве по реализации для регулируемых организаций,[80] Агентство Европейского союза по кибербезопасности (ENISA) разъясняет понятие «прямого поставщика и провайдера услуг» применительно к FOSS: «В случае FOSS сообщества и проекты, которые открыто разрабатывают, сопровождают и распространяют программное обеспечение, не могут считаться прямыми поставщиками или провайдерами услуг, если между соответствующим субъектом и проектом с открытым исходным кодом не существует договорных отношений, помимо соблюдения стандартизированной лицензии на авторские права, или если договорные отношения установлены с координатором ПО с открытым исходным кодом». Вместо этого рекомендуется «рассмотреть возможность поддержки сообществ, разрабатывающих и сопровождающих бесплатное и открытое программное обеспечение, и инвестировать во взаимовыгодные отношения с ними. В случае эффективности это может включать отношения с

[78] Директива (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе (Директива NIS 2), 2022 O.J. (L 333) 80, https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[79] Исполнительный регламент Комиссии (ЕС) 2024/2690 от 22 октября 2024 года, устанавливающий правила применения Регламента (ЕС) 2024/2847 Европейского парламента и Совета, 2024 O.J. (L 2024/2690) 1, https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj.

[80] Агентство Европейского союза по кибербезопасности (ENISA), Руководство по технической реализации NIS2 (отчет, Бюро публикаций Европейского союза, 2025 год), https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

соответствующим координатором ПО с открытым исходным кодом, который «оказывает постоянную поддержку разработке и гарантирует жизнеспособность этих продуктов».

В отчете за 2025 год, подготовленном по заказу Министерства науки, инноваций и технологий Великобритании, проанализированы отраслевые практики на предмет рисков, связанных с открытым исходным кодом, и цепочками поставок.[81] Среди прочего, в отчете организациям рекомендуется «разработать внутреннюю политику ПО с открытым исходным кодом для управления внедрением его компонентов» и «способствовать активному взаимодействию с сообществом ПО с открытым исходным кодом для [..] обеспечения высокого качества его компонентов и устойчивости его экосистемы». Напротив, регулирование безопасности цепочки поставок, не адаптированное к FOSS, налагало бы контрактные требования на операторов, требуя проверки биографических данных лиц, оказывающих услуги по сопровождению FOSS, рассматривая их, как «поставщиков», даже если бесплатное и открытое программное обеспечение не закупается. Такое непродуманное регулирование может привести к тому, что талантливые специалисты, оказывающие услуги по сопровождению FOSS, откажутся от своих проектов, оставив их с меньшим количеством или менее компетентными специалистами по сопровождению, что приведет к снижению качества. Это противоречит предполагаемому эффекту регулирования безопасности цепочки поставок.

5.4 Недопущение конфликтных региональных режимов для глобальных сообществ FOSS

Прямое регулирование разработки программного обеспечения и его использования в критической инфраструктуре не является широко распространенной практикой. Поскольку FOSS допускает разработку в рамках глобального сотрудничества (Раздел 3.2.1), будущие режимы регулирования должны избегать создания дублирующих и взаимно противоречивых требований, различающихся по физическому местонахождению отдельных лиц, оказывающих услуги по сопровождению такого ПО.

В вышеупомянутой Директиве[82] ЕС NIS 2 предприняты все возможные меры, чтобы избежать аналогичной ситуации дублирования режимов в требованиях к провайдерам услуг DNS, исключив корневые серверы имен из сферы регулирования, тем самым избежав ситуации, когда операторы корневых серверов будут подпадать под действие дублирующих, а иногда и конфликтующих региональных режимов.[83]

[81] «Рекомендации по разработке программного обеспечения с открытым исходным кодом и управлению рисками в цепочке поставок».

[82] Директива NIS 2.

[83] Краткое изложение аргументов Берта Хуберта можно найти в статье «Дорогой ЕС: пожалуйста, не губите корень», 10 мая 2021 года, https://berthub.eu/articles/posts/dont-ruin-the-root/.

6 Ключевые выводы

В этом разделе основной анализ отчета сведен в ряд выводов, которые формируют доказательную базу для последующих практических рекомендаций.

Вывод 1. FOSS лежит в основе критической инфраструктуры DNS. Поскольку организации, формирующие политику, и регулирующие органы по всему миру стремятся обезопасить цепочку поставок программного обеспечения, крайне важно, чтобы эти усилия основывались на четком понимании того, как на самом деле создаются основополагающие системы интернета и как осуществляется их сопровождение. Исследования, проведенные для этого отчета, показывают, что сегодня глобальная инфраструктура DNS в огромной степени зависит от бесплатного и открытого программного обеспечения. В наиболее важных частях этой инфраструктуры FOSS является нормой, а коммерческое программное обеспечение — исключением. Сюда входит система корневых серверов, где по крайней мере девять из 12 операторов используют исключительно реализации FOSS для DNS, и TLD, где девять из 10 крупнейших провайдеров услуг используют FOSS.

Вывод 2. Модель разработки FOSS принципиально отличается от проприетарного программного обеспечения. В то время как проприетарное программное обеспечение обычно создается внутри одной организации, модель FOSS является открытой и распределенной. Модель основана на четырех основных свободах, предоставляемых ее лицензиями: свобода использовать, изучать, распространять и изменять программное обеспечение. Эта концепция способствует формированию уникальной экосистемы оказывающих услуги по сопровождению, участников и операторов, которые, как правило, не ограничены договорными отношениями, определяющими традиционную коммерческую цепочку поставок.

Вывод 3. FOSS по своей сути не более и не менее безопасно, чем коммерческое программное обеспечение; безопасность зависит от процесса и обслуживания, а не от видимости исходного кода. Последствия этой открытой модели лицензирования для безопасности следует рассматривать в контексте многолетних споров, в которых не было получено четкого ответа. Как подытожил исследователь в области безопасности Росс Андерсон, для больших и сложных систем видимость исходного кода в равной степени помогает как злоумышленникам, так и защитникам. В конечном счете то, является ли система открытой или закрытой, не оказывает существенного влияния на ее безопасность. Сокрытие исходного кода не обеспечивает дополнительной безопасности; скорее, безопасность системы определяется качеством процессов ее разработки, проверки и сопровождения.

Вывод 4. Экосистема FOSS системы DNS обладает уникальными преимуществами, способствующими стабильности и устойчивости. Хотя открытость сама по себе носит нейтральный характер, процесс сотрудничества, который она обеспечивает, особенно эффективен для создания и сопровождения критической инфраструктуры интернета.

Присущая FOSS транспарентность позволяет мировому сообществу разработчиков, исследователей и операторов изучать исходный код и совместно устранять уязвимости, что часто приводит к более быстрому исправлению ошибок, чем в коммерческих системах. Это обеспечивает неотъемлемые преимущества, включая улучшенную безопасность, обеспечиваемую сотрудничеством, эксплуатационную устойчивость за счет разнообразия программного обеспечения и замечательную стабильность, обеспечиваемую долгосрочной поддержкой со стороны специализированных некоммерческих и коммерческих организаций.

Вывод 5. Модель FOSS сопряжена с неотъемлемыми рисками, которые требуют индивидуального, а не универсального подхода к политике. Те же характеристики, которые обеспечивают эти сильные стороны, также влекут за собой определенный набор рисков, требующих особого подхода к политике. Поскольку модель разработки FOSS отделяет финансирование от использования, проекты могут столкнуться с проблемами финансовой устойчивости и выгоранием лиц, оказывающих услуги по сопровождению, когда критическая инфраструктура может зависеть от неоплачиваемой волонтерской работы нескольких человек. Более того, широкое повторное использование компонентов FOSS создает риск возникновения общих взаимозависимых элементов, когда уязвимость в одной библиотеке может иметь каскадные последствия для всей экосистемы. Эти проблемы невозможно решить посредством правил, разработанных для рынка коммерческого программного обеспечения.

Вывод 6. Привязка новой юридической и финансовой ответственности к разработке и распространению FOSS должна осуществляться осторожно, чтобы избежать отравления среды, которая привела к развитию этого основополагающего элемента инфраструктуры интернета. Отсутствие единого ответственного юридического лица или традиционной договорной цепочки в проектах FOSS делает нецелесообразным и рискованным применение традиционных концепций ответственности. Модель разработки FOSS зависит от отдельных волонтеров и небольших, организаций с минимальным финансированием. Возложение тяжелого нормативного бремени на этих лиц, оказывающих услуги по сопровождению проекта, может отбить у них желание участвовать в этой деятельности, что потенциально задушит инновации и приведет к отказу от программного обеспечения, имеющего решающее значение для критической инфраструктуры интернета.

Вывод 7. FOSS играет важную роль в выходе новых провайдеров на рынок интернет-услуг и предоставляет организациям, формирующим политику, возможность стимулировать развитие местных услуг и снижать зависимость от иностранных провайдеров облачных услуг. Помимо своей технической роли, FOSS является фактором, способствующим экономическому росту, цифровой автономии и рыночной конкуренции. Модель разработки FOSS снижает стоимость выхода на рынок для новых предпринимателей за счет устранения сборов за лицензирование программного обеспечения. Такая доступность способствует развитию местных инноваций и навыков,

предоставляя политикам эффективный способ создания более разнообразной цифровой экосистемы и помогая снизить зависимость от иностранных облачных сервисов.

7 Практические рекомендации для организаций, формирующих политику

В этом разделе на основе выводов отчета излагаются прямые и действенные рекомендации для организаций (лиц), формирующих политику. Цель состоит в том, чтобы обеспечить разработку эффективного и безопасного регулирования, которое укрепляет, а не подрывает экосистему FOSS, имеющую решающее значение для безопасной и стабильной работы интернета.

Рекомендация 1. Признать критически важную роль FOSS. В отчете устанавливается тот факт, что глобальная инфраструктура DNS зависит от FOSS. В наиболее важных частях этой инфраструктуры FOSS является нормой, а коммерческое программное обеспечение — исключением. Поэтому организациям, формирующим политику, следует открыто признать в любом соответствующем законодательстве или нормативных актах, что FOSS лежит в основе критической инфраструктуры интернета и что его использование является преимуществом, которое необходимо сохранить. Это понимание должно учитываться при формирование нормативных правовых актов, начиная с начальной стадии разработки их проектов, чтобы предотвратить непреднамеренный ущерб экосистеме.

Рекомендация 2. Прислушаться к сообществу FOSS. Модель разработки FOSS, распределенной и принципиально отличается от модели разработки проприетарного программного обеспечения. Это экосистема лиц, оказывающих услуги по сопровождению проекта, участников и операторов, которые, как правило, не связаны договорными отношениями, определяющими традиционную коммерческую цепочку поставок. Крайне важно вовлекать все секторы экосистемы FOSS, включая компании, некоммерческие организации, отдельных лиц, оказывающих услуги по сопровождению проекта, и общественные институты, на протяжении всего процесса разработки политики. Это гарантирует, что правила будут соответствовать реалиям их работы, и предотвратит непреднамеренный ущерб экосистеме FOSS и, следовательно, критически важной инфраструктуре интернета.

Рекомендация 3. Использовать современные методы нормативного регулирования FOSS. Как подробно изложено в Разделе 5, недавние усилия по нормативному регулированию уже начали учитывать уникальные характеристики FOSS, продолжая при этом достигать важных целей политики. Эти примеры обеспечивают ценную основу для разработки новых политик, учитывающих уникальные характеристики экосистемы FOSS. Применение извлеченных из этого уроков означает разработку политик и правил, которые:

- Обеспечивают распределение ответственности между заинтересованными сторонами, наиболее способными к действию. Возлагают обязанность по обеспечению интересов клиента на организации, которые внедряют программное обеспечение в коммерческие продукты или критическую инфраструктуру, а не на разработчиков-волонтеров FOSS, которые создают компоненты.
- Стимулируют межотраслевое сотрудничество в области устойчивого сопровождения проектов. Жизнеспособность критически важных продуктов FOSS может быть обеспечена за счет поддержки инновационных правовых моделей, таких как «координатор ПО с открытым исходным кодом», которые направляют ресурсы из отрасли.
- Недопущение требований безопасности цепочки поставок, предполагающих использование модели проприетарного программного обеспечения. Напомним, что в FOSS зачастую нет прямых договорных отношений между лицами, оказывающими услуги по сопровождению, и оператором, кроме самой лицензии с открытым исходным кодом.
- Предотвращение создания конфликтных региональных режимов для глобальных сообществ FOSS. Следует избегать дублирования и противоречий в нормативных актах, затрагивающих глобальные проекты FOSS, чтобы не допустить фрагментации разработки и подрыва безопасности.

Рекомендация 4. Стимулировать устойчивое развитие FOSS. Модель FOSS отделяет финансирование от использования, что, как известно, приводит к проблемам с финансовой устойчивостью и выгоранием лиц, оказывающих услуги по сопровождению. Критическая инфраструктура может зависеть от небольших организаций или неоплачиваемой волонтерской работы нескольких человек. Для борьбы с этим риском политикам рекомендуется разрабатывать благоприятную политику, поощряющую вклад государственного и частного секторов в критически важные проекты FOSS как форму инвестиций в общее общественное благо.

Рекомендация 5. Коллективно устранять системные риски. Широкое повторное использование компонентов FOSS создает риск возникновения общих взаимозависимых элементов, когда уязвимость в одной библиотеке может иметь каскадные последствия для всей экосистемы как в FOSS, так и в проприетарных программных продуктах. Поскольку это системный риск, присущи всем современным разработкам программного обеспечения, политика должна поощрять и финансировать решения на основе сотрудничества в масштабах всей экосистемы, такие как усовершенствованные инструменты безопасности и независимые исследования, а не возлагать всю нагрузку на отдельных волонтеров, оказывающих услуги по сопровождению.

8 Благодарности, раскрытие информации о заинтересованности и отказы от участия

В интересах транспарентности в этих разделах читателю предлагается информация о различных аспектах деятельности SSAC. В разделе «Благодарности» перечислены члены SSAC, внешние эксперты и персонал ICANN, которые были соавторами или внесли непосредственный вклад в этот конкретный документ или предоставили рецензии. В разделе «Раскрытие информации о заинтересованности» содержатся ссылки на биографии всех членов SSAC, в которых раскрывается вся информация о заинтересованности, которая может привести к конфликту — фактическому, кажущемуся или потенциальному — при участии члена комиссии в подготовке данного отчета. В разделе «Отказы от участия» указаны отдельные лица, которые взяли самоотвод от участия в обсуждении темы, которой касается настоящий отчет. За исключением членов, перечисленных в разделе «Отказы от участия», настоящий документ получил одобрение на основании консенсуса со стороны всех членов SSAC.

8.1 Благодарности

Комитет хотел бы поблагодарить следующих членов SSAC, приглашенных гостей и персонал ICANN за их время, вклад и рецензирование при подготовке этого отчета.

Члены SSAC
Джо Эбли (Joe Abley)
Мартен Артсен (Maarten Aertsen) (сопредседатель рабочей группы)
Гаутам Акива (Gautam Akiwate)
Тим Эйприл (Tim April)
Набил Бенамар (Nabil Benamar)
Кей Си Клаффи (KC Claffy)
Хадиа Эль-миньяви (Hadia Elminiawi)
Онджей Филип (Ondrej Filip) (член SSAC до 31 декабря 2024 года)
Джеймс Галвин (James Galvin)
Роберт Герра (Robert Guerra)
Расс Хаузли (Russ Housley)
Матиас Худобник (Matthias Hudobnik)
Джефф Хьюстон (Geoff Huston)
Лайал Джебран (Layal Jebran)
Мерике Каэо (Merike Kaeo) (член SSAC до 31 декабря 2024 года)
Андрей Колесников (Andrei Kolesnikov)
Уоррен «Эйс» Кумари (Warren “Ace” Kumari)
Барри Лейба (Barry Leiba) (сопредседатель рабочей группы)
Джон Левин (John Levine)
Расс Мунди (Russ Mundy)
Рам Мохан (Ram Mohan)
Мэтт Томас (Matt Thomas)
Питер Томассен (Peter Thomassen)

Тара Уейлен (Tara Whalen)
Сюзан Вульф (Suzanne Woolf)
Йианканг Яо (Jiankang Yao)

Приглашенные гости
Витторио Бертола (Vittorio Bertola)
Мерике Каэо (Merike Kaeo) (приглашенный гость после 01 января 2025 года)
Викки Риск (Vicky Risk)
Раффаеле Соммесе (Raffaele Sommese)

Персонал ICANN
Джон Эмери (John Emery) (редактор)
Даниэл Глак (Daniel Gluck)
Густаво Лозано Ибарра (Gustavo Lozano Ibarra)
Майкл Пакетт (Michael Puckett)
Карлос Рейес (Carlos Reyes)
Даниелла Рутефорд (Danielle Rutherford) (редактор, соавтор)
Кати Шнитт (Kathy Schnitt)
Стив Шэн (Steve Sheng) (сотрудник службы поддержки SSAC до 30 ноября 2024 года)

8.2 Раскрытие информации о заинтересованности

Биографические сведения о членах SSAC и раскрытие информации о заинтересованности на момент публикации представлены здесь: https://www.icann.org/en/ssac/members/archive/16-05-2025.

8.3 Отказы от участия

Отказов от участия не поступило.

Приложение A. Глоссарий и аббревиатуры

A.1 Глоссарий терминов

Авторитативный сервер: Сервер, на котором хранятся окончательные официальные записи DNS для конкретного доменного имени. Он предоставляет окончательные ответы на DNS-запросы для данного домена.

Участник: Физическое лицо или организация, предлагающие улучшения для проекта FOSS, например путем предоставления кода, документации или отчетов об ошибках.

Временное депонирование данных: Хранение копии регистрационных данных доменного имени у аккредитованной ICANN третьей стороны в целях безопасности.

Доменное имя: Уникальное, легко читаемое человеком имя (например, icann.org), которое идентифицирует конкретный адрес в интернете и составляет основу URL-адресов.

Система доменных имен (DNS): Глобальная децентрализованная система, которая действует как «адресная книга интернета», преобразуя понятные человеку доменные имена в числовые IP-адреса, необходимые для поиска компьютерных служб и устройств.

Протокол EPP: Стандартизированный технический протокол, используемый для автоматизации транзакций между регистраторами доменных имен и регистратурами, таких как регистрация, продление и передача.

Ответвление проекта (форк): Новый, отдельный программный проект, который начинается с копирования исходного кода из существующего проекта FOSS.

Бесплатное и открытое программное обеспечение (FOSS): Программное обеспечение, лицензированное таким образом, который предоставляет пользователям четыре основные свободы: использовать, изучать, распространять и изменять программное обеспечение. Это определяет модель разработки на основе сотрудничества, а не просто бесплатное программное обеспечение.

Адрес интернет-протокола (IP-адрес): Уникальная числовая метка, присваиваемая каждому устройству, подключенному к компьютерной сети, которая использует интернет-протокол для связи.

Интернационализированное доменное имя (IDN): Доменное имя, в котором одна или несколько меток содержат символы, не являющиеся буквами, цифрами или дефисами в кодировке ASCII.

Лицо, оказывающее услуги по сопровождению проекта: Физическое лицо или группа, ответственные за общее руководство проектом и контроль качества FOSS. Они имеют

полномочия принимать или отклонять дополнения к официальной версии программного обеспечения.

Оператор: Физическое лицо или организация, которая развертывает и использует программное обеспечение для управления сервисом. В контексте DNS, оператор — это организация, которая управляет компонентами инфраструктуры DNS, такими как авторитативные серверы или резолверы.

Публикация (в DNS): Технический процесс, обеспечивающий доступность записей DNS домена на авторитативных серверах, чтобы другие пользователи могли найти доменное имя в интернете.

Рекурсивный резолвер (резолвер): Сервер, часто управляемый интернет-провайдером (ISP), который действует от имени устройства пользователя, чтобы найти правильный IP-адрес для запрошенного доменного имени.

Регистрация (в DNS): Административный процесс резервирования уникального доменного имени путем добавления его в авторитативную основную базу данных (регистратуру) для определенного домена верхнего уровня.

Владелец домена: Физическое или юридическое лицо, которое регистрирует определенное доменное имя и владеет правами на него.

Регистратор: Общественная организация, выступающая в качестве розничного продавца доменных имен и управляющая резервированием доменов от имени владельцев доменов.

Регистратура: Авторитативная главная база данных всех доменных имен, зарегистрированных в определенном домене верхнего уровня (например, регистратура .org). Организация, которая ведет эту базу данных, является оператором регистратуры.

Система корневых серверов (RSS) Совокупность серверов на самом высоком уровне иерархии DNS, которые отвечают за направление запросов на правильные серверы доменов верхнего уровня.

Домен верхнего уровня (TLD): Фрагмент доменного имени, расположенный справа от последней точки, например .com, .org или .uk.

Унифицированный адрес ресурса (URL): Полный адрес, используемый для поиска определенного ресурса в интернете, который обычно включает протокол (например, https), доменное имя и конкретный путь (например, https://www.icann.org/resources).

A.2 Сокращения, используемые в данном отчете

ccTLD: Национальный домен верхнего уровня
DNS: Система доменных имен

EPP: Протокол EPP
FOSS: Бесплатное и открытое программное обеспечение
gTLD: Домен общего пользования верхнего уровня
IP: Интернет-протокол
ISP: Интернет-провайдер
RSS: Система корневых серверов
SSAC: Консультативный комитет по безопасности и стабильности
TLD: Домен верхнего уровня
URL: Унифицированный адрес ресурса
IDN-домен: Интернационализированное доменное имя

Приложение B. Методология и результаты исследования распространенности FOSS

В настоящем приложении представлено полное, исчерпывающее резюме оригинального исследования, отраженного в отчете. В нем подробно описывается как методология, использованная для получения результатов о распространенности бесплатного и открытого программного обеспечения (FOSS), так и сами результаты, которые представлены в разделе 4 настоящего отчета.

B.1 Общий подход и проблемы

Сложно с уверенностью определить, какое программное обеспечение используют операторы в реальных условиях. Хотя некоторые записи системы доменных имен (DNS) (например, version.bind, author.bind, id.server) были введены, чтобы помочь конечным пользователям идентифицировать версию DNS-сервера, с которым они взаимодействуют, эти записи не получили широкого распространения из-за потенциальных рисков безопасности и необходимости ручной настройки. В литературе рассматриваются и другие методы, включая пассивный анализ и активные измерения. Однако эти подходы часто ограничены в области применения (некоторые из них могут определить только рекурсивную инфраструктуру) и сталкиваются с проблемами масштабируемости.

По этим причинам подход, принятый в данном отчете, сосредоточен на оценке крупных DNS-операторов по доле рынка, где можно напрямую подтвердить значительное использование программного обеспечения с открытым исходным кодом.

B.2 Инфраструктура регистрации доменных имен

B.2.1 Методология

Чтобы оценить использование FOSS в инфраструктуре регистрации, Консультативный комитет по безопасности и стабильности (SSAC) провел опрос крупных регистратур и провайдеров серверных решений для регистратур. Для оценки использования FOSS в услугах временного депонирования данных был проведен опрос среди утвержденных ICANN провайдеров услуг временного депонирования данных (DEA), перечисленных на сайте ICANN. Особое внимание было уделено программному обеспечению, используемому для ключевых компонентов услуг (передача данных, проверка подписи, проверка депонирования и взаимодействие с интерфейсами программирования приложений формы предоставления регистрационной отчетности (RRI).

B.2.2 Результаты

Инфраструктура регистрации относится к системам, которые облегчают регистрацию отдельных доменных имен и делают их доступными в публичной DNS. Хотя точные данные о масштабах использования FOSS отсутствуют, имеющиеся данные свидетельствуют о глубокой зависимости от него как комплексных систем, так и основополагающих компонентов.

Ряд операторов регистратур, особенно в пространстве национальных доменов верхнего уровня (ccTLD), поддерживают инфраструктуру регистрации, которая полностью основана на FOSS (Таблица 1, Таблица 2). Например, известно, что платформа регистратуры FRED используется по меньшей мере 12 регистратурами ccTLD, а платформа Nomulus используется для нескольких доменов общего пользования верхнего уровня (gTLD).

Напротив, крупнейшие регистраторы и провайдеры backend-сервиса для регистратур часто используют проприетарные системы. Однако такие системы, как правило, не создаются с нуля; они используют коммерческие, индивидуальные расширения и интегрированные компоненты, такие как базы данных и серверы, которые в основном являются FOSS.

Такая зависимость от FOSS характерна и для служб временного депонирования данных (Таблица 3), которые надежно хранят копии регистрационных данных доменных имен. Крупнейшие провайдеры этих услуг как для регистратур, так и для регистраторов построили свои системы, по крайней мере частично, на компонентах FOSS.

B.3 Инфраструктура системы доменных имен

B.3.1 Методология

Анализ авторитативных серверов: Для исследования использования FOSS в инфраструктуре TLD была использована следующая процедура:

1. Корневая зона была получена из IANA, а TLD были сопоставлены с IP-адресами их DNS-серверов.
2. Отдельный анализ был проведен по ccTLD с учетом как двухбуквенных TLD, так и их эквивалентов A-label (Punycode) (для учета ccTLD с интернационализированными доменными именами (IDN-доменами)).
3. Для сопоставления этих IP-адресов с соответствующими им номерами автономной системы (ASN) и именами ASN (операторами) использовалась библиотека Python ip2asn.
4. Доля рынка рассчитывалась как количество TLD, размещенных определенным оператором, деленное на общее количество TLD (при этом один TLD может размещаться несколькими операторами одновременно).

5. Были определены 25 ведущих операторов, и использование ими программного обеспечения с открытым исходным кодом для авторитативных серверов имен было проверено вручную.

Анализ резолверов: Достоверных обзоров всей установленной базы резолверов нет. В рамках данного отчета анализ был сосредоточен на перечислении основных операторов и типов развертываний (например, локальные, облачные, публичные), а также на исследовании того, использовали ли ониFOSS или проприетарное программное обеспечение на основе публичных заявлений и непосредственных знаний.

B.3.2 Выводы

Авторитативные серверы: Доказательства доминирования бFOSS наиболее очевидны в инфраструктуре, публикующей информацию о доменах. На самых высоких уровнях иерархии DNS — корневом и TLD — FOSS встречается практически повсеместно. Система корневых серверов (RSS) находится на вершине DNS. Из 12 независимых организаций, которые управляют корневыми серверами, по крайней мере девять используют для DNS исключительно реализации FOSS для ответа на запросы (Таблица 4).

Эта закономерность сохраняется и на следующем уровне иерархии с серверами имен TLD (Таблица 5). Исследование, проведенное для этого отчета, показало, что девять из 10 крупнейших операторов, предоставляющих авторитетные услуги DNS для регистратур TLD, используют для этого FOSS. Кроме того, 20 из 25 крупнейших операторов, предоставляющих эту услугу для ccTLD, используют FOSS для DNS, в совокупности обслуживая 234 уникальных ccTLD.

Резолверы: Доминирование FOSS не ограничивается публикацией данных DNS; она столь же значима и в инфраструктуре, которая извлекает эту информацию: разнообразной экосистеме DNS-резолверов.

Большинство пользователей обслуживаются локальными резолверами, которыми управляют их интернет-провайдеры (ISP), предприятия или образовательные учреждения. Хотя для этого рынка существует множество коммерческих продуктов, большинство из них включают одно или несколько решений FOSS в качестве основного компонента DNS для предлагаемых ими услуг.

Глобальные облачные вычислительные платформы, такие как Microsoft Azure, Google Cloud и Amazon Web Services, используют значительную инфраструктуру резолверов для поддержки своих служб. По крайней мере четыре крупнейших глобальных оператора используют FOSS для разрешения DNS, в то время как другие создали проприетарные решения на основе библиотек FOSS для DNS.

Приложение C. Исследование взглядов операторов DNS на FOSS и регулирование программного обеспечения

Консультативный комитет по безопасности и стабильности (SSAC) провел неформальный онлайн-опрос на тему ожидаемого влияния регулирования ПО с открытым исходным кодом на инфраструктуру системы доменных имен (DNS) с целью сбора данных для этого отчета. Инструмент EUSurvey использовался для защиты конфиденциальности и анонимности опрошенных.[84] Техническому сообществу DNS было предложено ответить на вопросы из нескольких листов рассылки, включая технические и юридические списки рассылки Совета европейских регистратур национальных доменов (CENTR), рабочие группы DNS и открытого исходного кода Réseaux IP Européens Network Coordination Centre (Европейский сетевой координационный центр IP-сетей) (RIPE NCC), а также листы рассылки пользователей для нескольких систем программного обеспечения DNS с открытым исходным кодом. Опрос также был представлен на февральском заседании Центра исследований и анализа работы DNS (DNS-OARC).

Основной целью опроса было выяснить, осведомлены ли технические операторы DNS об инициативах в области регулирования , а также выяснить, какие последствия, по их мнению, могут возникнуть в результате регулирования FOSS. Опрос проводился в феврале 2025 года. Было получено 98 ответов, охватывающих весь спектр ролей в инфраструктуре DNS.

Сначала мы спросили респондентов об их участии в DNS. 96 из 98 опрошенных сообщили об участии в инфраструктуре DNS, а 64 из них также сообщили об участии в инфраструктуре регистрации доменных имен. Двадцать четыре опрошенных указали «разработчика/поставщика программного обеспечения» в качестве одной из своих ролей, но никто из них не ответил исключительно как разработчик программного обеспечения. (Мы не спрашивали, имеет ли их программное обеспечение открытый или закрытый исходный код.)

Респонденты были пользователями ПО с открытым исходным кодом и хорошо знали о регулировании. Почти все опрошенные сообщили об использовании ПО с открытым исходным кодом (93%). Примерно треть (33%) сообщили, что также используют проприетарное программное обеспечение. Тридцать процентов опрошенных также консультируют других по вопросам внедрения и эксплуатации FOSS. Эта группа имела высокий уровень осведомленности о текущих регуляторных инициативах. Мы предоставили список регуляторных инициатив и спросили: «О каких из этих регуляторных инициатив вам известно? (отметьте все, о чем вам известно)». Семьдесят семь опрошенных (то есть примерно 77%) указали, что им известно об одной или нескольких из них. С Законом ЕС о киберустойчивости, Законом о кибербезопасности и

[84] «EUSurvey – О нас». https://ec.europa.eu/eusurvey/home/about.

NIS2 знакомы более 40% опрошенных. Тридцать процентов опрошенных также указали, что они знакомы с одной или несколькими инициативами правительства США, включая указы президента 14028 и 14144, Программу аттестации безопасной разработки программного обеспечения или знак CyberTrust для устройств интернета вещей (IoT). Другие нормативные акты, упомянутые респондентами, включали Закон Австралии о безопасности критической инфраструктуры (SOCI), Общие положения о защите данных (GDPR), Стандарт безопасности данных индустрии платежных карт (PCI DSS) и положения Федеральной программы управления рисками и авторизацией США и Канады (FedRAMP).

Мы спросили: «Какие конкретные опасения есть у вас относительно влияния регулирования программного обеспечения на вашу организацию?», предоставив как положительные, так и отрицательные варианты ответа. На этот вопрос смогли ответить все опрошенные, включая тех, кто не указал на знакомство ни с одним из упомянутых нами конкретных нормативных актов.

- 72% опрошенных посчитали, что вполне вероятно, что некоторые проекты с открытым исходным кодом могут быть заброшены или станут недоступными.
- 66% считают, что необходимость выполнения требований увеличит для них стоимость программного обеспечения
- 49% опрошенных обеспокоены тем, что некоторые проекты с открытым исходным кодом, на которые они полагаются, могут перейти на коммерческое лицензирование
- 29% опрошенных считают, что регулирование будет помешает их организациям публиковать программное обеспечение с открытым исходным кодом
- 21% опрошенных ожидают, что безопасность открытого исходного кода, который они используют, улучшится
- 7% опрошенных ожидают, что регулирование снизит нагрузку на их организации по оценке безопасности и качества программного обеспечения.

Хотя мы специально запрашивали комментарии о позитивных воздействиях и возможностях, пытаясь занять сбалансированную позицию, опрошенные в основном были настроены пессимистично.

C.1 Открытые комментарии (конкретные проблемы)

В ходе опроса предлагалось дать открытые комментарии по конкретным вопросам, касающимся влияния регулирования программного обеспечения, а также задать вопросы об ожидаемых возможностях или положительном влиянии.

Наиболее часто упоминаемыми проблемами были:

- Увеличение затрат на соблюдение требований
- Более медленное развертывание программного обеспечения

- Потенциальный отказ от некоторых проектов с открытым исходным кодом из-за нормативных ограничений
- Повышение сложности соблюдения юридических требований для пользователей программного обеспечения с открытым исходным кодом