Итоговый отчет второй группы по анализу безопасности, стабильности и отказоустойчивости (SSR2) - основные положения и рекомендации

Из итогового отчета группы по анализу SSR2

25 января 2021 г.

СОДЕРЖАНИЕ

A. Основные положения

В соответствии с Уставом Интернет-корпорация по присвоению имен и номеров (ICANN), раздел 4.6(c):

«*Правление должно проводить регулярный анализ соблюдения ICANN своих обязательств по повышению рабочей стабильности, надежности, отказоустойчивости, безопасности и глобальной функциональной совместимости систем и процессов, как внутренних, так и внешних, которые напрямую влияют на систему уникальных идентификаторов интернета, координированием которой занимается ICANN, и/или на которые влияет указанная выше система («Анализ SSR»)».*[1]

Эти проверки SSR являются важной частью мандата корпорации ICANN[2] «работать в максимально возможной степени, открыто и прозрачно и в соответствии с процедурами, разработанными для обеспечения справедливости». Это вторая проведенная проверка SSR, и в соответствии с указаниями Устава она включает в себя проверку того, как корпорация ICANN выполняет рекомендации первой проверки SSR, а также новые рекомендации для рассмотрения корпорацией ICANN.

Группа по анализу SSR2 предлагает 24 группы рекомендаций, в результате чего сформулировано 63 конкретные рекомендации, начиная с оценки ответа корпорации ICANN на рекомендации SSR1. Мы решили разбить их на очень конкретные рекомендации в ответ на отсутствие конкретики в рекомендациях SSR1. Затем рекомендации структурируются таким образом, чтобы дать представление о внутренней деятельности корпорации ICANN, вовлеченности корпорации ICANN (в частности, о контрактах и рассмотрении жалоб) и о том, как корпорация ICANN может предпринять шаги для улучшения своих собственных действий по SSR и помочь другим понять, как улучшить свои действия. Рекомендации в документе часто влияют друг на друга и взаимозависимы. Корпорация и Правление ICANN должны учитывать это при разработке планов выполнения. Группа по анализу достигла полного консенсуса по каждой рекомендации.

Чтобы обеспечить более эффективную оценку будущими группами по анализу SSR, группа по анализу SSR2 попыталась сформулировать свои собственные рекомендации в соответствии с критериями SMART: *конкретные, измеримые, назначаемые, актуальные и отслеживаемые*. Во многих случаях детали, необходимые для того, чтобы сделать каждую рекомендацию полностью соответствующей принципам SMART, включая определение соответствующих сроков, потребуют размышлений и действий со стороны группы внедрения и должны быть включены в окончательный план реализации. Группа по анализу также представила на рассмотрение несколько предложений относительно того, как можно было бы проводить будущие проверки, признавая, что они выходят за рамки прямого мандата самой проверки SSR. Дополнительная информация о процессе и методологии, использованной группой по анализу SSR2 для выполнения своего мандата, представлена в Приложении C: «Процесс и методология».

[1] ICANN, «Устав Интернет-корпорации по присвоению имен и номеров: Раздел 4.6(c): Особые проверки: Обзор безопасности, стабильности и отказоустойчивости» с поправками от 28 ноября 2019 г., https://www.icann.org/resources/pages/governance/bylaws-en/#article4.

[2] Устав ICANN, Раздел 3.1: https://www.icann.org/resources/pages/governance/bylaws-en/.

1. Для справки

Как отмечено в разделе A.2. «Цели проверки SSR», Устав ICANN требует периодической оценки безопасности, стабильности и отказоустойчивости системы доменных имен (DNS). Правление ICANN официально получило первый отчет о проверке SSR 13 сентября 2012 года. Пять лет спустя вторая проверка началась с первого собрания группы по анализу SSR2, которое состоялось 2 марта 2017 года. Однако с момента своего создания группа по анализу SSR2 столкнулась с рядом проблем, из-за которых продолжительность проверки значительно превысила ожидания. Группа по анализу SSR2 регулярно собиралась до октября 2017 года, когда Правление приостановило деятельность группы.[3] Совещания возобновились с восстановленного членства 19 июня 2018 года.[4]

Ситуация в глобальной экосистеме уникальных идентификаторов продолжала развиваться в течение длительного периода времени проведения проверки. Несмотря на глобальное нарушение деловой активности и путешествий в результате пандемии COVID-19, что привело к дополнительным задержкам в процессе проверки SSR2, группа по анализу SSR2 смогла завершить проверку. В последний год проведения проверки группа решила не возобновлять оценку своих первоначальных рекомендаций, а скорее сохранила свой фундаментальный и исторический вклад. Группа по анализу считает, что эти рекомендации по-прежнему актуальны для корпорации ICANN и способствуют обеспечению безопасности, стабильности и отказоустойчивости глобальной DNS.

2. Цели проверки SSR

Согласно разделу 4.6(c) Устава ICANN: «*Правление должно проводить регулярный анализ соблюдения ICANN своих обязательств по повышению рабочей стабильности, надежности, отказоустойчивости, безопасности и глобальной функциональной совместимости систем и процессов, как внутренних, так и внешних, которые напрямую влияют на систему уникальных идентификаторов интернета, координированием которой занимается ICANN, и/или на которые влияет указанная выше система («Анализ SSR»)».*[5]

В частности, в нем говорится следующее:

«ii. Вопросы, оценкой которых может заниматься рабочая группа по анализу SSR («Рабочая группа по анализу SSR»), включают в себя, помимо прочего, следующее:

1. *физическую и сетевую безопасность, стабильность и отказоустойчивость в контексте координирования системы уникальных идентификаторов интернета;*

[3] Письмо группе по анализу SSR2 от доктора Стивена Д. Крокера, председателя Правления ICANN, 28 октября 2017 г. https://www.icann.org/en/system/files/correspondence/crocker-to-ssr2-28oct17-en.pdf.

[4] ICANN, «Вторая проверка безопасности, стабильности и отказоустойчивости DNS (SSR2) возобновляется», блог, 7 июня 2018 г., https://www.icann.org/news/announcement-2-2018-06-07-en.

[5] Устав ICANN, раздел 4.6 (c), https://www.icann.org/resources/pages/governance/bylaws-en.

2. *соответствие применимой концепции плана по обеспечению безопасности в случае непредвиденных обстоятельств для систем уникальных идентификаторов интернета;*
3. *обеспечение четких и глобально применимых процессов обеспечения безопасности для таких областей системы уникальных идентификаторов интернета, координированием которых занимается ICANN.*

iii. Группа по анализу SSR также должна оценивать, насколько успешно корпорация ICANN справляется с обеспечением безопасности, эффективность работы корпорации в контексте реальных и потенциальных задач и угроз в области безопасности и стабильности DNS, а также степень надежности мер по обеспечению безопасности и устранению угроз безопасности, стабильности и отказоустойчивости DNS в будущем в рамках миссии ICANN.

iv. Группа по анализу SSR также оценивает степень выполнения рекомендаций, полученных после предыдущего анализа SSR, а также степень, в которой выполнение данных рекомендаций привело к ожидаемому эффекту.

v. Анализ SSR должен проводиться не реже одного раза в пять лет, считая от даты формирования предыдущей Группы по анализу SSR».

3. Влияние других групп по анализу и консультативных комитетов

Корпорация ICANN должна взаимодействовать с несколькими группами по анализу и консультативными комитетами (AC), как того требует Устав ICANN. Хотя у всех этих групп и комитетов есть конкретные полномочия, рекомендации, разработанные этими группами, могут частично совпадать с областями работы других групп по анализу и комитетов. Группа по анализу SSR2 оценила рекомендации других групп по анализу и AC, чтобы определить, где опубликованные ими рекомендации повлияли на SSR корпорации ICANN и глобальной DNS. В нескольких случаях группа по анализу SSR2 сочла необходимым включить и развить эти рекомендации для разработки необходимого руководства по SSR для корпорации ICANN (см., в частности, раздел E.1. Недостигнутые механизмы защиты для программы New gTLD и раздел E.3. Альтернативы PDP). Группа по анализу SSR2 рассматривала эти совпадения в рекомендациях как негласное подтверждение достоинств соответствующих вопросов и далее рассматривала согласованность между рекомендациями группы проверки и рекомендациями других групп как эмпирическую поддержку их необходимости. Рекомендации SSR2 призваны дополнить рекомендации этих других групп по анализу.

B. Рекомендации SSR2

Группа по анализу SSR2 достигла полного консенсуса по каждой рекомендации.

1. Сводная таблица

№	Рекомендация	Исполнитель	Приоритет
Рекомендация SSR2 № 1: Дальнейший анализ SSR1			
1.1	Правление и корпорация ICANN должны провести дальнейшую всестороннюю проверку рекомендаций SSR1 и выполнить новый план для завершения выполнения рекомендаций SSR1 (см. Приложение D: Выводы, относящиеся к рекомендациям SSR1).	Правление и корпорация ICANN	Низкий
Рекомендация SSR2 № 2: Ввести должность ответственного за стратегию и тактику безопасности и управление рисками			
2.1	Корпорации ICANN следует ввести должность директора по безопасности (CSO) или директора по информационной безопасности (CISO) на уровне высшего руководства корпорации ICANN, нанять на эту должность человека с соответствующей квалификацией и выделить конкретный бюджет, достаточный для выполнения соответствующих функциональных задач.	Корпорация ICANN	Умеренно высокий
2.2	Корпорация ICANN должна включить в описание этой роли, что лицо на этой должности будет управлять функцией безопасности корпорации ICANN и контролировать взаимодействие персонала во всех соответствующих областях, влияющих на безопасность. Лицо на этой должности будет предоставлять регулярные отчеты Правлению ICANN и сообществу по всей деятельности, связанной с SSR, в рамках корпорации ICANN. Существующие функции безопасности следует реструктурировать и переместить в организационном плане, чтобы они вошли в компетенцию этой новой должности.	Корпорация ICANN	Умеренно высокий

2.3	Корпорация ICANN должна включить в описание этой роли, что лицо на этой должности будет отвечать как за стратегическую, так и за тактическую безопасность и управление рисками. Эти области ответственности включают в себя руководство и стратегическую координацию функции централизованной оценки рисков, планирования непрерывности бизнеса (BC) и аварийного восстановления (DR) (см. также рекомендацию 7 SSR2: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления) в сфере внутренней безопасности корпорации, включая корневой сервер, управляемый ICANN (IMRS, широко известный как «корневой сервер L»), и координировать свои действия с другими заинтересованными сторонами, участвующими во внешней глобальной системе идентификаторов, а также публикацию методологии и подхода к оценке рисков.	Корпорация ICANN	Умеренно высокий
2.4	Корпорация ICANN должна включить в описание этой роли, что эта роль будет нести ответственность за все связанные с безопасностью статьи бюджета и обязанности и принимать участие во всех связанных с безопасностью переговорах по контрактам (например, соглашения с регистратурами и регистраторами, цепочки поставок оборудования и программного обеспечения и связанные с ними соглашения об уровне обслуживания), заключенные корпорацией ICANN, подписывая все договорные условия, связанные с безопасностью.	Корпорация ICANN	Умеренно высокий
Рекомендация SSR2 № 3: Повышение транспарентности бюджета, связанного с SSR			
3.1	Директор по безопасности (см. рекомендацию № 2 SSR2: Ввести должность ответственного за стратегию и тактику безопасности и управление рисками) должен информировать сообщество от имени корпорации ICANN о стратегии, проектах и бюджете корпорации ICANN в области SSR дважды в год, а также ежегодно обновлять и публиковать обзоры бюджета.	Корпорация ICANN	Высокий

3.2	Правление и корпорация ICANN должны гарантировать, что конкретные статьи бюджета, относящиеся к выполнению корпорацией ICANN функций, связанных с SSR, связаны с конкретными целями и задачами стратегического плана ICANN. Корпорации ICANN следует реализовать эти механизмы посредством последовательного, подробного, ежегодного процесса составления бюджета и отчетности.	Правление и корпорация ICANN	Высокий
3.3	Правление и корпорация ICANN должны создавать, публиковать и запрашивать комментарии общественности по подробным отчетам, касающимся затрат и бюджетирования, связанного с SSR, в рамках цикла стратегического планирования.	Правление и корпорация ICANN	Высокий
Рекомендация SSR2 № 4: Улучшение процессов и процедур управления рисками			
4.1	Корпорации ICANN следует продолжить централизацию управления рисками, четко сформулировать концепцию управления рисками в области безопасности и обеспечить ее стратегическое соответствие требованиям и целям корпорации. Корпорация ICANN должна определить соответствующие показатели успеха и порядок их оценки.	Корпорация ICANN	Высокий
4.2	Корпорация ICANN должна принять и внедрить стандарт ISO 31000 «Управление рисками», а также подтвердить внедрение этого стандарта с привлечением соответствующих независимых аудиторов. Корпорации ICANN следует предоставлять сообществу аудиторские отчеты, возможно, в сокращенной форме. Усилия по управлению рисками должны учитываться в планах и процедурах BC и DR (см. рекомендацию 7 SSR2: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления).	Корпорация ICANN	Высокий
4.3	Корпорация ICANN должна назначить специальное должностное лицо, отвечающее за управление рисками в области безопасности, которое подчиняется директору по безопасности (см. рекомендацию 2 SSR2:	Корпорация ICANN	Высокий

	Ввести должность ответственного за стратегию и тактику безопасности и управление рисками). Это должностное лицо должно регулярно информировать о положении дел и сообщать о реестре рисков в области безопасности и направлять деятельность корпорации ICANN. Выводы должны учитываться в планах и процедурах BC и DR (см. рекомендацию 7 SSR2: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления) и в системе управления информационной безопасностью (ISMS) (см. рекомендацию 6 SSR2: Соблюдать требования к соответствующим системам управления информационной безопасностью и сертификатам безопасности).		
Рекомендация SSR2 № 5: Соблюдать требования к соответствующим системам управления информационной безопасностью и сертификатам безопасности			
5.1	Корпорация ICANN должна внедрить ISMS и пройти аудит и сертификацию третьей стороной в соответствии с отраслевыми стандартами безопасности (например, ITIL, семейство ISO 27000, SSAE-18) для выполнения своих операционных обязанностей. План должен включать дорожную карту и контрольные даты получения сертификатов, а также отмечать области, которые станут целью постоянного улучшения.	Корпорация ICANN	Высокий
5.2	На основе этой ISMS корпорация ICANN должна составить план сертификации и установить требования к обучению должностных лиц корпорации, отслеживать процент выполнения работ, обосновать свой выбор и документально отразить, как сертификаты соответствуют стратегии безопасности и управления рисками корпорации ICANN.	Корпорация ICANN	Высокий
5.3	Корпорации ICANN следует требовать от внешних сторон, предоставляющих услуги корпорации ICANN, соблюдения соответствующих стандартов безопасности и документирования их комплексных проверок в отношении поставщиков товаров и услуг.	Корпорация ICANN	Высокий

5.4	Корпорация ICANN должна обратиться к сообществу и более широкой общественности с четкими отчетами, демонстрирующими, что корпорация ICANN делает и чего добивается в сфере безопасности. Эти отчеты были бы наиболее полезными, если бы они содержали информацию, описывающую, как корпорация ICANN следует передовым практикам и зрелым, постоянно совершенствующимся процессам управления рисками, безопасностью и уязвимостями.	Корпорация ICANN	Высокий
Рекомендация SSR2 № 6: Раскрытие уязвимостей SSR и транспарентность			
6.1	Корпорации ICANN следует активно продвигать добровольное принятие передовых методов и целей SSR для раскрытия информации об уязвимостях сторонами, связанными договорными отношениями. Если добровольных мер окажется недостаточно для внедрения таких передовых практик и целей, корпорация ICANN должна реализовать передовые практики и цели в контрактах, соглашениях и MoU.	Корпорация ICANN	Высокий
6.2	Корпорация ICANN должна внедрить слаженный процесс раскрытия информации об уязвимостях. Информация о проблемах, связанных с SSR, таких как нарушения обязательств сторонами, связанными договорными обязательствами, и в случае выявления и доведения до сведения корпорации ICANN информации о критических уязвимостях, должна незамедлительно раскрываться и доводиться до сведения соответствующих доверенных сторон (например, тех, кто пострадал или должен исправить данную проблему). Корпорация ICANN должна регулярно сообщать об уязвимостях (не реже одного раза в год), включая анонимные показатели и использование ответственного раскрытия информации.	Корпорация ICANN	Высокий
Рекомендация SSR2 № 7: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления			
7.1	Корпорация ICANN должна разработать план обеспечения бесперебойной деятельности	Корпорация ICANN	Умеренно высокий

	для всех систем, находящихся в собственности или в ведении корпорации ICANN, на основе стандарта ISO 22301 «Менеджмент непрерывности бизнеса», определив приемлемые сроки для BC и DR.		
7.2	Корпорация ICANN должна обеспечить, чтобы план DR для операций по открытым техническим идентификаторам (PTI) (т. е. по функциям IANA) охватывал все уместные системы, способствующие безопасности и стабильности DNS, а также управление корневой зоной и соответствовал стандарту ISO 27031. Корпорация ICANN должна разработать этот план в тесном сотрудничестве с Консультативным комитетом системы корневых серверов (RSSAC) и операторами корневых серверов (RSO).	Корпорация ICANN	Умеренно высокий
7.3	Корпорация ICANN также должна разработать план DR для всех систем, находящихся в собственности или в ведении корпорации ICANN, опять же на основе стандарта ISO 27031.	Корпорация ICANN	Умеренно высокий
7.4	Корпорация ICANN должна создать новый сайт аварийного восстановления для всех систем, находящихся в собственности или в ведении корпорации ICANN, с целью замены сайтов в Лос-Анджелесе или Калпепере или добавления постоянного третьего сайта. Корпорации ICANN следует разместить этот сайт за пределами Североамериканского региона и любых территорий Соединенных Штатов. Если корпорация ICANN решит заменить один из существующих сайтов, любой сайт, который заменяет корпорация ICANN, не следует закрывать до тех пор, пока корпорация не убедится, что новый сайт полностью функционирует и способен обрабатывать аварийное восстановление этих систем для корпорации ICANN.	Корпорация ICANN	Умеренно высокий
7.5	Корпорации ICANN следует опубликовать сводку своих общих планов и процедур BC и DR. Это повысит транспарентность и надежность, помимо решения стратегических целей и задач корпорации ICANN. Для проверки соответствия этим планам BC и DR корпорации ICANN следует привлечь независимого аудитора.	Корпорация ICANN	Умеренно высокий

Рекомендация SSR2 № 8: Обеспечение и демонстрация представления общественных интересов в переговорах со сторонами, связанными договорными обязательствами			
8.1	Корпорации ICANN следует создать группу по ведению переговоров, в которую входят эксперты по вопросам злоупотреблений и безопасности, не связанные со сторонами по контракту или не оплачиваемые ими, для представления интересов организаций, не связанных контрактами, и работы с корпорацией ICANN над пересмотром условий контрактов со сторонами добросовестно, с публичной транспарентностью и с целью улучшения SSR DNS для конечных пользователей, предприятий и правительств.	Корпорация ICANN	Средний
Рекомендация SSR2 № 9: Мониторинг и обеспечение соблюдения обязательств			
9.1	Правление ICANN должно поручить отделу по контролю исполнения договорных обязательств контролировать и строго обеспечивать соблюдение сторонами по контракту текущих и будущих обязательств по SSR и связанных со злоупотреблениями обязательств в контрактах, базовых соглашениях, временных спецификациях и политиках сообщества.	Правление ICANN	Высокий
9.2	Корпорация ICANN должна активно отслеживать и обеспечивать выполнение договорных обязательств регистратурами и регистраторами для повышения точности регистрационных данных. Этот мониторинг и обеспечение должны включать проверку адресных полей и проведение периодических аудитов точности регистрационных данных. Корпорации ICANN следует сосредоточить свои правоприменительные усилия на тех регистраторах и регистратурах, в отношении которых ежегодно поступает более 50 жалоб или сообщений в отношении предоставления ими неточных данных в корпорацию ICANN.	Корпорация ICANN	Высокий
9.3	Корпорация ICANN должна проводить внешний аудит деятельности по обеспечению соблюдения обязательств не реже одного раза в год и публиковать отчеты об аудите и ответ корпорации ICANN на рекомендации аудита, включая планы выполнения.	Корпорация ICANN	Высокий

9.4	Корпорации ICANN следует поручить функции соблюдения обязательств и публикации регулярных отчетов с перечислением отсутствующих инструментов, которые помогли бы поддерживать корпорацию ICANN в целом для эффективного использования договорных рычагов в целях устранения угроз безопасности DNS, включая меры, которые потребуют внесения изменений в контракты.	Корпорация ICANN	Высокий
Рекомендация SSR2 № 10: Обеспечение ясности определений терминов, связанных со злоупотреблениями			
10.1	Корпорации ICANN следует опубликовать веб-страницу, содержащую рабочее определение неправильного использования DNS, т. е. того, которое она использует для проектов, документов и контрактов. В определении следует четко указать, какие типы угроз безопасности корпорация ICANN в настоящее время рассматривает в рамках своей компетенции для устранения с помощью договорных механизмов и механизмов соблюдения требований, а также те угрозы, которые корпорация ICANN считает выходящими за рамки ее компетенции. Если корпорация ICANN использует другую подобную терминологию – например, угроза безопасности, злонамеренное поведение – корпорация ICANN должна включить как свое рабочее определение этих терминов, так и то, как корпорация ICANN отличает эти термины от неправильного использования DNS. Эта страница должна включать ссылки на выдержки из всех текущих обязательств, связанных со злоупотреблениями, в контрактах со сторонами по договору, включая любые процедуры и протоколы реагирования на злоупотребления. Корпорация ICANN должна обновлять эту страницу ежегодно, датировать последнюю версию и ссылаться на более старые версии с соответствующими датами публикации.	Корпорация ICANN	Высокий
10.2	Создать поддерживаемую персоналом сквозную рабочую группу сообщества (CCWG) для создания процесса разработки определений запрещенного неправильного использования DNS, по крайней мере, один	Корпорация ICANN	Высокий

	раз в два года, по предсказуемому графику (например, каждый второй январь), что не займет более 30 рабочих дней на выполнение. В эту группу должны входить заинтересованные стороны, представляющие защиту потребителей, операционную кибербезопасность, научные или независимые исследования кибербезопасности, правоохранительные органы и электронную коммерцию.		
10.3	Правление и корпорация ICANN должны последовательно использовать согласованные определения в общедоступных документах, контрактах, планах реализации в группах по анализу и других мероприятиях, а также ссылаться на эту веб-страницу.	Корпорация ICANN	Высокий
Рекомендация SSR2 № 11: Решение проблем с доступом к данным CZDS			
11.1	Сообщество ICANN и корпорация ICANN должны предпринять шаги, обеспечивающие своевременный доступ к Централизованной службе файлов корневой зоны (CZDS) без лишних препятствий для запрашивающих данные лиц, например автоматическое продление учетных данных.	Сообщество и корпорация ICANN	Средний
Рекомендация SSR2 № 12: Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку			
12.1	Корпорация ICANN должна создать консультативную группу по анализу неправильного использования DNS, состоящую из независимых экспертов (т. е. экспертов без конфликтов финансовых интересов), чтобы рекомендовать существенный пересмотр отчетности о неправильном использовании DNS с применением действенных данных, проверки, транспарентности и независимой воспроизводимости аналитических данных в качестве приоритетов наивысшего уровня.	Корпорация ICANN	Средний
12.2	Корпорации ICANN следует структурировать свои соглашения с поставщиками данных, чтобы разрешить дальнейший обмен данными для некоммерческого использования, в частности, для проверки	Корпорация ICANN	Средний

	или рецензируемых научных исследований. Эта специальная бесплатная некоммерческая лицензия на использование данных может включать временную задержку, чтобы не мешать коммерческому доходу поставщика данных. Корпорация ICANN должна должна публиковать все условия контрактов о совместном использовании данных на веб-сайте ICANN. Корпорация ICANN должна расторгнуть любые контракты, которые не позволяют независимую проверку методологии, стоящей за блокировкой.		
12.3	Корпорация ICANN должна указывать в публикуемых отчетах регистратуры и регистраторов, чьи домены в наибольшей степени способствуют злоупотреблениям. Корпорация ICANN должна включать данные в пригодных для машинного считывания форматах, в дополнение к графическим данным, представленным в текущих отчетах.	Корпорация ICANN	Средний
12.4	Корпорация ICANN должна сопоставлять и публиковать отчеты о действиях, которые регистратуры и регистраторы предприняли, как добровольно, так и в связи с юридическими обязательствами, в ответ на жалобы о незаконных и/или злонамеренных действиях на основании применимого законодательства в связи с использованием DNS.	Корпорация ICANN	Средний
Рекомендация SSR2 № 13: Повышение транспарентности и подотчетности сообщений о нарушениях			
13.1	Корпорация ICANN должна создать и поддерживать центральный портал для жалоб на злоупотребление DNS, который обеспечивает автоматическую пересылку всех сообщений о злоупотреблениях соответствующим сторонам. Система будет действовать исключительно для получения данных, при этом корпорация ICANN будет собирать и обрабатывать только сводку и метаданные, включая временные метки и типы жалоб (по категориям). Использование системы должно стать обязательным для всех доменов общего пользования (gTLD); участие каждого национального домена верхнего уровня (ccTLD) будет добровольным. Кроме того, корпорация	Корпорация ICANN	Высокий

	ICANN должна предоставлять отчеты о злоупотреблениях (например, по электронной почте) всем ccTLD.		
13.2	Корпорация ICANN должна публиковать количество поданных жалоб в форме, позволяющей независимым третьим сторонам анализировать типы жалоб по DNS.	Корпорация ICANN	Высокий
Рекомендация SSR2 № 14: Создать временную спецификацию для улучшения безопасности на основе доказательств			
14.1	Корпорация ICANN должна создать временную спецификацию, которая требует, чтобы все стороны, связанные договорными обязательствами, сохраняли процентную долю доменов, определенных в обновленных отчетах о неправильном использовании DNS (см. Рекомендацию 13.1 SSR2) как неправомерные, ниже разумного и опубликованного порогового значения.	Корпорация ICANN	Высокий
14.2	Чтобы обеспечить возможность принятия мер по борьбе со злоупотреблениями, корпорация ICANN должна предоставить сторонам по договору списки доменов в их портфелях, идентифицированных как злоупотребляющие, в соответствии с Рекомендацией SSR2 12.2, касающейся независимой проверки данных и методов для внесения доменов в черный список.	Корпорация ICANN	Высокий
14.3	Если количество доменов, связанных с злонамеренной деятельностью, достигнет опубликованного порогового значения, описанного в Рекомендации 14.1 SSR2, корпорация ICANN должна провести расследование, чтобы подтвердить достоверность данных и анализа, а затем направить уведомление соответствующей стороне.	Корпорация ICANN	Высокий
14.4	Корпорация ICANN должна предоставить сторонам по договору 30 дней, чтобы уменьшить долю недобросовестных доменов ниже порогового значения или продемонстрировать ошибочность выводов или данных корпорации ICANN. Если сторона по контракту не внесет исправления в течение 60 дней, отдел соблюдения	Корпорация ICANN	Высокий

	договорных обязательств ICANN должен перейти к процессу отмены аккредитации.		
14.5	Корпорация ICANN должна рассмотреть возможность предложения финансовых стимулов: стороны, связанные договором, в портфелях которых меньше определенного процента доменных имен, используемых для злоупотреблений, должны получить снижение комиссии за платные транзакции до соответствующего порогового значения.	Корпорация ICANN	Высокий
Рекомендация SSR2 № 15: Запустить EPDP для улучшения безопасности на основе доказательств			
15.1	После создания временной спецификации (см. Рекомендацию 14 SSR2: Создать временную спецификацию для улучшения безопасности на основе доказательств) корпорация ICANN должна создать поддерживаемый персоналом ускоренный процесс формирования политики (EPDP) для разработки политики предотвращения злоупотреблений. Волонтеры EPDP должны представлять сообщество ICANN, используя в качестве образца номера и распределение из Временной спецификации для регистрационных данных gTLD, определенной в уставе группы EPDP.	Корпорация ICANN	Высокий
15.2	EPDP должен опираться на фундамент определений CCWG, предложенный в рекомендации 10.2 SSR2. Эта концепция политики должна определять соответствующие контрмеры и действия по исправлению положения для различных типов злоупотреблений, временные рамки для действий сторон по договору, таких как сроки сообщения о злоупотреблениях / отчета об ответах, а также меры по обеспечению соблюдения договорных обязательств ICANN в случае нарушения политики. Корпорация ICANN должна настаивать на праве прекращать действия контрактов в случае систематической практики укрывательства злоупотреблений со стороны любой стороны, связанной контрактом. Результат должен включать механизм обновления каждые два года контрольных показателей и договорных обязательств, связанных со	Корпорация ICANN	Высокий

	злоупотреблениями, с использованием процесса, который не займет более 45 рабочих дней.		
Рекомендация SSR2 № 16: Требования к конфиденциальности и RDS			
16.1	Корпорация ICANN должна размещать единообразные перекрестные ссылки на своем веб-сайте, чтобы предоставлять связную и легко доступную информацию обо всех действиях – прошлых, настоящих и запланированных, – предпринятых по теме конфиденциальности и управления данными, с особым вниманием к информации, касающейся Служба каталогов регистрации (RDS).	Корпорация ICANN	Средний
16.2	Корпорация ICANN должна создать специализированные группы в рамках функции соблюдения договорных обязательств, которые понимают требования и принципы конфиденциальности (такие как ограничение сбора, квалификация данных, спецификация цели и меры безопасности для раскрытия) и которые могут облегчить потребности правоохранительных органов в рамках концепции RDS по мере исправления и принятия сообществом этой концепции (см. также Рекомендацию 11 SSR2: Решение проблем с доступом к данным CZDS).	Корпорация ICANN	Средний
16.3	Корпорация ICANN должна проводить периодическую проверку соблюдения политики конфиденциальности регистраторами, чтобы убедиться в наличии у них процедур для устранения нарушений конфиденциальности.	Корпорация ICANN	Средний
Рекомендация SSR2 № 17: Измерение доменных коллизий			
17.1	Корпорация ICANN должна создать концепцию, которая позволит определить характер и частоту доменных коллизий и возникающие в результате этого проблемы. Эта концепция должна включать метрики и механизмы для измерения степени, в которой управляемое прерывание является успешным для выявления и устранения доменных коллизий. Это может поддерживаться механизмом, обеспечивающим защищенное	Корпорация ICANN	Средний

	раскрытие экземпляров доменных коллизий. Эта концепция должна позволять надлежащую обработку конфиденциальных данных и угроз безопасности.		
17.2	Сообщество ICANN должно разработать четкую политику для предотвращения и разрешения доменных коллизий, связанных с новыми gTLD, и реализовать эту политику до следующего раунда gTLD. Корпорация ICANN должна обеспечить, чтобы оценка этой политики проводилась сторонами, не имеющими финансовой заинтересованности в расширении gTLD.	Сообщество и корпорация ICANN	Средний
Рекомендация SSR2 № 18: Информационное обеспечение дебатов по вопросам политики			
18.1	Корпорация ICANN должна следить за событиями в научном сообществе, уделяя особое внимание конференциям по вопросам исследования сетей и безопасности, включая по крайней мере ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, Симпозиум IEEE по безопасности и конфиденциальности, а также конференции по оперативной безопасности и FIRST, и публиковать для сообщества ICANN отчет, в котором обобщаются последствия публикаций, имеющих отношение к работе корпорации ICANN или сторон, связанных договорными обязательствами.	Корпорация ICANN	Низкий
18.2	Корпорация ICANN должна обеспечить, чтобы эти отчеты содержали важную информацию, которая может повлиять на рекомендации относительно действий, в том числе изменений в договорах с регистратурами и регистраторами, которые могли бы смягчить, предотвратить или устранить вред потребителям и инфраструктуре в области SSR, который указан в рецензируемой научной литературе.	Корпорация ICANN	Низкий
18.3	Корпорация ICANN должна обеспечить, чтобы эти отчеты также включали рекомендации по дополнительным исследованиям для подтверждения результатов экспертной оценки, описание того, какие данные потребуются сообществу	Корпорация ICANN	Низкий

	для проведения дополнительных исследований, и то, как корпорация ICANN может предложить помощь брокеру в доступе к таким данным, например через CZDS.		
Рекомендация SSR2 № 19: Полная разработка набора тестов регрессии DNS			
19.1	Корпорация ICANN должна завершить разработку пакета для тестирования резолверов DNS.	Корпорация ICANN	Низкий
19.2	Корпорация ICANN должна обеспечить возможность продолжения реализации и поддержки функционального тестирования различных конфигураций и версий программного обеспечения.	Корпорация ICANN	Низкий
Рекомендация SSR2 № 20: Официальные процедуры обновления ключей			
20.1	Корпорация ICANN должна установить формальную процедуру, опирающуюся на формальный инструмент и язык моделирования процессов, чтобы определить детали будущих обновлений ключа, включая точки принятия решений, ветви обработки исключений, полный поток управления и т. д. Проверка процесса обновления ключа должна предусматривать опубликование программной процедуры (например, программы, системы с конечным числом состояний (FSM)) для общественного обсуждения, и корпорация ICANN должна включать отзывы сообщества. У процесса на каждом этапе должны быть эмпирически проверяемые критерии приемлемости, которые должны соблюдаться для продолжения процесса. Этот процесс должен подвергаться пересмотру не реже самого обновления ключа (то есть с той же периодичностью), чтобы корпорация ICANN могла использовать извлеченные уроки для корректировки процесса.	Корпорация ICANN	Средний
20.2	Корпорация ICANN должна создать группу заинтересованных сторон с участием соответствующего персонала (из корпорации ICANN или сообщества) для периодического проведения деловых игр по окончании процесса обновления ключа KSK корневой зоны.	Корпорация ICANN	Средний

Рекомендация SSR2 № 21: Повышение безопасности связи с операторами TLD			
21.1	Операции корпорации ICANN и PTI должны ускорить внедрение новых мер безопасности системы управления корневой зоной (RZMS) в отношении аутентификации и авторизации запрошенных изменений и предоставить операторам TLD возможность воспользоваться этими мерами безопасности, в частности, MFA и шифрованной электронной почтой.	Корпорация ICANN и PTI	Средний
Рекомендация SSR2 № 22: Измерение качества услуг			
22.1	Для каждой службы, находящейся в сфере управления корпорации ICANN, включая корневую зону и службы, связанные с gTLD, а также регистратуры IANA, корпорация ICANN должна создать список статистических данных и показателей, отражающих рабочее состояние (например, доступность и скорость реагирования) этой службы, и опубликовать каталог этих услуг, наборов данных и показателей на одной странице веб-сайта icann.org, например, на платформе открытых данных. Корпорация ICANN должна произвести измерения для каждой из этих услуг в виде сводных данных как за предыдущий год, так и в долгосрочном плане (для иллюстрации базового поведения).	Корпорация ICANN	Низкий
22.2	Корпорация ICANN должна ежегодно запрашивать у сообщества отзывы об измерениях. Эти отзывы следует рассматривать, публично резюмировать после каждого отчета и включать в последующие отчеты. Данные и связанные с ними методологии, используемые для измерения результатов этих отчетов, следует архивировать и делать общедоступными, чтобы способствовать воспроизводимости.	Корпорация ICANN	Низкий
Рекомендация SSR2 № 23: Обновление алгоритма			
23.1	Операции PTI должны обновлять методику поддержки DNSSEC на корневых серверах (DPS), чтобы разрешить переход от одного алгоритма цифровой подписи к другому,	PTI	Средний

	включая ожидаемый переход от алгоритма цифровой подписи RSA к другим алгоритмам или к будущим постквантовым алгоритмам, которые обеспечивают такие же или более высокие показатели безопасности и сохранение или повышение устойчивости DNS.		
23.2	Поскольку обновление алгоритма DNSKEY корневой зоны — очень сложный и требующий особого внимания процесс, PTI должна сотрудничать с другими партнерами корневой зоны и мировым сообществом при подготовке согласованного плана будущего обновления алгоритма DNSKEY корневой зоны с учетом уроков, извлеченных из первого обновления KSK в 2018 году.	PTI	Средний
Рекомендация SSR2 № 24: Повышение транспарентности и сквозного тестирования процесса EBERO			
24.1	Корпорация ICANN должна координировать сквозное тестирование всего процесса EBERO через заранее определенные промежутки времени (не реже одного раза в год), используя план тестирования, который включает наборы данных, используемые для тестирования, состояния выполнения и крайние сроки, и заранее согласовывается со сторонами, связанными с ICANN, чтобы обеспечить выполнение всех этапов исключения и опубликовать результаты.	Корпорация ICANN	Средний
24.2	Корпорация ICANN должна упростить поиск Общего руководства по процессу перехода, предоставив ссылки на веб-сайте EBERO.	Корпорация ICANN	Средний

2. Определение приоритетов

Группа по анализу SSR2 привела все рекомендации SSR2 в соответствие со стратегическим планом ICANN на 2021–2025 годы, а также со своими целями и задачами.[6] Группа проверки удалила из этого отчета все рекомендации, которые явно не соответствовали стратегическому плану. Все рекомендации RT SSR2 соответствуют стратегическому плану корпорации ICANN и поэтому считаются важными.

Группа по анализу SSR2 использовала инструмент онлайн-опроса (интернет-решение Qualtrics) для опроса всех членов группы на предмет их мнений относительно приоритета

[6] См. Приложение E: Сопоставление рекомендаций SSR2 со Стратегическим планом ICANN на 2021-2025 годы и Уставом ICANN.

каждой группы рекомендаций в этом отчете.[7] Этот опрос позволил оценить каждую группу по пятибалльной шкале, которая варьировалась от очень низкого приоритета, низкого приоритета, среднего приоритета, высокого приоритета до очень высокого приоритета.

Группа по анализу определила, что из двадцати четырех групп рекомендаций двадцать семь конкретных рекомендаций должны считаться высокоприоритетными, большинство из которых касается управления внутренней безопасностью корпорации ICANN и действий по борьбе со злоупотреблениями. Девять рекомендаций имеют умеренно высокий приоритет. Восемнадцать рекомендаций, преимущественно из разделов, посвященных глобальной DNS, были оценены как средний приоритет, а остальные восемь рекомендаций были оценены как более низкий приоритет.

C. Выполнение рекомендаций SSR1 и ожидаемые результаты

В 2012 году Правление ICANN пришло к заключению, *«что 28 рекомендаций в итоговом отчете [SSR1] осуществимы»,* единогласно приняло их и поручило персоналу выполнить все 28 рекомендаций SSR1.[8] Помимо прочего, группе по анализу SSR2 было поручено оценить «*степень выполнения рекомендаций, полученных после предыдущего анализа SSR, а также степень, в которой выполнение данных рекомендаций привело к ожидаемому эффекту».*

Процесс и методология, которые группа по анализу SSR2 использовала для оценки выполнения рекомендаций и их воздействия кратко изложены в Приложении C: «Процесс и методология». В этом разделе описан процесс оценки, виды использованных фактов и данных, а также утвержденная методология вынесения заключения о степени выполнения рекомендаций. Выводы группы по анализу SSR2 и их обоснование для каждой из рекомендаций SSR1 представлены в Приложении D: «Выводы, относящиеся к рекомендациям SSR1».

Каждая проверка позволяет извлечь новые уроки. Поэтому, оценив рекомендации SSR1, группа по анализу SSR2 отмечает важность и необходимость предоставления рекомендаций, в основе которых лежат измеримые показатели эффективности, которых часто не хватало в рекомендациях SSR1. Это наблюдение подкрепляется необходимостью обеспечивать результативность выполнения и оценки любых рекомендаций будущих групп по анализу.

[7] См. https://www.qualtrics.com/.

[8] ICANN, «Очередное заседание Правления ICANN», в последней редакции от 18 октября 2012 года, https://www.icann.org/resources/board-material/minutes-2012-10-18-en; «Итоговый отчет группы по анализу безопасности, стабильности и отказоустойчивости DNS», группа по анализу SSR, 20 июня 2012 года, https://www.icann.org/en/system/files/files/final-report-20jun12-en.pdf.

1. Краткая сводка: Проверка SSR1

Группа по анализу SSR2 рассмотрела 28 рекомендаций SSR1 и пришла к заключению, что все 28 рекомендаций сохраняют свою актуальность на момент публикации настоящего отчета (см. Таблицу 2).[9] По мнению группы, ни одна из рекомендаций не выполнена полностью по причинам, изложенным в Приложении D: «Выводы, относящиеся к рекомендациям SSR1».

Таблица 2. Обзор рекомендаций SSR1

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Актуально																												
Выполнено																												
Результативно																												

Пояснение: Д = Да, Н = Нет, Ч = Частично, - = Невозможно определить

Группа по анализу SSR2 отмечает следующие неоднократно возникающие проблемы:

1. Как правило, в рекомендациях SSR1 и соответствующих планах по их выполнению отсутствуют индикаторы, показатели и цели, которые позволили бы сообществу и корпорации ICANN отслеживать и понимать ситуацию и собственную деятельность в сфере безопасности.

2. Отсутствуют доступные для всеобщего ознакомления факты, определения и процедуры, что препятствует независимому наблюдению за деятельностью в области SSR. Такой дефицит информации приводит к отсутствию ясности в отношении того, выполнила ли корпорация ICANN рекомендации SSR1 и каким образом.

3. Отсутствует проверка сообществом и подотчетность в отношении различных планов по выполнению рекомендаций, что лишает сообщество ICANN возможности вносить свой вклад по вопросам SSR.

4. В настоящее время у корпорации ICANN нет всеобъемлющей стратегии, конкретных целей или четкой и всесторонней политики в области SSR. В отсутствие конструктивной стратегии в области SSR и интегрированного управления безопасностью и рисками (например, политики, процедур, стандартов, базовых показателей, руководящих принципов) обязанности, связанные с SSR, не возлагаются, а их выполнение не измеряется и не отслеживается, что приводит к недостаточной транспарентности и подотчетности и наличию очевидных пробелов в обязанностях корпорации ICANN, связанных с SSR.

[9] ICANN, Отчет о выполнении рекомендаций по итогам проверки SSR, июнь 2015 года: https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf.

Группа по анализу SSR2 признает, что первоначальные ориентиры, предоставленные группой по анализу SSR1, не всегда были достаточно измеримыми, и хотя корпорация ICANN сообщила, что, по ее мнению, все рекомендации были выполнены, планы выполнения этих рекомендаций также часто были нечеткими и плохо поддающимися количественной оценке. В связи с этим группа по анализу SSR2 не смогла признать рекомендации SSR1 полностью выполненными. Корпорация ICANN должна провести дополнительную комплексную проверку выполнения рекомендаций SSR1 с учетом выводов, представленных группой по анализу SSR2.

В настоящий отчет также включены предложения, выходящие за рамки проверки SSR2 (см. Приложение A. «Дополнительные предложения»), чтобы будущие группы по анализу смогли избежать некоторых проблем, с которыми столкнулась группа по анализу SSR2.

Рекомендация SSR2 № 1: Дальнейший анализ SSR1

1.1. Правление и корпорация ICANN должны провести дальнейшую всестороннюю проверку рекомендаций SSR1 и реализовать новый план для завершения выполнения рекомендаций SSR1 (см. Приложение D: Выводы, относящиеся к рекомендациям SSR1).

D. Основные вопросы стабильности в ICANN

Основное внимание в этом разделе уделяется областям, касающимся разделов 4.6(c) (ii) A, 4.6(c) (ii) B и 4.6(c) (iii) Устава ICANN.[10] К ним относятся физическая и сетевая безопасность, стабильность и отказоустойчивость в контексте координирования системы уникальных идентификаторов интернета; концепция планирования действий по обеспечению безопасности в случае непредвиденных обстоятельств для системы уникальных идентификаторов интернета; полнота и эффективность внутренних процедур обеспечения безопасности корпорации ICANN и концепции безопасности ICANN.

Фундаментальная проблема, которая лежит в основе рекомендаций этого раздела, — это отсутствие у группы по анализу SSR2 фактов, демонстрирующих, что у корпорации ICANN есть эффективная, всеобъемлющая и транспарентная программа в области SSR. При проверке внутренней безопасности корпорации ICANN стало ясно, что корпорация ICANN осуществляет различные проекты и принимает различные меры, связанные с безопасностью. Однако группе по анализу не удалось обнаружить достаточно исчерпывающих доказательств существования программы управления информацией и обеспечения безопасности, надлежащим образом организованной и задокументированной (см. раздел D.3. «Управление рисками и безопасностью»), процессов обеспечения непрерывности бизнеса и аварийного восстановления (см. раздел D.4. «Управление непрерывностью бизнеса») или в целом независимой структуры обеспечения безопасности, подходящей для организации, которая поддерживает критически важную для функционирования интернета систему (см. Раздел D.1. «Совершенствование организационной структуры»).

[10] См. Приложение H — разделы Устава и Стратегического плана, наиболее актуальные для рекомендаций SSR2 из данного отчета, где приведены копии разделов Устава и Стратегического плана ICANN на 2021–2025 годы, которые имеют наибольшее отношение к SSR.

Устав гласит, что корпорация ICANN должна «*в максимально возможной степени придерживаться принципов открытости и транспарентности и действовать в соответствии с процедурами, нацеленными на соблюдение справедливости*».[11] Рекомендации этого раздела призваны помочь корпорации ICANN максимально улучшить раскрытие информации и транспарентность SSR во всех аспектах с учетом задач в сфере безопасности. Следуя этим рекомендациям, корпорация ICANN эффективно и результативно устранит краеугольную проблему информационной транспарентности и отсутствия четкой, очевидной руководящей и организационной роли в области безопасности.

1. Совершенствование организационной структуры — должность директора по безопасности

В настоящее время связанная с SSR деятельность корпорации ICANN распределена по всей организации. Группа по анализу SSR2 принимает во внимание функции офиса технического директора (OCTO), в обязанности которого помимо прочего входит следующее:

Изучение вопросов, связанных с системой уникальных идентификаторов интернета (доменные имена, IP-адреса/номера AS, параметры протокола и т. д.)

Содействие повышению безопасности, стабильности и отказоустойчивости этих идентификаторов.[12]

Также есть директор по информационным технологиям, в сферу ответственности которого, как правило, входит *«мониторинг и обслуживание систем и технических операций, корпоративная безопасность, информационные технологии ICANN и работа технического отдела ICANN по обслуживанию DNS (http://www.dns.icann.org/), управляющего корневым сервером L и сетевыми службами DNS ICANN»,*[13] а также защита, мониторинг и управление информационными активами, такими как конфиденциальные данные сторон, связанных договорными обязательствами.

Корпорация ICANN должна ввести должность руководителя высшего звена, отвечающего за все вопросы, связанные с безопасностью, включая постановку стратегических целей, управление соблюдением нормативных требований и составление бюджета, а также за защиту активов организации.[14]

К компетенции этого должностного лица будут относиться несколько положений Устава ICANN и обязательств в Стратегическом плане ICANN на 2021–2025 ФГ. Кроме того, рекомендация SSR1 № 24 предусматривала создание централизованной службы безопасности.[15] В существующей структуре эти обязанности распределены между

[11] Устав ICANN, раздел 3.1: https://www.icann.org/resources/pages/governance/bylaws-en/#article3

[12] Офис технического директора (OCTO) ICANN, источник проверен 27 декабря 2019 года: https://www.icann.org/octo.

[13] ICANN, «Информационные системы и инновации», источник проверен 21 января 2020 года: https://www.icann.org/resources/pages/technical-functions-cio.

[14] Институт педагогических наук (IES): Национальный центр статистики образования, «ГЛАВА 3. Политика в области безопасности: разработка и внедрение», источник проверен 9 декабря 2020 года: https://nces.ed.gov/pubs98/safetech/chapter3.asp.

[15] См. Приложение D: «Выводы, относящиеся к рекомендациям SSR1».

двумя обособленными подразделениями корпорации ICANN. Централизованное управление позволило бы повысить эффективность управления стратегической координацией всей соответствующей деятельности за счет консолидации работы в рамках одной роли с соразмерным бюджетом.[16] Это будет способствовать усилиям по предоставлению сообществу и будущим группам по анализу согласованной и непротиворечивой документации.

Рекомендация SSR2 № 2: Ввести должность ответственного за стратегию и тактику безопасности и управление рисками

Группа по анализу SSR2 считает, что в корпорации ICANN должен быть руководитель высшего звена, который занимается координацией и стратегическим управлением деятельностью корпорации ICANN, связанной с безопасностью и рисками для безопасности, а также реализацией миссии и стратегических целей ICANN в области безопасности.[17]

2.1. Корпорация ICANN должна ввести должность директора по безопасности (CSO) или директора по информационной безопасности (CISO) на уровне высшего руководства корпорации ICANN, нанять на эту должность квалифицированного специалиста и выделить конкретный бюджет, достаточный для выполнения соответствующих функциональных задач.

2.2. Корпорации ICANN следует включить в должностную инструкцию этого лица задачи управления функцией обеспечения безопасности корпорации ICANN и контроля за взаимодействием персонала во всех соответствующих областях, влияющих на безопасность. Лицо на этой должности будет предоставлять регулярные отчеты Правлению ICANN и сообществу по всей деятельности, связанной с SSR, в рамках корпорации ICANN. Существующие функции безопасности следует реструктурировать и переместить в организационном плане, чтобы они вошли в компетенцию этой новой должности.

2.3. Корпорации ICANN следует предусмотреть в должностной инструкции этого лица ответственность как за стратегическое, так и за тактическое управление безопасностью и рисками. Эти области ответственности охватывают управление централизованной оценкой рисков и ее стратегическую координацию, а также планирование непрерывности бизнеса (BC) и аварийного восстановления (DR) (см. рекомендацию SSR2 № 7: Улучшить процессы и процедуры обеспечения непрерывности бизнеса и аварийного восстановления) в сфере внутренней безопасности корпорации, включая корневой сервер, находящийся под управлением ICANN (IMRS, широко известный как «корневой сервер L»), координацию действий с другими заинтересованными сторонами во внешней глобальной системе идентификаторов, а также публикацию методологии и подхода к оценке рисков.

---

[16] См. пункт 5.1 в стандартах и сериях стандартов Международной организации по стандартизации ISO 27001, ISO/IEC 27001:2013 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования», который также соответствует SSAE18 2017 года «Критерии трастовых услуг CC1.3/Принцип № 3 COSO»: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/othermapping/trust-services-map-to-iso-27001.xlsx.

[17] Правление ICANN может руководствоваться такими ресурсами, как справочник рисков для кибербезопасности Национальной ассоциации директоров корпораций, «Справочник NACD по контролю киберрисков для директоров», 2017 год: http://boardleadership.nacdonline.org/Cyber-Risk-Handbook-GCNews.html.

2.4. Корпорации ICANN следует предусмотреть в должностной инструкции этого лица ответственность за все связанные с безопасностью статьи бюджета и обязанности, а также участие в любых связанных с безопасностью переговорах корпорации ICANN по контрактам (например, соглашения с регистратурами и регистраторами, цепочки поставок оборудования и программного обеспечения и соответствующие соглашения об уровне обслуживания) для утверждения всех договорных условий, касающихся безопасности.

Эту рекомендацию можно будет считать выполненной после введения и заполнения корпорацией ICANN должности директора по безопасности с обязанностями, указанными в рекомендациях.

Эту рекомендацию можно будет считать действенной, если централизация корпорацией ICANN обязанностей по обеспечению безопасности с полной очевидностью позволит корпорации ICANN координировать деятельность и бюджет в области SSR и обсуждать вопросы безопасности на соответствующем уровне управления.

2. Бюджеты и отчетность, связанные с SSR

Хотя корпорация ICANN, возможно, охватывает связанную с SSR деятельность в различных статьях своего годового бюджета, остается неясным, как корпорация ICANN в настоящее время распределяет средства на конкретные функции, относящиеся к SSR. В этом разделе отчета SSR2 исследуются цели и результаты (где их можно обнаружить и измерить) рекомендаций SSR1, касающихся составления бюджета и отчетности в области SSR.

Рекомендации SSR1 № 20, 21 и 22 затрагивают различные аспекты потребности в более детальном и транспарентном наборе процессов составления бюджета и отчетности по статьям бюджета, относящимся к SSR. Например, рекомендация SSR1 № 20 предусматривает большую степень детализации для изучения и общественного обсуждения статей бюджета, относящихся SSR, а также для регулярной проверки.[18] [19] В рекомендации SSR1 № 21 указано, что ICANN должна создать более упорядоченный внутренний процесс для демонстрации связи решений по организационной структуре и бюджетным средствам с концепцией обеспечения SSR, включая лежащий в основе анализ издержек и выгод. В рекомендации SSR1 № 22 корпорации ICANN рекомендовано публиковать, постоянно контролировать и обновлять документацию по организационной структуре и бюджетным ресурсам, необходимым для решения различных вопросов SSR во взаимосвязи с вводом новых gTLD.

Для оценки степени выполнения корпорацией ICANN этих рекомендаций группа по анализу SSR2 изучила документы, находящиеся в открытом доступе, документы, предоставленные группе по анализу корпорацией ICANN, отчет о выполнении рекомендаций SSR1 и полученные ответы на многие вопросы, отправленные персоналу корпорации ICANN.[20] Корпорация ICANN не предоставила группе по анализу SSR2 никакой дополнительной информации, помимо детализации сведений, полученных от

[18] Подробнее о результатах и выводах группы по анализу SSR2 в отношении этих рекомендаций см. Приложение D — рекомендация SSR1 № 20 и рекомендация SSR1 № 22.

[19] ICANN, «Концепция безопасности, стабильности и отказоустойчивости систем идентификаторов на 2015–2016 ФГ», 15 сентября 2016 года: https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

[20] Вики-страница группы по анализу SSR2 ICANN, справочные материалы, источник проверен 10 декабря 2020 года: https://community.icann.org/display/SSR/Background+Materials.

персонала группой SSR1, которые привели к этим первоначальным рекомендациям (рекомендации SSR1 № 20, 21 и 22). Группа по анализу обнаружила, что, хотя ежегодная отчетность о деятельности в области SSR действительно предоставляется в составе документов концепции IS-SSR и годовых отчетов, большая часть информации, относящейся к вопросам бюджетирования SSR, носит слишком общий характер, что не соответствует рекомендации по итогам проверки SSR1. Годовой бюджет корпорации ICANN не содержит подробной информации о деятельности, связанной с SSR, а подготовка документов в рамках концепции IS-SSR прекращена.[21]

Если рассматривать конкретно Программу New gTLD корпорации ICANN, в структуре и бюджете новой программы отражены на верхнем уровне вопросы SSR, связанные с программой создания новых gTLD (например, Комиссия по стабильности DNS, EBERO).[22] Однако корпорация ICANN не достигла желаемых результатов в виде повышения детализации данных и ясности информации, касающейся организационной структуры и бюджета для реализации концепции IS-SSR и выполнения функций SSR, связанных с Программой New gTLD. Примечательно, что в архиве документов по безопасности, стабильности и отказоустойчивости систем идентификаторов ICANN (IS-SSR) нет ни одного документа, относящегося к Программе New gTLD.[23] При изучении документов концепции IS-SSR и годовых отчетов за 2016 год выяснилось, что gTLD упоминаются дважды: один раз в Модуле A как тенденция в экосистеме интернета и еще раз в Модуле B как часть общего стратегического плана ICANN.[24] В предыдущей концепции, опубликованной в марте 2013 года, корпорация ICANN называет Программу New gTLD «тенденцией» и движущей силой политики для Организации поддержки доменов общего пользования (GNSO).[25] За исключением этого, Программа New gTLD упоминается только в разделе, посвященном выполнению рекомендаций SSR1. Хотя корпорация ICANN опубликовала годовой отчет, где указаны прямые затраты на совместно используемые ресурсы и затраты на вспомогательные функции, выделенные для SSR, в этом отчете отсутствует разбивка финансирования, ресурсов или другой деятельности в разрезе Программы New gTLD.[26]

Резюмируя соображения группы по анализу в данной области, следует отметить: хотя корпорация ICANN, возможно, охватывает связанную с SSR деятельность в различных статьях своего годового бюджета, остается неясным, как корпорация ICANN распределяет средства на конкретные функции, относящиеся к SSR. Группе по анализу не удалось найти фактов, подтверждающих наличие у корпорации ICANN отчетности о влиянии мероприятий

[21] ICANN, «Текущая финансовая информация ICANN (2020 и 2021 ФГ)», дата не указана: https://www.icann.org/resources/pages/governance/current-en, и ICANN, «Архив документов IS-SSR», дата не указана: https://www.icann.org/ssr-document-archive. Примечание: Бюджет ICANN не содержит отчетов о каких-либо конкретных расходах, связанных с SSR.В архиве документов IS-SSR нет документов концепции IS-SSR, составленных после 2015–2016 ФГ.

[22] ICANN, «Утвержденный бюджет Интернет-корпорации по присвоению имен и номеров (ICANN) на 2021 ФГ», 7 мая 2020 года, 26–28, https://www.icann.org/en/system/files/files/adopted-budget-fy21-07may20-en.pdf.

[23] Архив документов IS-SSR: https://www.icann.org/ssr-document-archive

[24] ICANN, Концепция IS-SSR на 2015–2016 ФГ: https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

[25] ICANN, «Концепция безопасности, стабильности и отказоустойчивости», март 2013 год, 8, https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf.

[26] ICANN, «План операционной деятельности, связанной с SSR на 2018 ФГ», дата не указана: https://community.icann.org/x/DqNYAw.

в сфере SSR на бюджет и соответствующие ресурсы. Если такие документы и существуют, то они недоступны.

Рекомендация SSR2 № 3: Повышение транспарентности бюджета, связанного с SSR

3.1. Директор по безопасности (см. рекомендацию № 2 SSR2: Ввести должность ответственного за стратегию и тактику безопасности и управление рисками) должен информировать сообщество от имени корпорации ICANN о стратегии, проектах и бюджете корпорации ICANN в области SSR дважды в год, а также ежегодно обновлять и публиковать обзоры бюджета.

3.2. Правлению и корпорации ICANN следует связать конкретные статьи бюджета, относящиеся к выполнению корпорацией ICANN своих функций в области SSR, с конкретными целями и задачами стратегического плана ICANN. Корпорация ICANN должна реализовать эти механизмы посредством последовательного, подробного, ежегодного процесса составления бюджета и отчетности.

3.3. Правлению и корпорации ICANN следует создавать, публиковать и выносить на общественное обсуждение подробные отчеты, касающиеся затрат и бюджетирования в области SSR, в рамках цикла стратегического планирования.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN передаст все соответствующие функции и статьи бюджета в ведение нового руководителя высшего звена.

Эту рекомендацию можно будет считать действенной, если сообщество ICANN получит ясное представление о бюджете, связанном с SSR.

3. Управление рисками и безопасностью

Управление рисками для безопасности — это непрерывный процесс, который позволяет организации выявлять риски для безопасности и реализовывать стратегии снижения таких рисков. Группа по анализу обнаружила, что, хотя корпорация ICANN инициировала всестороннюю и целесообразную деятельность в области управления рисками для безопасности, которая привела к подготовке отчета рабочей группы по концепции рисков для DNS и концепции IS-SSR на 2015–2016 ФГ, результаты этой деятельности не поддерживаются в актуальном состоянии.[27] Такое бездействие заставляет сомневаться в завершенности усилий по управлению рисками для безопасности, а именно в цикличности и четкости процессов.

Из-за отсутствия актуальной документации группе по анализу не удалось найти доказательств того, что корпорация ICANN соблюдает отраслевые стандарты и использует передовые методы.[28] К отсутствующей актуальной документации относятся

[27] ICANN, «Отчет о концепции управления рисками для DNS», рабочая группа по концепции управления рисками для DNS, последняя редакция от 4 октября 2013 года: https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en и ICANN, Концепция IS-SSR на 2015–2016 ФГ.

[28] См. рекомендацию SSR2 № 5: Соблюдать требования к соответствующим системам управления информационной безопасностью и сертификатам безопасности, рекомендацию SSR2 № 6: Раскрытие

и крайне важные результаты сторонних проверок подхода корпорации ICANN и ее мер по реализации. В то же время группа по анализу отмечает, что различные стороны, связанные договорными обязательствами, и ccTLD соблюдают соответствующие стандарты безопасности и отраслевые стандарты, подчеркивая тем самым применимость этих стандартов в пространстве DNS.[29] В конечном итоге группе по анализу не удалось определить, проделана ли корпорацией ICANN достаточная работа в области управления рисками для безопасности или нет.

В отсутствие актуальной общедоступной информации члены сообщества и другие стороны (например, правительства, владельцы доменов) также вряд ли смогут оценить работу корпорации ICANN. Следствием такого отсутствия является недостаточная транспарентность, что негативно влияет на соблюдение основных ценностей корпорации ICANN и глобальное доверие к корпорации ICANN и экосистеме DNS. Правильное управление рисками и безопасностью требует наличия четких процессов, которые соответствуют общепризнанным международным стандартам и рекомендациям по передовой практике, а также четких и общедоступных обязанностей и структур. Сторонние проверки, при условии их проведения в соответствии с принятыми стандартами и подготовки общедоступных аудиторских заключений, предоставят возможность оценки с другого ракурса, подтвердят адекватность мер и укрепят доверие между сообществом и корпорацией ICANN. Создание и поддержание структур и процедур управления безопасностью поможет корпорации ICANN более полно и независимо от отдельных сотрудников сохранять свою позицию в области безопасности.

Группа по анализу SSR2 четко осознает, что чрезмерное раскрытие определенной оперативной информации может создать проблемы, особенно в плане безопасности. Тем не менее, корпорация ICANN управляет критически важной системой с глобальным влиянием и должна предоставлять сообществу сведения и данные, имеющие отношение к безопасности. Надзор за процессами раскрытия информации (риск, безопасность и уязвимости), в том числе определение сроков моратория и принятие решений о публичном раскрытии информации, должен входить в круг полномочий директора по безопасности (см. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками).

Рекомендация SSR2 № 4: Улучшение процессов и процедур управления рисками

4.1. Корпорация ICANN должна продолжить централизацию управления рисками, четко сформулировать концепцию управления рисками в области безопасности и обеспечить ее стратегическое соответствие требованиям и целям корпорации. Корпорация ICANN должна определить соответствующие показатели успеха и порядок их оценки.

уязвимостей SSR и транспарентность, а также рекомендацию SSR2 № 7: Рекомендация SSR2 № 7: Улучшить процессы и процедуры обеспечения непрерывности бизнеса и аварийного восстановления.

[29] Примеры ccTLD, сертифицированных в соответствии с ISO/IEC 27001:2013 и (или) ISO 22301:2012: DENIC https://www.denic.de/en/content-pool/information-security-master/, IIS https://internetstiftelsen.se/docs/27001-eng-Certificate.pdf, nic.at https://www.nic.at/en/the-company/certificates-and-awards, Nominet https://www.nominet.uk/security-at-nominet/.

4.2. Корпорация ICANN должна принять и внедрить стандарт ISO 31000 «Управление рисками», а также подтвердить внедрение этого стандарта с привлечением соответствующих независимых аудиторов.[30] Корпорации ICANN следует предоставлять сообществу аудиторские отчеты, возможно, в сокращенной форме. Усилия по управлению рисками должны учитываться в планах и процедурах BC и DR (см. рекомендацию 7 SSR2: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления).

4.3. Корпорации ICANN следует назначить специальное должностное лицо, отвечающее за управление рисками в области безопасности, которое подчиняется директору по безопасности (см. рекомендацию SSR2 № 2: Ввести должность ответственного за стратегию и тактику безопасности и управление рисками). Это должностное лицо должно регулярно информировать о положении дел и сообщать о реестре рисков в области безопасности и направлять деятельность корпорации ICANN. Выводы должны учитываться в планах и процедурах BC и DR (см. рекомендацию 7 SSR2: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления) и в системе управления информационной безопасностью (ISMS) (см. рекомендацию 6 SSR2: Соблюдать требования к соответствующим системам управления информационной безопасностью и сертификатам безопасности).

Эту рекомендацию можно будет считать выполненной, когда процессы управления рисками корпорации ICANN будут в достаточной степени задокументированы в соответствии с международными стандартами (например, ISO 31000) и корпорация организует цикл регулярных аудиторских проверок этой программы, предусматривающих публикацию кратких аудиторских заключений.

Эту рекомендацию можно будет считать действенной, если у корпорации ICANN будет мощная и четко задокументированная программа управления рисками.

Рекомендация SSR2 № 5: Соблюдать требования к соответствующим системам управления информационной безопасностью и сертификатам безопасности

5.1. Корпорация ICANN должна внедрить ISMS и пройти сторонний аудит и сертификацию выполнения своих операционных обязанностей в соответствии с отраслевыми стандартами безопасности (например, ITIL, семейство ISO 27000, SSAE-18). План должен включать дорожную карту и контрольные даты получения сертификатов, а также отмечать области, которые станут целью постоянного улучшения.

5.2. На основе ISMS корпорации ICANN следует составить план сертификации и установить требования к обучению должностных лиц корпорации, отслеживать процент выполнения работ, обосновать свой выбор и документально отразить, как сертификаты соответствуют стратегии безопасности и управления рисками корпорации ICANN.

[30] Международная организация по стандартизации, *ISO 31000 «Управление рисками»*: https://www.iso.org/iso-31000-risk-management.html.

5,3. Корпорация ICANN должна требовать от внешних сторон, предоставляющих услуги корпорации ICANN, соблюдения соответствующих стандартов безопасности и документирования их комплексных проверок в отношении поставщиков товаров и услуг.

5.4. Корпорация ICANN должна предоставлять сообществу и широкой общественности ясные отчеты, демонстрирующие деятельность и достижения корпорации ICANN в сфере безопасности. Эти отчеты были бы наиболее полезными, если бы они содержали информацию, описывающую, как корпорация ICANN следует передовым практикам и зрелым, постоянно совершенствующимся процессам управления рисками, безопасностью и уязвимостями.

Эту рекомендацию можно будет считать выполненной, когда у корпорации ICANN будет ISMS, соответствующая принятым стандартам (например, ITIL, семейство ISO 27000, SSAE-18), при условии проведения регулярных аудиторских проверок, которые подтверждают правильность соответствующих процедур управления безопасностью.

Эту рекомендацию можно будет считать действенной, если у корпорации ICANN будет система управления информационной безопасностью, которая тщательно задокументирована и адекватно устраняет текущие угрозы безопасности, а также предлагает планы по устранению потенциальных будущих угроз безопасности.

Рекомендация SSR2 № 6: Раскрытие уязвимостей SSR и транспарентность

Группа по анализу SSR2 рекомендует корпорации ICANN улучшить свои внутренние процессы для поддержки управления и отчетности по уязвимостям, связанным с SSR, посредством следующих действий:

6.1. Корпорация ICANN должна активно продвигать добровольное принятие передовых методов и целей SSR для раскрытия информации об уязвимостях сторонами, связанными договорными отношениями. Если добровольных мер окажется недостаточно для внедрения таких передовых практик и целей, корпорация ICANN должна реализовать передовые практики и цели в контрактах, соглашениях и MoU.

6.2. Корпорация ICANN должна внедрить слаженный процесс раскрытия информации об уязвимостях. Информация о проблемах, связанных с SSR, таких как нарушения обязательств сторонами, связанными договорными обязательствами, и в случае выявления и доведения до сведения корпорации ICANN информации о критических уязвимостях, должна незамедлительно раскрываться и доводиться до сведения соответствующих доверенных сторон (например, тех, кто пострадал или должен исправить данную проблему). Корпорация ICANN должна регулярно сообщать об уязвимостях (не реже одного раза в год), включая анонимные показатели и использование ответственного раскрытия информации.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN будет содействовать добровольному внедрению сторонами, связанными договорными

обязательствами, передовых методов раскрытия уязвимостей в области SSR и организует подготовку соответствующих отчетов о раскрытии уязвимостей.

Эти рекомендации можно будет считать действенными, если корпорация ICANN и стороны, связанные договорными обязательствами, внедрят передовые методы и цели в области SSR для раскрытия информации об уязвимостях.

4. Управление непрерывностью бизнеса и планирование аварийного восстановления

Учитывая важность всего спектра функций корпорации ICANN от DNS до реестров IANA (включая управление и обслуживание критически важных реестров, таких как корневая зона, IP-адреса и номера AS, а также реестры протоколов), корпорация ICANN должна заниматься тщательным планированием, выполнением и документированием управления непрерывностью бизнеса, а также планированием аварийного восстановления. Исходя из первостепенной важности этой роли, группа по анализу SSR2 считает, что у корпорации ICANN должны быть более надежные и лучше организованные программы BC и DR. ICANN выиграет от применения передовой отраслевой практики, в частности, от внедрения применимых международных стандартов (например, ISO/IEC 27001, NIST 800-53) и подготовки документации об их соблюдении. После принятия таких мер следует организовать независимые аудиторские проверки для подтверждения адекватности процедур.

Команда изучила доступную документацию на тему BC и DR. Самая свежая документация была датирована 2017 годом.[31] Согласно определениям ISO 22301 и 22730, передовая практика требует ежегодного пересмотра этих процедур и политики. Учитывая огромную важность DNS, необходимы независимые проверки, чтобы гарантировать актуальность и соответствие планов BC и DR передовой практике. В целом, группа по анализу SSR2 и персонал корпорации ICANN не смогли найти и представить достаточно подробную документацию, которая позволила бы надлежащим образом оценить реализацию корпорацией ICANN своих планов BC и DR. У корпорации ICANN имеется простор для серьезного улучшения работы над BC и DR для своих основных функций.[32]

Соблюдение общепринятых международных стандартов, подтвержденное независимыми сторонними проверками, имеет решающее значение для любой организации, которая управляет критически важной инфраструктурой интернета, даже если такое соблюдение не требуется по закону. Независимые эксперты способствовали бы транспарентности и легитимности планов и процедур BC и DR корпорации ICANN за счет проведения открытого конкурса среди аудиторов и последующей публикации итоговых заключений (если

[31] Вики-страница SSR2, документы и проекты группы по анализу, «Вопросы и ответы SSR2», дата не указана, 2: https://community.icann.org/pages/viewpage.action?pageId=64076120. Примечание: По информации, полученной от персонала ICANN: «Эти документы конфиденциальные и не публикуются из соображений безопасности.Существует план аварийного восстановления систем, план обеспечения бесперебойного выполнения функций IANA и более широкий план обеспечения непрерывности бизнеса, который разрабатывается для всей корпорации ICANN и будет представлен в 2019 году».

[32] Группе известно о взаимосвязи и взаимозависимости между ISMS, BC, DR и управлением рисками в соответствии с ISO. Тем не менее, группа сочла целесообразным предоставить подробную информацию о выявленных потребностях, выполнении рекомендаций и необходимых шагах.

необходимо, после цензурирования). В частности, ISO 31000 «Управление рисками», семейство ISO/IEC 27000 «Системы управления информационной безопасностью» и ISO 22301 «Управление непрерывностью бизнеса» принесли бы пользу в качестве руководства и, что более важно, целевых стандартов для независимых аудиторских организаций.[33] Хотя ICANN уникальна по своей организационной структуре и миссии, стандарты ISO гибки и применимы к ней, особенно в том, что касается корпорации ICANN и функций IANA. Кроме того, группа по анализу считает целесообразным применение стандартов NIST при условии, что корпорация ICANN тщательно задокументирует этот процесс и организует его независимый аудит авторитетной третьей стороной.[34]

Оценка соответствующих процессов и процедур BC и DR — это работа, в основе которой лежит более широкая деятельность по оценке рисков, описанная выше в разделе D.3. Управление рисками и безопасностью. ICANN поддерживает систему, критически важную для функционирования интернета, и поэтому она на уровень выше обычных требований к BC и DR. Возможность нарушения процедур, относящихся ключу для подписания ключей (KSK), особенно во время кризиса, может стать серьезной проблемой, и этого нельзя допустить.Глобальные потрясения 2020 года, от пандемии COVID-19 до серьезных общественных беспорядков, демонстрируют, что двух объектов в одной стране (в данном случае в США) недостаточно, и это привело к неожиданно высокому уровню риска для функций BC и DR в корпорации ICANN. Запреты на поездки в равной степени влияют на разные объекты в США. Кроме того, бурные события одновременно происходили в большинстве крупных городов страны. Более того, хотя это крайне маловероятно, оба объекта могут быть затронуты другими неблагоприятными событиями, такими как землетрясения, пожары или другие стихийные бедствия. Виды рисков, способных повлиять на деятельность корпорации ICANN, будут меняться, и корпорация ICANN обязана реагировать на это должным образом посредством регулярной и документируемой оценки планов BC и DR, включая надлежащее и своевременное составление и выполнение планов там, где необходимы изменения.

Рекомендация SSR2 № 7: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления

7.1. Корпорация ICANN должна разработать план обеспечения бесперебойной деятельности для всех систем, находящихся в собственности или в ведении корпорации ICANN, на основе стандарта ISO 22301 «Менеджмент непрерывности бизнеса», определив приемлемые сроки для BC и DR.[35]

---

[33] Стандарты и серии стандартов Международной организации по стандартизации *ISO 31000, ISO/IEC 27000:2018 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Обзор и терминология»* и *ISO 22301:2019 «Безопасность и отказоустойчивость — Системы управления непрерывностью бизнеса — Требования».*

[34] Министерство торговли США, Национальный институт стандартов и технологий.*Специальное издание NIST (SP) 800-30 ред. 1, «Руководство по оценке рисков»*.Гейтерсберг, штат Мэриленд: Министерство торговли США, 2012 год. https://doi.org/10.6028/NIST.SP.800-30r1 и Министерство торговли США, Национальный институт стандартов и технологий, Центр ресурсов по компьютерной безопасности. *SP 800-53 ред. 5, «Средства контроля безопасности и конфиденциальности для информационных систем и организаций»*.Гейтерсберг, штат Мэриленд: Министерство торговли США, 2020 год. https://doi.org/10.6028/NIST.SP.800-53r5.

[35] ISO 22301:2019

7.2. Корпорация ICANN должна обеспечить, чтобы план DR для операций по открытым техническим идентификаторам (PTI) (т. е. по функциям IANA) охватывал все уместные системы, способствующие безопасности и стабильности DNS, а также управление корневой зоной и соответствовал стандарту ISO 27031.[36] Корпорация ICANN должна разработать этот план в тесном сотрудничестве с Консультативным комитетом системы корневых серверов (RSSAC) и операторами корневых серверов (RSO).

7.3. Корпорация ICANN также должна разработать план DR для всех систем, находящихся в собственности или в ведении корпорации ICANN, опять же с соблюдением стандарта ISO 27031.

7.4. Корпорация ICANN должна создать новый сайт аварийного восстановления для всех систем, находящихся в собственности или в ведении корпорации ICANN, с целью замены сайтов в Лос-Анджелесе или Калпепере или добавления постоянного третьего сайта. Корпорации ICANN следует разместить этот сайт за пределами Североамериканского региона и любых территорий Соединенных Штатов. Если корпорация ICANN решит заменить один из существующих сайтов, любой сайт, который заменяет корпорация ICANN, не следует закрывать до тех пор, пока корпорация не убедится, что новый сайт полностью функционирует и способен обрабатывать аварийное восстановление этих систем для корпорации ICANN.

7.5. Корпорация ICANN должна опубликовать сводку своих общих планов и процедур BC и DR. Это повысит транспарентность и надежность, помимо решения стратегических целей и задач корпорации ICANN. Для проверки соответствия этим планам BC и DR корпорации ICANN следует привлечь независимого аудитора.

Эту рекомендацию можно будет считать выполненной, когда планы и процессы корпорации ICANN по BC и DR будут тщательно задокументированы в соответствии с принятыми отраслевыми стандартами, включая регулярные проверки соблюдения этих процессов, и когда будет введен в эксплуатацию объект, находящийся за пределами США и Северной Америки.

Эту рекомендацию можно будет считать действенной, когда корпорация ICANN продемонстрирует свою способность справляться с инцидентами, влияющими на всю территорию США или Северной Америки.

[36] Стандарты и серии стандартов Международной организации по стандартизации *ISO 27031, ISO/IEC 27031:2011 «Информационные технологии — Методы обеспечения безопасности — Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».*

E. Контракты, соблюдение требований и транспарентность в отношении неправильного использования DNS

С момента создания ICANN в ее миссию входила «*координация разработки и реализации политики, формируемой по принципу «снизу-вверх» на основе консенсуса с участием многих заинтересованных сторон и направленной на обеспечение стабильной и безопасной работы систем уникальных имен интернета*».[37] Группа по анализу SSR2 пришла к выводу, что, несмотря на вышеупомянутое обязательство, текущая система, координируемая ICANN, не защищает в достаточной степени от неправильного использования DNS и сопутствующего вреда. Группы внутри и за пределами сообщества ICANN уже много лет отмечают этот пробел.[38] Некоторые из наиболее острых замечаний на эту тему поступили через Правительственный консультативный комитет (GAC) от представителей правительств, которые уже более десяти лет утверждают, что не считают процессы и процедуры ICANN достаточными для удовлетворения интересов общественной безопасности.[39]

Неправильное использование DNS в мошеннических или преступных целях имело место и до создания корпорации ICANN.[40] Характер угроз, которые раньше ограничивались спамом, фишингом и мошенничеством, расширился за счет более сложных атак, например вредоносного ПО, программ-вымогателей и компрометации рабочей электронной почты (BEC), нацеленных на коммерческие предприятия, органы государственной власти и интернет вещей (IoT).[41] В число злоумышленников теперь входят лица, финансируемые государствами, и коммерческие субъекты, которые разрабатывают промышленные платформы для поддержки злоупотреблений. Пандемия COVID-19 и соответствующие карантины расширили возможности атак со стороны беспринципных преступников.[42]

Как отмечено далее в разделе E.1. Нереализованные меры защиты для Программы New gTLD, в тот момент неправильное использование DNS было основной проблемой для

[37] Устав ICANN, раздел 1.1(a): https://www.icann.org/resources/pages/governance/bylaws-en/#article1.

[38] Примеры: «Открытое письмо сообществу ICANN от Группы заинтересованных сторон регистратур», 19 августа 2020 года: https://docs.wixstatic.com/ugd/ec8e4c_00d2dbac27b24330b8342686e9c2e53a.pdf, а также письмо Группы интересов коммерческих пользователей ICANN, адресованное Правлению ICANN, президенту и генеральному директору ICANN Йорану Марби (Göran Marby), председателю Совета GNSO Киту Дразеку (Keith Drazek) и сообществу ICANN, 28 октября 2019 года: https://www.bizconst.org/assets/docs/positions-statements/2019/2019_10October_28%20BC%20Statement%20on%20DNS%20Abuse.pdf.

[39] Правительственный консультативный комитет ICANN, «Заявление GAC о неправильном использовании DNS», 18 сентября 2019 года, 1: https://gac.icann.org/file-asset/public/gac-statement-dns-abuse-final-18sep19.pdf.

[40] Подробнее об исторических тенденциях в этой области см. Приложение F: Исследовательские данные из отчетов о тенденциях неправильного использования DNS.

[41] Консультативный комитет по безопасности и стабильности ICANN, «SAC105: DNS и Интернет вещей: возможности, риски и проблемы», 28 мая 2019 года: https://www.icann.org/en/system/files/files/sac-105-en.pdf.

[42] Интерпол, «Глобальная картина киберугроз, связанных с COVID-19», апрель 2020 года: https://www.interpol.int/en/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf.

всех заинтересованных сторон, и у корпорации ICANN имелся ряд возможностей для разработки политики, призванной обеспечить стабильную и безопасную работу системы уникальных имен интернета во время этого расширения глобального пространства имен. Корпорация ICANN также могла стать лидером всех сообществ, занимающихся вопросами DNS и безопасности, в деле разработки общего набора терминов, определений и данных, которые облегчили бы общение и сотрудничество, как указано в разделе E.2. Проблемы: определения и данные.

Эти возможности у корпорации ICANN все еще сохраняются. Рекомендации этого раздела содержат конкретные предложения корпорации ICANN о том, где и как можно улучшить выполнение своей собственной миссии и стать более сильным лидером в сообществах специалистов по DNS и безопасности.

1. Нереализованные меры защиты для Программы New gTLD

Неправильное использование DNS было ключевой проблемой при запуске программы New gTLD в 2010 году. Правоохранительные органы, правительства, сообщества специалистов по безопасности, а также коммерческие и пользовательские группы интересов выступали за введение договорных обязательств по снижению угроз злонамеренного поведения как в базовом Соглашении об администрировании нового gTLD, так и в Соглашении об аккредитации регистраторов (RAA) 2013 года. В рамках этих дискуссий сообщество ICANN подготовило в 2009 году пояснительную записку с предложением предусмотреть в Программе New gTLD меры по снижению угроз злонамеренного поведения.[43] Эта пояснительная записка содержала рекомендации по проверке операторов регистратур на благонадежность, определению контактов и процедур для борьбы со злоупотреблениями на уровне регистратуры, а также централизованному доступу к файлам зон. К сожалению, возникло расхождение между мерами, изложенными в этом меморандуме, и результатом закрытых переговоров между корпорацией ICANN и регистратурами. Более поздние попытки улучшить методы обеспечения безопасности с помощью поправок к соглашениям подверглись критике из-за отсутствия транспарентности и недостаточного участия сообщества в этом процессе.[44]

В 2013 году группа по анализу конкуренции, потребительского доверия и потребительского выбора (CCT) ICANN оценила эффективность этих мер защиты, предназначенных именно для снижения масштаба злонамеренных и преступных действий в новых gTLD. Группа CCT заказала независимое исследование (далее — отчет SADAG), в котором на основе общедоступных источников данных было продемонстрировано, что масштабы злоупотреблений в новых gTLD выше, чем в

[43] ICANN, «Снижение угроз злонамеренного поведения», пояснительная записка на тему новых gTLD, 3 октября 2009 года: https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf.

[44] ICANN, Группа интересов коммерческих пользователей GNSO, «Комментарий относительно предлагаемых поправок к базовому Соглашению об администрировании нового gTLD», документ Группы интересов коммерческих пользователей, 3-я редакция, 20 июля 2016 года: https://www.bizconst.org/assets/docs/positions-statements/2016/2016_07july_20%20bc%20comment%20on%20proposed%20gtld%20base%20registry%20agreement%20final.pdf.

исторических TLD, а это подразумевает неэффективность мер защиты.[45] В итоговом отчете по CCT был сделан следующий вывод:

«Хотя злоупотребления не совершаются повсеместно, во всех новых gTLD, во многих они широко распространены. Еще большую тревогу вызывает то, что в настоящее время у сообщества мало средств, позволяющих пресечь деятельность регистратур и регистраторов новых gTLD с высоким уровнем злоупотреблений. Это, в свою очередь, создает стимулы для одностороннего блокирования сетевыми операторами всего трафика от конкретных TLD или регистраторов, что противоречит стремлению сообщества добиться универсального принятия всех новых gTLD.

Неспособность предотвратить распространение в новых gTLD определенных видов неправомерных действий, ранее выявленных сообществом, имеет большое значение. Группа по анализу CCT признает инфраструктурную роль, которую играют доменные имена в обеспечении возможности совершения неправомерных действий, негативно влияющих на безопасность, стабильность и отказоустойчивость DNS, подрывающих потребительское доверие и, в конечном итоге, оказывающих воздействие на конечных пользователей по всему миру. Соответственно, это крайне актуальный вопрос, который обязательно нужно решить до какого-либо дальнейшего расширения DNS, и группа по анализу дает несколько рекомендаций по устранению имеющихся недочетов и повышению безопасности DNS».[46]

Анализ CCT и соответствующий отчет SADAG, а также отчеты других сторонних организаций тоже показали, что после запуска Программы New gTLD некоторые регистратуры и регистраторы оперативно внедрили практику быстрого и значительного увеличения количества зарегистрированных доменов, например массовую регистрацию, многие из которых используются для злоупотреблений и преступной деятельности.[47] Spamhaus (среди прочих) также публикует данные о TLD и регистраторах, которые, по их оценке, наиболее часто используются для совершения злоупотреблений, и некоторые организации появляются в этих списках год за годом.[48] Alpnames, отмеченный в отчете SADAG как один из регистраторов, причастных к наиболее вопиющим нарушениям в

[45]Корчиньски, Мацей, Мартен Вуллинк, Самане Таджализадехуб, Джоване С.М. Моура и Кристиан Хессельман, итоговый отчет «Статистический анализ неправильного использования DNS в gTLD», SIDN Labs и Делфтский технический университет, август 2017 года, источник проверен 3 августа 2018 года: https://www.icann.org/public-comments/sadag-final-2017-08-09-en.

[46] Группа по анализу конкуренции, потребительского доверия и потребительского выбора, «Конкуренция, потребительское доверие и потребительский выбор: итоговый отчет», ICANN, 8 сентября 2018 года: https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf; Пискателло, Дэйв, «Использование доменных имен в качестве оружия: как массовая регистрация способствует глобальным спамерским кампаниям», Spamhaus, 21 марта 2020 года: https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns.

[47] Тот же источник; Дэйв Писцителло, «Использование доменных имен в качестве оружия: как массовая регистрация способствует глобальным спамерским кампаниям», Spamhaus, 21 марта 2020 года: https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns.

[48] Spamhaus, «TLD с наибольшим количеством злоупотреблений в мире», источник проверен 5 декабря 2020 года: https://www.spamhaus.org/statistics/tlds/; Spamhaus, «Регистраторы доменов с наибольшим количеством злоупотреблений в мире», источник проверен 5 декабря 2020 года: https://www.spamhaus.org/statistics/registrars/.Примечание: вспомогательные материалы на страницах Spamhaus позволяют понять, как принимается решение о том, что домены и регистраторы «плохие».

контексте неправильного использования DNS, предлагал дешевую массовую регистрацию и «*выступал в качестве спонсирующего регистратора для 53,97% (59 044) доменов в новых gTLD, внесенных в черный список Spamhaus*».[49] Отдел по контролю исполнения договорных обязательств ICANN не смог в достаточной мере устранить это продолжающееся систематическое нарушение даже после неоднократных призывов со стороны многих организаций обратить на это внимание.[50] Отдел по контролю исполнения договорных обязательств ICANN не лишал Alpnames аккредитации до тех пор, пока ему не стало известно о том, что Alpnames прекратил свою деятельность.[51] Мы надеемся, что корпорация ICANN и отрасль DNS смогут продемонстрировать измеримый прогресс в предотвращении и смягчении последствий неправильного использования DNS. В противном случае правительства, скорее всего, придут к выводу, что модель отраслевого самоуправления ICANN больше не соответствует своему назначению.

Как отмечается в отчете о проверке WHOIS2/RDS, отдел ICANN по контролю исполнения договорных обязательств мог бы использовать более активный подход, в соответствии с которым «*при обнаружении потенциальных системных проблем, получении жалоб на недостоверность данных и результатов исследования точности данных RDS или отчетов DAAR, сотрудники отдела выполняли бы исследование и анализ и принимали бы меры по устранению недостоверности регистрационных данных*».[52]

Рекомендация SSR2 № 8: Обеспечение и демонстрация представления общественных интересов в переговорах со сторонами, связанными договорными обязательствами

8.1. Корпорация ICANN должна создать группу по ведению переговоров, в которую входят эксперты по вопросам злоупотреблений и безопасности, не аффилированные со сторонами, связанными договорными обязательствами, и не оплачиваемые ими, для представления интересов организаций, не связанных договорными обязательствами, и работы вместе с корпорацией ICANN над

[49] Отчет SADAG, 19: https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf.

[50] Письмо компаний Adobe Systems, DomainTools, eBay, Facebook, Microsoft и Time Warner (также известных как Независимая рабочая группа по вопросам соблюдения обязательств) Джейми Хедлунду, старшему вице-президенту, отдел ICANN по контролю исполнения обязательств и обеспечению мер защиты потребителей, и управляющему директору офиса в Вашингтоне, 27 февраля 2018 года: https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf.

[51] Письмо Джейми Хедлунда, старшего вице-президента, отдел ICANN по контролю исполнения обязательств и обеспечению мер защиты потребителей, и управляющего директора офиса в Вашингтоне Иэну Роучу (Iain Roache), Alpnames Limited, «ТЕМА: УВЕДОМЛЕНИЕ О ПРЕКРАЩЕНИИ ДЕЙСТВИЯ СОГЛАШЕНИЯ ОБ АККРЕДИТАЦИИ РЕГИСТРАТОРА», источник проверен 15 марта 2019 года: https://www.icann.org/uploads/compliance_notice/attachment/1113/hedlund-to-roache-15mar19.pdf.

[52] Группа по анализу RDS-WHOIS, «Итоговый отчет о проверке службы каталогов регистрационных данных RDS-WHOIS2», 3 сентября 2019 года: https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf, 46. Примечание: см. рекомендацию R4.1: «*Правлению ICANN следует принять меры, чтобы отделу ICANN по контролю исполнения договорных обязательств было поручено активно отслеживать и обеспечивать соблюдение регистраторами обязательств в отношении достоверности данных RDS (WHOIS), используя сведения из поступающих жалоб на неточность информации и результаты исследований точности данных RDS для выявления и решения системных проблем. Следует применять подход, основанный на определении риска, чтобы оценить и понять проблемы с точностью данных, а затем принять подходящие меры для устранения этих проблем».*

добросовестным пересмотром условий договоров в условиях публичной транспарентности и с целью улучшения SSR системы доменных имен для конечных пользователей, коммерческих предприятий и государственных органов.

Эту рекомендацию можно будет считать выполненной, если корпорация ICANN привлечет к этим переговорам специалистов по злоупотреблениям и безопасности, а управление системой доменных имен будет отвечать интересами общественной безопасности и потребителей, а не только интересам участников доменной отрасли.

Эту рекомендацию можно будет считать действенной, когда более широкий и сбалансированный круг заинтересованных сторон сможет вносить прямой вклад в обсуждение условий соглашений со сторонами, связанными договорными обязательствами.

Рекомендация SSR2 № 9: Мониторинг и обеспечение соблюдения обязательств

9.1. Правлению ICANN следует поручить отделу по контролю исполнения договорных обязательств контролировать и строго обеспечивать соблюдение сторонами по контракту текущих и будущих обязательств по SSR и связанных со злоупотреблениями обязательств в контрактах, базовых соглашениях, временных спецификациях и политиках сообщества.

9.2. Корпорация ICANN должна активно отслеживать и обеспечивать выполнение договорных обязательств регистратурами и регистраторами для повышения точности регистрационных данных. Этот мониторинг и обеспечение должны включать проверку адресных полей и проведение периодических аудитов точности регистрационных данных. Корпорации ICANN следует сосредоточить свои правоприменительные усилия на тех регистраторах и регистратурах, в отношении которых ежегодно поступает более 50 жалоб или сообщений в отношении предоставления ими неточных данных в корпорацию ICANN.

9.3. Корпорация ICANN должна проводить внешний аудит деятельности по обеспечению соблюдения обязательств не реже одного раза в год и публиковать отчеты об аудите и ответ корпорации ICANN на рекомендации аудита, включая планы выполнения.

9.4. Корпорация ICANN должна дать отделу по контролю исполнения обязательств поручение регулярно публиковать отчеты с перечислением отсутствующих инструментов, которые помогли бы поддерживать корпорацию ICANN в целом для эффективного использования договорных рычагов в целях устранения угроз безопасности DNS, включая меры, которые потребуют внесения изменений в контракты.

Эту рекомендацию можно будет считать выполненной, когда будут регулярно проводиться аудиторские проверки и публиковаться их сводные результаты.

Эту рекомендацию можно будет считать действенной, если корпорация ICANN успешно проведет аудит и сообщит его результаты сообществу.

Эта рекомендация требует действий со стороны Правления ICANN и корпорации ICANN. Возможно, Правлению потребуется обновить свою позицию и инструкции после завершения ускоренного процесса формирования политики (EPDP) (см. рекомендацию SSR2 № 15: Запустить EPDP для улучшения безопасности на основе фактов).

2. Проблемы: Определения и доступ к данным

Группа по анализу SSR2 выявила две категории постоянных проблем, требующих решения: одна из них связана с определениями и кругом злоупотреблений, входящих в компетенцию отдела по контролю исполнения договорных обязательств ICANN, а вторая с доступом к данным, которые могут способствовать обнаружению, смягчению, предотвращению и реагированию на злоупотребления. Рекомендации SSR2 № 11–14 направлены на повышение транспарентности и подотчетности в обеих областях.

A. Определение злоупотреблений

В ходе диалога с группой по анализу SSR2 в апреле 2018 года отдел по контролю исполнения договорных обязательств ICANN заявил, что действующие договора с регистратурами и регистраторами не позволяют корпорации ICANN требовать, чтобы регистратуры приостанавливали или удаляли доменные имена, потенциально используемые в злонамеренных целях. Таким образом, эти договора неэффективны в плане преследования лиц, вовлеченных в систематическое неправильное использование DNS.[53] Об этом также было публично заявлено в письме отдела по контролю исполнения договорных обязательств ICANN, адресованном Независимой рабочей группе по вопросам соблюдения обязательств.[54]

Год спустя, в апреле 2019 года, отдел по контролю исполнения договорных обязательств ICANN сообщил группе по анализу SSR2, что отсутствие договорного запрета на «систематическое неправильное использование DNS» не позволяет отделу по контролю исполнения договорных обязательств ICANN эффективно бороться с этим явлением до тех пор, пока сообщество не выработает согласованную политику, определяющую и запрещающую его.[55] Кроме того, Правление ICANN недавно объявило, что отложит дальнейшие меры по выполнению рекомендаций № 14 и 15 по итогам проверки CCT, в которых предлагаются поправки к существующим соглашениям в целях предупреждения неправильного использования DNS. Правление подчеркнуло, что эта задержка возникла, потому что «*в сообществе еще не завершены дискуссии, направленные на достижение единого для всего сообщества трактования неправильного использования DNS и*

[53] Материалы брифингов: Обсуждение с отделом по контролю исполнения договорных обязательств ICANN — завершено 14 мая 2019 года, ответ ICANN на вопросы SSR2 по состоянию на 26 апреля 2019 года: https://community.icann.org/display/SSR/Briefing+Materials.

[54] Письмо Джейми Хедлунда, старшего вице-президента, отдел ICANN по контролю исполнения обязательств и обеспечению мер защиты потребителей, и управляющего директора офиса в Вашингтоне Независимой рабочей группе по вопросам соблюдения обязательств, «ТЕМА: Письмо Независимой рабочей группы по вопросам соблюдения обязательств от 27 февраля 2018 года», 4 апреля 2018 года: https://www.icann.org/en/system/files/correspondence/hedlund-to-vayra-04apr18-en.pdf.См. также сноску № 44 по вопросу:Письмо Независимой рабочей группы по вопросам соблюдения обязательств от 27 февраля 2018 года.

[55] Материалы брифингов: https://community.icann.org/display/SSR/Briefing+Materials, 4.Примечание: см. ответ на вопрос 6.

связанных с этим понятий».[56] Группа по анализу SSR2 отмечает, что неструктурированный и неограниченный характер этих дискуссий усложняет поиск решения, а корпорация ICANN и стороны, связанные договорными обязательствами, заинтересованы в том, чтобы отложить решение этой проблемы на неопределенный срок. Мы рекомендуем трехкомпонентный подход к этой проблеме, в том числе временную спецификацию на короткий срок, создание CCWG с ограничением времени завершения ее работы на среднесрочный период и структурированный EPDP на долгосрочную перспективу.

Корпорация ICANN уже более десяти лет использует в своей деятельности описания и рабочие определения «неправильного использования DNS» и сопутствующих понятий, включая (среди прочего) концепции безопасности, стабильности и отказоустойчивости корпорации ICANN с 2009 по 2017 год,[57] консенсусные результаты работы сообщества ICANN в рамках Программы New gTLD и принятые впоследствии консенсусные решения по мерам защиты,[58] договорное обязательство в Спецификации 11b от 2013 года, где перечислены неправомерные действия,[59] и собственный проект ICANN Платформа отчетности о случаях злоупотребления DNS (DAAR).[60]

---

[56] Правление ICANN, «Утвержденные резолюции | Очередное заседание Правления ICANN, основная повестка дня, Остающиеся невыполненными рекомендации группы по анализу конкуренции, потребительского доверия и потребительского выбора (CCT-RT)», 22 октября 2020 года: https://www.icann.org/resources/board-material/resolutions-2020-10-22-en#2.a.

[57] Архив документов IS-SSR: https://www.icann.org/ssr-document-archive.

[58] ICANN, Рабочая группа GNSO по политике в сфере противодействия злоупотреблениям при регистрации, «Итоговый отчет Рабочей группы по политике в сфере противодействия злоупотреблениям при регистрации», 29 мая 2010 года: https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf, 3.Примечание: в указанном отчете злоупотреблению дано следующее определение — «*это действие, которое а) причиняет фактический или существенный вред, или служит материальным признаком вреда, и б) является незаконным или неправомерным, или по иным основаниям противоречит заявленным намерениям и легитимным целям, если цель использования была раскрыта»*. См. также Исследование деятельности и политики ICANN, «Меры защиты от неправильного использования DNS, предусмотренные в составе Программы New gTLD», июль 2016 года: https://newgtlds.icann.org/en/reviews/dns-abuse/safeguards-against-dns-abuse-18jul16-en.pdf, 3. Примечание: В этом отчете также используется проведенное группой RAPWG различие между злоупотреблениями при *регистрации* и *использовании* и отмечается, что злоупотребления при регистрации можно с большей определенностью отнести к сфере выработки политики ICANN и GNSO.Группа привела примеры злоупотреблений при регистрации: киберсквоттинг, неправомерное использование информации для опережающей регистрации, сайты для жалоб, вводящие в заблуждение и/или оскорбительные доменные имена, фальшивые уведомления о необходимости продления регистрации, видоизменение доменного имени, оплата за клик, переадресация трафика, фальсификация принадлежности, мошенничество с регистрацией в другом TLD, пробное использование доменных имен. RAPWG также перечислила следующие виды злоупотреблений: фишинг, спам, вредоносное ПО/ботнеты с командным центром управления, DDoS и Fast Flux.

[59] ICANN, «Базовое соглашение об администрировании домена верхнего уровня — обновлено 31 июля 2017 года», Спецификация 11 (3)(a) и Спецификация 11 (3)(b): https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf; ICANN, «Рекомендация, Спецификация 11 (3)(b) соглашения об администрировании нового gTLD», 8 июня 2017 года: https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en.

[60] См. вопрос «Какие виды угроз безопасности отслеживает DAAR?»Корпорация ICANN, часто-задаваемые вопросы по DAAR:https://www.icann.org/octo-ssr/daar-faqs/#security-threats. А именно: фишинг, вредоносное ПО, ботнеты с командным центром управления и спам.

Совет GNSO также попросил Рабочую группу по политике в сфере противодействия злоупотреблениям при регистрации (RAPWG) изучить вопросы, связанные с незаконным использованием доменных имен. В итоговом отчете говорится:

«*RAPWG признает, что киберпреступность является важной проблемой сообщества ICANN. Интернет-сообщество часто выражает ICANN свою озабоченность злонамеренным поведением и, в частности, масштабом использования криминальными элементами служб регистрации доменов и разрешения имен. Различные стороны — в том числе компании, потребители, правительства и правоохранительные органы— обращаются к ICANN и связанным с ней договорными обязательствами сторонам с просьбой обеспечить контроль над злонамеренным поведением и, в соответствующих случаях, предпринимать необходимые меры по обнаружению, блокированию и смягчению последствий такого поведения*».[61]

RAPWG рекомендовала организовать процесс с участием сообщества при ресурсной поддержке со стороны ICANN, чтобы разработать не имеющие обязательной силы передовые методы для содействия регистраторам и регистратурам в решении проблемы незаконного использования доменных имен. Десять лет спустя корпорация ICANN все еще не достигла существенного прогресса в решении этих вопросов. [62] (См. также рекомендацию SSR2 № 9: Мониторинг и обеспечение соблюдения обязательств.)

B. Доступ к данным

Вторая серьезная проблема связана с доступом к данным о доменных именах, используемым для проведения операций по обеспечению безопасности и исследований. Четыре типа данных, которым уделяется наибольшее внимание, — это регистрационные данные, облегчающие отслеживание злонамеренных действий до владельца и оператора соответствующего домена, данные файлов зон TLD (поступают через Централизованную службу файлов корневой зоны (CZDS)), способствующие исследованиям в области безопасности, данные сообщений о злоупотреблениях, необходимые ICANN для анализа неправильного использования DNS, и данные о соблюдении договорных обязательств, помогающие анализировать тенденции и оценивать операционные подходы к сокращению количества злоупотреблений.

i. Регистрационные данные

По крайней мере с 2003 года корпорация ICANN признает необходимость баланса между потребностью в обеспечении транспарентности и подотчетности регистрационных метаданных доменных имен, то есть контактных данных владельцев доменов, и действующими в разных странах мира законодательными требованиями, которые иногда запрещают или затрудняют обмен такими данными.[63] RAPWG пришла к выводу,

[61] Итоговый отчет RAPWG, 6: https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf.

[62] Письмо Клаудии Селли, председателя Группы интересов коммерческих пользователей ICANN, Мартену Боттерману, председателю Правления Интернет-корпорации по присвоению имен и номеров (ICANN), 9 декабря 2019 года, 1 и 3:https://www.icann.org/en/system/files/correspondence/selli-to-botterman-09dec19-en.pdf.

[63] ICANN, «Пересмотренная процедура ICANN по разрешению противоречий между политикой в отношении WHOIS и законами о защите конфиденциальной информации», 18 апреля 2017 года: https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law.

что базовая доступность службы каталогов регистрационных данных (RDS, ранее известной как WHOIS) неразрывно связана со злоупотреблениями при регистрации доменов и является ключевой проблемой в том, что касается злонамеренного использования доменных имен.[64] Также был сделан вывод, что не всегда есть возможность гарантированного доступа к данным RDS, их надежного и последовательного предоставления регистраторами, как этого следовало бы ожидать. Кроме того, пользователи иногда получают разные данные RDS в зависимости от места или способа их поиска. Это привело к двум рекомендациям RAPWG:

«GNSO следует предложить отделу по контролю исполнения договорных обязательств ICANN публиковать больше данных о доступности WHOIS не реже одного раза в год. Эти данные должны отражать а) число регистраторов, которые необоснованно ограничивают доступ к порту 43 своих серверов WHOIS, и б) результаты ежегодной проверки соблюдения всех договорных обязательств в части доступа к WHOIS».

и

«*GNSO следует определить, какие дополнительные исследования и процедуры могут потребоваться для обеспечения требуемой надежности, возможности осуществления в принудительном порядке и постоянства доступа к данным WHOIS*».[65]

В июне 2018 года, реагируя на новые трудности с доступом к регистрационным данным, связанные с GDPR, Консультативный комитет ICANN по безопасности и стабильности (SSAC) настоятельно рекомендовал Правлению ICANN внести поправки в соглашения, чтобы устранить постоянные проблемы с доступом к данным. Ни одна из этих рекомендаций пока не выполнена.[66] Согласно отчету о состоянии дел, который корпорация ICANN представила группе по анализу SSR2 (2 июля 2020 года), корпорация ICANN передала эти рекомендации SSAC101 GNSO для включения в рабочий план 2-й фазы EPDP в области доступа к регистрационным данным.[67] Ни одна из этих рекомендаций никогда не входила в рабочий план 2-й фазы EPDP, эти темы не обсуждались в рамках EPDP, и GNSO не занималась какой-либо соответствующей работой. SSAC предпринял и другие попытки, но без заметных последствий.[68] Некоторые

[64] Итоговый отчет RAPWG, 71-80: https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf.

[65] Тот же источник, 79–80.

[66] Консультативный комитет по безопасности и стабильности ICANN, «SAC101: Рекомендация SSAC относительно доступа к регистрационным данным доменных имен», рекомендация Комитета, 14 июня 2018 года: https://www.icann.org/en/system/files/files/sac-101-en.pdf. Примечание: SSAC опубликовал «версию 2» этого документа, в которой рекомендации Правлению ICANN по внесению поправок в соглашения для решения постоянных проблем с доступом к данным были существенно смягчены по сравнению с версией 1. https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf. См. стр. 4–5 полного текста рекомендаций SSAC101v2.

[67] Сообщение Дженнифер Брайс, отправленное группе по анализу SSR2 через лист рассылки, 2 июля 2020 года, Тема: Состояние дел с документами SAC097 и SAC102v2: https://mm.icann.org/pipermail/ssr2-review/2020-July/002280.html. См. стр. 2 вложения к этому сообщению.

[68] Письмо Консультативного комитета ICANN по безопасности и стабильности Рассу Вайнштейну, директору по предоставлению услуг регистратурам и взаимодействию с регистратурами и Джейми Хедлунду, старшему вице-президенту, отдел соблюдения договорных обязательств и обеспечения мер защиты

исследователи, занимающиеся вопросами безопасности, отметили, что Временная спецификация для регистрационных данных в gTLD теперь позволяет регистраторам доменов gTLD вымарывать из публикуемой в RDS информации все контактные данные домена, даже те, которые не подпадают под действие законов о конфиденциальности, таких как GDPR.[69]

Этот недавний EPDP представляет собой самую последнюю и самую широкую дискуссию о доступе к регистрационным данным.[70] Заявления о мнении меньшинства неизменно указывают на то, что рекомендации отчета не обеспечивают должного баланса между правами лиц, предоставляющих данные регистратурам и регистраторам, и общественными интересами по предотвращению вреда, вызванного злонамеренными действиями с использованием DNS.[71] Существенное несогласие с итоговым отчетом означает, что в ходе этого процесса не удалось достичь консенсуса сообщества в отношении политики доступа к данным. Отмечая, что составной частью этой проблемы является «*нынешняя фрагментированная система раскрытия данных*» в сочетании с относительно неопределенной правовой базой, генеральный директор ICANN недавно попросил Комиссию ЕС обеспечить правовую ясность положений GDPR об обязанностях контролера данных.[72]

В состав RAA 2013 года было включено требование о перекрестной проверке полей адреса в составе регистрационных данных домена.[73] Перекрестная проверка полей —

потребителей, «Тема: SSAC2019-02: Отчетность о запросах к службам регистрационных данных», 3 мая 2019 года: https://www.icann.org/en/system/files/files/ssac2019-02-03may19-en.pdf. Примечание: SSAC опубликовал документ SSAC 2019-2, в котором рекомендовал корпорации ICANN выпустить руководство для всех операторов регистратур, разъясняющее цели, ожидания и договорные обязательства в области отчетов о запросах к порту 43 и RDAP. Нет никаких свидетельств того, что это произошло.

[69] Аарон, Грег, Лайман Чапин, Дэвид Писцителло и д-р Колин Струтт, «Картина фишинга в 2020 году: исследование масштабов и распространения фишинга», Interisle Consulting Group, LLC, 13 октября 2020 года: http://www.interisle.net/PhishingLandscape2020.pdf.

[70] Организация поддержки доменов общего пользования ICANN, «Итоговый отчет по фазе 2 ускоренного процесса формирования политики в области Временной спецификации для регистрационных данных в gTLD», 31 июля 2020 года: https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.

[71] Тот же источник, Приложение F. Заявление меньшинства, стр. 151–154. Содержит заявления о мнении меньшинства, которые поступили от следующих групп: Консультативный комитет At-Large (ALAC), Группа интересов коммерческих пользователей (BC)/Группа интересов по вопросам интеллектуальной собственности (IPC), Правительственный консультативный комитет (GAC), Группа некоммерческих заинтересованных сторон (NCSG), Группа заинтересованных сторон-регистраторов (RrSG), Группа заинтересованных сторон-регистратур (RySG), Консультативный комитет по безопасности и стабильности (SSAC).

[72] Письмо Йорана Марби, президента и генерального директора Интернет-корпорации по присвоению имен и номеров (ICANN), г-ну Роберто Виоле, генеральному директору, Генеральный директорат коммуникационных сетей, контента и технологий Европейской комиссии, г-же Монике Париат, генеральному директору, Генеральный директорат по миграции и внутренним делам Европейской комиссии и г-же Салле Саастамойнен, исполняющей обязанности генерального директора, Генеральный директорат по вопросам юстиции и потребителей Европейской комиссии, 2 октября 2020 года: https://www.icann.org/en/system/files/correspondence/marby-to-viola-et-al-02oct20-en.pdf.

[73] ICANN, «Соглашение об аккредитации регистраторов в редакции 2013 года», источник проверен 8 декабря 2020 года: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. Примечание: См. раздел 1(e) спецификации программы проверки достоверности данных WHOIS: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy.

широко распространенная автоматизированная проверка достоверности данных (например, что указанный дом действительно существует на указанной улице, которая существует в указанном городе и области, и что почтовый индекс тоже указан правильно). На дату подготовки этого отчета корпорация ICANN не ввела в действие требование о такой проверке. Что касается регистрации с сохранением конфиденциальности и через доверенных лиц, Совет GNSO корпорации ICANN единогласно поддержал политику аккредитации поставщиков услуг сохранения конфиденциальности и регистрации через доверенных лиц, которая могла бы предусматривать усовершенствование методов работы, в том числе ответы правоохранительным органам и владельцам интеллектуальной собственности.[74] Правление ICANN одобрило эту политику в августе 2016 года.[75] По состоянию на октябрь 2020 года ICANN не выполнила эти требования, а сайт, посвященный этой рабочей задаче, не обновлялся с марта 2018 года.[76]

ii. Централизованная служба файлов корневой зоны

Доступ к файлам зон всегда был важным аспектом операций и исследований, связанных с безопасностью. В рамках программы создания новых gTLD сообщество решило, что регистратуры новых gTLD должны брать на себя обязательство «*после технического делегирования gTLD предоставлять данные корневой зоны одобренным отправителям запросов (например, сотрудникам правоохранительных органов, юристам по интеллектуальной собственности, исследователям)*».[77] Однако полноценный доступ к этим данным остается проблематичным, например в том, что касается запроса и продления доступа, а также фактического получения файлов.[78] В настоящее время регистратуры не предоставляют доступ должным образом, периодически аннулируют доступ и применяют длительные процедуры его продления.[79] Эти данные регулярно используются для изучения злоупотреблений в DNS.[80] SSAC подготовил консультативное

[74] ICANN, «Услуги сохранения конфиденциальности и регистрации через доверенных лиц», источник проверен 8 декабря 2020 года: https://whois.icann.org/en/privacy-and-proxy-services.Примечание: см. раздел 2 «Процесс принятия рекомендаций по политике».

[75] Тот же источник.

[76] Рабочая группа по вопросам проверки достоверности данных WHOIS регистраторов, «Документы», последняя редакция от 21 марта 2018 года: https://community.icann.org/display/AFAV/Documents.

[77] ICANN, «Централизованная служба файлов корневой зоны (CZDS)», источник проверен 7 декабря 2020 года: https://czds.icann.org/home.

[78] Дэйв Писцителло, «Лишенные конкретики договорные положения по CZDS делают получение разрешений на доступ к данным зоны рискованным предприятием», блог The Security Skeptic, 13 августа 2019 года: https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html.

[79] Дэйв Писцителло, «Лишенные конкретики договорные положения по CZDS делают получение разрешений на доступ к данным зоны рискованным предприятием», блог The Security Skeptic, 14 августа 2019 года: https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html; ICANN SSAC, «SAC 096: Рекомендация SSAC в отношении Централизованной службы файлов корневой зоны (CZDS) и ежемесячных отчетов о деятельности операторов регистратур», 16 июня 2017 года: https://www.icann.org/resources/files/1207653-2017-06-16-en.

[80] Клэффи (KC) и Дэвид Кларк, «Отчет о семинаре по экономике интернета (WIE 2019)», апрель 2020 года: https://ccronline.sigcomm.org/2020/ccr-april-2020/workshop-on-internet-economics-wie-2019-report%EF%BB%BF/.

заключение по этой теме в июне 2017 года (SAC097), более трех лет назад.[81] Правление ICANN приняло соответствующие рекомендации, но до сих пор не выполнило их.[82] Группа по анализу SSR2 признает, что для некоторых TLD (например, TLD-брендов) может потребоваться компромисс в том, что касается CZDS, для защиты бренда или из соображений безопасности, однако доступ к критически важным данным через CZDS в целом остается проблематичным.[83]

После июньской резолюции Правления 2018 года количество жалоб на доступ к файлу корневой зоны увеличилось и остается выше, чем в середине 2018 года. Сейчас это самая крупная категория жалоб на операторов регистратур.[84] Отдел по контролю исполнения договорных обязательств ICANN иногда не обрабатывал жалобы на ZFA в течение нескольких месяцев после их подачи.[85] В 2018 году корпорация ICANN обратилась к рабочей группе по последующим процедурам, применимым к новым gTLD (обычно называемой рабочей группой SubPro), с просьбой решить эту проблему.[86] Рабочая группа SubPro не упомянула об этом в недавнем 363-страничном проекте своего отчета.[87] Нет никаких признаков того, что корпорация ICANN, Правление ICANN или сообщество регистратур приняли достаточные меры для решения проблем с доступом к CZDS. Эта проблема является предметом рекомендации SSR2 № 11 «Решить проблемы доступа к данным CZDS».

[81] Консультативный комитет по безопасности и стабильности ICANN, «SAC097: Рекомендация SSAC в отношении Централизованной службы файлов корневой зоны (CZDS) и ежемесячных отчетов о деятельности операторов регистратур», 12 июня 2017 года: https://www.icann.org/en/system/files/files/sac-097-en.pdf.

[82] Консультативный комитет ICANN по безопасности и стабильности, «Состояние дел с рекомендациями Консультативного комитета по безопасности и стабильности (SSAC)», последняя редакция от 31 октября 2020 года: https://features.icann.org/board-advice/ssac. См. «SAC097: Рекомендация SSAC в отношении Централизованной службы файлов корневой зоны (CZDS) и ежемесячных отчетов о деятельности операторов регистратур, R-1 (12 июня 2017 года)».

[83] Партридж, Марк В.Б. и Джордан А. Арнот. «Расширение системы доменных имен: преимущества, возражения и разногласия». DePaul J. Art Tech. & Intell. Prop. L 22 (2011 год): 317 (см. стр. 5 статьи); «CZDS-API-Testbed — лист рассылки для пользователей API CZDS, которые могут подписаться и участвовать в обсуждении тем, относящихся к API»: https://mm.icann.org/mailman/listinfo/czds-api-testbed. См. ветки жалоб в архиве (обратите внимание, что доступ предоставляется только подписчикам, но подписка открыта).

[84] ICANN, «Показатели эффективности деятельности отдела по контролю исполнения договорных обязательств», источник проверен 7 декабря 2020 года: https://features.icann.org/compliance/dashboard/report-list. Обратите внимание, что жалобы на доступ к файлам зон по состоянию на март 2020 года составили 85,5% всех жалоб по сравнению с 31,9% в марте 2018 года.

[85] «CZDS-API-Testbed — лист рассылки для пользователей API CZDS, которые могут подписаться и участвовать в обсуждении тем, относящихся к API»: https://mm.icann.org/mailman/listinfo/czds-api-testbed. См. ветки жалоб в архиве (обратите внимание, что доступ предоставляется только подписчикам, но подписка открыта).

[86] ICANN, «Устав рабочей группы по PDP в области последующих процедур, применимых к новым gTLD», 21 января 2016 года: https://gnso.icann.org/sites/default/files/filefield_48475/subsequent-procedures-charter-21jan16-en.pdf.

[87] Рабочая группа ICANN по последующим процедурам, применимым к новым gTLD, «Проект итогового отчета GNSO по последующим процедурам, применимым к новым gTLD», источник проверен 7 декабря 2020 года: https://www.icann.org/public-comments/gnso-new-gtld-subsequent-draft-final-report-2020-08-20-en.

iii. Платформа отчетности о случаях неправильного использования DNS

Проект ICANN по подготовке отчетности о случаях неправильного использования DNS (DAAR) — это «*платформа для изучения регистрации доменных имен и поведения регистратур доменов верхнего уровня (TLD) и регистраторов, создающего угрозы для безопасности (злоупотреблений)*» с основной целью «*информировать сообщество ICANN о деятельности, которая угрожает безопасности, чтобы сообщество могло воспользоваться этими данными для принятия обоснованных решений*».[88] Корпорация ICANN начала свою программу DAAR в 2017 году. Корпорация ICANN заявила, что DAAR призвана предоставить сообществу транспарентный и воспроизводимый научный подход к отчетности о неправильном использовании DNS.[89] С января 2018 года OCTO ICANN на основе анализа данных DAAR ежемесячно публикует отчет высокого уровня, но с детализацией, которая не позволяет сделать выводы о том, какие регистраторы или регистратуры допускают серьезные злоупотребления. Кроме того, корпорация ICANN не передает исследователям полные (необработанные) данные, которые могли бы способствовать улучшению методологии или подтвердить выводы. Персонал OCTO сообщил группе по анализу SSR2, что эти задачи (практически полезные данные, проверка достоверности) не входили в состав целей разработки DAAR.[90] Группа по анализу SSR2 считает, что подход, который корпорация ICANN, по-видимому, использует при формировании структуры соглашений с провайдерами данных, является серьезным препятствием для достижения этих целей, и предлагает пересмотреть программу анализа неправильного использования DNS, сделав ее основными целями транспарентность, воспроизводимость и получение практически полезных информационных продуктов.

Выявление регистратур и регистраторов с непропорционально высоким уровнем злоупотреблений облегчило бы выработку обоснованной политики и обеспечило бы отсутствующую на сегодняшний день транспарентность и подотчетность системы регистрации доменных имен. В самом деле, группа по анализу не понимает, какая польза от инвестиций ICANN в этой области, если данные и результаты не имеют практического смысла и не передаются в целях воспроизводимости и проверки. Группа по анализу SSR2 считает, что программу DAAR целесообразно закрыть, если сообществу и корпорации ICANN не удастся провести пересмотр DAAR для достижения этих целей. Рекомендация SSR2 № 12: «Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку» посвящена именно этой проблеме.

iv. Жалобы

В отчете по CCT была отмечена сложность оценки воздействия мер защиты, вызванная отсутствием транспарентности со стороны отдела по контролю исполнения договорных обязательств ICANN в отношении жалоб и недостаточным контролем за выполнением договорных обязательств по соблюдению общественных интересов.[91] Группа по анализу

[88] Часто-задаваемые вопросы по DAAR: https://www.icann.org/octo-ssr/daar-faqs/#security-threats.

[89] Дэйв Писцителло, «Система отчетности о злоупотреблениях доменами (DAAR)», отчет APWG.EU для ICANN, октябрь 2017 года: https://www.icann.org/en/system/files/files/presentation-daar-31oct17-en.pdf.

[90] Стенограмма телеконференции: «Телеконференция SSR2 на тему DAAR — 24 июня 2020 года в 15:00 по UTC»: https://community.icann.org/x/WIJIC.

[91] Отчет по CCT, 9-10: https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

SSR2 обнаружила, что для лиц, которые информируют о вредоносных доменах, основной проблемой является сложность процедуры подачи жалоб, различия в требованиях сторон, связанных договорными обязательствами, и частое отсутствие (своевременного) ответа или действий. Группа по анализу SSR2 считает, что централизованная система подачи жалоб о злоупотреблениях упростит процесс подачи жалоб как для подателей, так и для сторон, связанных договорными обязательствами, и сократит количество неправильно жалоб, отправленных не по адресу.

Группа по анализу SSR2 считает, что пересмотренная программа анализа неправильного использования DNS позволит отделу по контролю исполнения договорных обязательств ICANN установить типовые ожидания в отношении показателей распространенности злоупотреблений. Поскольку черные списки могут не быть на 100% точными и ими можно манипулировать, ICANN придется приложить усилия для проверки результатов анализа, а у сторон, связанных договорными обязательствами, должна быть возможность опротестовать уведомление ICANN.

Рекомендация SSR2 № 10: Обеспечение ясности определений терминов, связанных со злоупотреблениями

10.1. Корпорация ICANN должна опубликовать веб-страницу, содержащую рабочее определение неправильного использования DNS, т. е. определение, которое она использует для проектов, документов и контрактов. В определении следует четко указать, какие типы угроз безопасности корпорация ICANN в настоящее время рассматривает в рамках своей компетенции для устранения с помощью договорных механизмов и механизмов соблюдения требований, а также те угрозы, которые корпорация ICANN считает выходящими за рамки ее компетенции. Если корпорация ICANN использует другую аналогичную терминологию — например, угроза безопасности, злонамеренное поведение — следует не только указать рабочее определение этих терминов, но и пояснить, в чем для корпорации ICANN состоит различие между этими терминами и неправильным использованием DNS. Эта страница должна содержать ссылки на выдержки из всех текущих обязательств, относящихся к злоупотреблениям, в контрактах со сторонами, связанными договорными обязательствами, включая любые процедуры и протоколы реагирования на злоупотребления. Корпорация ICANN должна обновлять эту страницу ежегодно, датировать последнюю версию и ссылаться на более старые версии с соответствующими датами публикации.

10.2. Создать поддерживаемую персоналом сквозную рабочую группу сообщества (CCWG) для организации процесса разработки определений запрещенного неправильного использования DNS, по крайней мере, один раз в два года по предсказуемому графику (например, каждый второй январь), длительность которого не превышает 30 рабочих дней. В эту группу должны входить заинтересованные стороны, представляющие защиту потребителей, операционную кибербезопасность, научные или независимые исследования кибербезопасности, правоохранительные органы и электронную коммерцию.

10.3. Правлению и корпорации ICANN следует последовательно использовать согласованные определения в общедоступных документах, контрактах, планах выполнения рекомендаций групп по анализу и другой деятельности, а также ссылаться на эту веб-страницу.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN опубликует веб-страницу с первыми результатами работы CCWG, а также процесс обновления этой веб-страницы.

Эту рекомендацию можно будет считать действенной, если корпорация ICANN сможет повысить транспарентность и подотчетность в том, что касается принятых и проверенных сообществом описаний, а также внести ясность в дискуссии сообщества и толкование документов по вопросам политики, что позволит другим заинтересованным сторонам определять кодексы поведения в отношении злоупотреблений DNS.

Рекомендация SSR2 № 11: Решение проблем с доступом к данным CZDS

11.1. Сообществу ICANN и корпорации ICANN следует предпринять шаги, обеспечивающие своевременный доступ к данным CZDS без лишних препятствий для запрашивающих данные лиц, например автоматическое продление срока действия учетных данных.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN и сообщество обеспечат возможность своевременного доступа к данным CZDS без лишних препятствий для запрашивающих данные лиц.

Эту рекомендацию можно будет считать действенной, когда корпорация ICANN сообщит о сокращении количества жалоб на доступ к файлу корневой зоны и предоставит исследователям более широкие возможности для изучения операций в DNS, имеющих отношение к безопасности.

Эта рекомендация призвана обеспечить надлежащий доступ к данным файлов зон, относящимся к безопасности, которые используются учеными и специалистами по безопасности. Эта рекомендация требует действий со стороны Правления ICANN, корпорации ICANN и GNSO.

Рекомендация SSR2 № 12: Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку

12.1. Корпорация ICANN должна создать консультативную группу по анализу неправильного использования DNS, состоящую из независимых экспертов (т. е. экспертов без конфликтов финансовых интересов), чтобы рекомендовать существенный пересмотр отчетности о неправильном использовании DNS, в которой получение практически полезных данных, проверка, транспарентность и независимая воспроизводимость аналитических результатов имеют наивысший приоритет.

12.2. Корпорация ICANN должна видоизменить структуру своих соглашений с поставщиками данных, чтобы разрешить последующую передачу данных для некоммерческого использования, в частности, для проверки или рецензируемых научных исследований. Эта специальная бесплатная некоммерческая лицензия на использование данных может включать временную задержку, чтобы не мешать коммерческому доходу поставщика данных. Корпорация ICANN должна должна публиковать все условия

контрактов о совместном использовании данных на веб-сайте ICANN. Корпорация ICANN должна расторгнуть любые контракты, которые не позволяют независимую проверку методологии, стоящей за блокировкой.

12.3. Корпорация ICANN должна указывать в публикуемых отчетах, у каких регистратур и регистраторов больше всего доменов, используемых для злоупотреблений. Корпорация ICANN должна включать данные в пригодных для машинного считывания форматах, в дополнение к графическим данным, представленным в текущих отчетах.

12.4. Корпорация ICANN должна сводить воедино и публиковать отчеты о действиях, которые регистратуры и регистраторы предприняли, как добровольно, так и в связи с юридическими обязательствами, в ответ на жалобы о незаконных и/или злонамеренных действиях на основании применимого законодательства в связи с использованием DNS.

Эту рекомендацию можно будет считать выполненной, когда в рамках деятельности корпорации ICANN по анализу неправильного использования DNS будут введены показатели, позволяющие получить практически полезные, точные и заслуживающие доверия данные.

Эту рекомендацию можно будет считать действенной, если все доступные корпорации ICANN данные также будут доступны сообществу и независимым исследователям (возможно, с задержкой по времени) для проверки и обратной связи.

Рекомендация SSR2 № 13: Повышение транспарентности и подотчетности сообщений о нарушениях

13.1. Корпорация ICANN должна создать и поддерживать центральный портал для жалоб на неправильное использование DNS, который обеспечивает автоматическую пересылку всех сообщений о злоупотреблениях соответствующим сторонам. Система будет действовать исключительно для получения данных, при этом корпорация ICANN будет собирать и обрабатывать только сводку и метаданные, включая временные метки и типы жалоб (по категориям). Использование системы должно стать обязательным для всех gTLD; участие каждого ccTLD будет добровольным. Кроме того, корпорации ICANN следует предоставлять отчеты о злоупотреблениях (например, по электронной почте) всем ccTLD.

13.2. Корпорация ICANN должна публиковать количество поданных жалоб в форме, позволяющей независимым третьим сторонам анализировать типы жалоб на операции в DNS.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN упростит процесс подачи и получения жалоб на злоупотребления и предоставит исследователям и членам сообщества данные о количестве жалоб и некоторые метаданные (например, вид заявленного нарушения, дата, срок рассмотрения жалобы). Эту рекомендацию можно будет считать полностью выполненной после запуска и начала работы портала.

Эту рекомендацию можно будет считать действенной, если сторонам, связанным договорными обязательствами, придется тратить меньше времени на жалобы, отправленные не по адресу, а исследовательское сообщество, а также все остальное сообщество ICANN смогут получать и изучать соответствующие данные об этих жалобах.

Из-за сложности этой инициативы ожидается, что выполнение этой рекомендации займет несколько лет (не менее трех) после принятия Правлением ICANN решения о ее выполнении.

3. Альтернативы процессу разработки политики (PDP)

Важно рассмотреть утверждения о том, что согласованная политика, сформированная в процессе разработки политики (PDP), является единственным путем к выполнению некоторых наших рекомендаций.Есть много способов, позволяющих Правлению ICANN продвинуться в деле выполнения наших рекомендаций. Правление может выбрать контрактные переговоры, дать рекомендации сторонам, связанным договорными обязательствами, или привлечь ограниченную по срокам и поддерживаемую экспертами сквозную рабочую группу сообщества.[92] Корпорация ICANN может даже выпустить временную спецификацию, исходя из убежденности Правления в том, что неправильное использование DNS является серьезной проблемой общественной безопасности, требующей безотлагательного внимания. Недавнее использование Правлением Временной спецификации в ответ на расхождения между GDPR EC и собственным Уставом ICANN служит полезным примером.У сообщества ICANN были годы для выработки политики доступа к регистрационным данным, которая согласовывалась бы с GDPR, но оно фактически отложило решение этого вопроса.Мы видим аналогичную картину в отношении неправильного использования DNS и доступа к регистрационным данным для борьбы со злоупотреблениями.

Корпорация ICANN может вести двусторонние контрактные переговоры и ведет их. Изменения в соглашения корпорации ICANN с регистратурами и регистрами вносились и без выработки согласованной политики в рамках PDP. Когда корпорация ICANN обновляла RAA в 2013 году и вводила базовое Соглашение об администрировании домена верхнего уровня в 2017 году, корпорация ICANN и делегация представителей соответствующей отрасли управляли этим процессом без какого-либо PDP. У сообщества была возможность прокомментировать проект текста, но в обсуждениях и принятии решений участвовала только группа, которая вела переговоры.[93] Такие закрытые переговоры между корпорацией ICANN и связанными договорными обязательствами сторонами являются ценным средством достижения прогресса, но ограничены в том, что касается неправильного использования DNS, поскольку из переговорного процесса исключены все остальные заинтересованные стороны, включая правительства, представителей бизнеса и общественность, которые также заинтересованы в уменьшении количества злонамеренных регистраций. Рекомендация SSR2 № 12: «Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку» устраняет этот пробел.

---

[92] С примерами предыдущих рекомендаций сторонам, связанным договорными обязательствами можно ознакомиться на сайте «Рекомендации регистраторам» (https://whois.icann.org/en/registrar-advisories).

[93] Соглашение об аккредитации регистраторов 2013 года: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. Примечание: ICANN может вносить поправки в соглашения либо путем выработки согласованной политики, либо путем переговоров между корпорацией ICANN и другими соответствующими сторонами соглашения в соответствии с RAA, раздел 1.2, «Согласованная политика и временные спецификации по вопросам политики»: https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary.

Группа по анализу считает, что процесс EPDP сам по себе не приведет к эффективному решению в области противодействия злоупотреблениям, особенно в свете того, что EPDP не позволил решить проблему доступа к регистрационным данным, процесс PDP отягощен огромными конфликтами интересов, а борьба с неправильным использованием DNS продвигается очень медленно. Для завершения EPDP в области доступа к регистрационным данным потребовались годы, а окончательный продукт вызвал несогласие со стороны большей части сообщества ICANN; поступили весомые заявления о мнении меньшинства от Консультативного комитета At-Large (ALAC), Группы интересов коммерческих пользователей и Группы интересов по вопросам интеллектуальной собственности (BC/IPC), Группы некоммерческих заинтересованных сторон (NCSG), Группы заинтересованных сторон-регистраторов (RrSG) и Группы заинтересованных сторон-регистратур (RySG). В заявлении меньшинства BC/IPC содержится следующее предупреждение: «*Регулирующим и законодательным органам следует учитывать, что модель с участием многих заинтересованных сторон ICANN не удовлетворяет потребности в защите потребителей, кибербезопасности и охране правопорядка*».[94] Меньшинство в лице SSAC также известило о том, что процесс разработки политики ICANN «*не дал результатов, которые способны обеспечить достаточную безопасность и стабильность*».[95]

Таким образом, смягчение, предотвращение и пресечение неправильного использования DNS затрудняется двусмысленностью существующей терминологии и контрактных требований, конфликтами интересов всех сторон, которым необходимо участвовать в этой работе, и разнообразными обязательствами правительств разных стран мира решать проблемы неправильного использования DNS также и посредством других юридических процессов. Уже есть несколько принципов политики и договорных обязательств, относящихся к неправильному использованию DNS, однако корпорации ICANN и связанным договорными обязательствами сторонам необходимо эффективнее претворять их в жизнь и контролировать их соблюдение, а сообществу необходимо разработать дополнительные принципы политики, договорные обязательства и мероприятия, чтобы не отставать от развития событий в области неправильного использования DNS. Группа по анализу SSR2 считает, что борьба с неправильным использованием DNS крайне необходима, и это дает основания для твердой руководящей роли ICANN в данной области. Временная спецификация GDPR продемонстрировала, что Правление ICANN сохраняет полномочия по выработке политики в ответ на различные потребности. Более того, на Правление возложены фидуциарные обязанности по обеспечению соответствия политики корпорации ICANN и производных контрактов целям корпорации ICANN как калифорнийской некоммерческой корпорации по обеспечению общественных интересов, которой поручено осуществлять надзор за безопасностью, стабильностью DNS и выработкой политики в общественных интересах. Возможно, наилучшим подходом является новая временная спецификация в сочетании с новым EPDP.[96]

---

[94] Отчет GNSO по фазе 2 EPDP, Заявление меньшинства BC/IPC, 114-121: https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.

[95] Тот же источник, 145–162, Заявление меньшинства SSAC.

[96] Группа по анализу SSR2 считает, что корпорация ICANN накопила достаточный объем знаний, в том числе знания, которые привели к созданию программы DAAR и самих отчетов DAAR, чтобы составить отчет о неразрешенных проблемах, подтверждая тем самым целесообразность запуска EPDP вместо PDP.

Рекомендация SSR2 № 14: Создать временную спецификацию для улучшения безопасности на основе доказательств

14.1. Корпорация ICANN должна создать временную спецификацию, требующую, чтобы все стороны, связанные договорными обязательствами, сохраняли процентную долю доменов, которые в обновленных отчетах о неправильном использовании DNS (см. рекомендацию SSR2 № 13.1) признаны используемыми для злоупотреблений, ниже разумного и опубликованного порогового значения.

14.2. Чтобы обеспечить возможность принятия мер по борьбе со злоупотреблениями, корпорации ICANN следует предоставить сторонам, связанным договорными обязательствами, списки доменов в их портфелях, идентифицированных как используемые для злоупотреблений, в соответствии с рекомендацией SSR2 № 12.2, касающейся независимой проверки данных и методов внесения доменов в черный список.

14.3. Если количество доменов, связанных с злонамеренной деятельностью, достигнет опубликованного порогового значения, указанного в рекомендации SSR2 № 14.1, корпорация ICANN должна провести расследование, чтобы подтвердить достоверность данных и анализа, а затем направить уведомление соответствующей стороне.

14.4. Корпорация ICANN должна предоставить связанным договорными обязательствами сторонам 30 дней на то, чтобы уменьшить долю недобросовестно используемых доменов ниже порогового значения или продемонстрировать ошибочность выводов или данных корпорации ICANN. Если сторона по контракту не внесет исправления в течение 60 дней, отдел соблюдения договорных обязательств ICANN должен перейти к процессу отмены аккредитации.

14.5. Корпорация ICANN должна рассмотреть возможность финансового стимулирования: сторонам, связанным договорными обязательствами, в портфелях которых процент используемых для злоупотреблений доменных имен меньше определенного значения, взимаемый транзакционный сбор следует снизить до целесообразного порогового значения.

Рекомендация SSR2 № 15: Запустить EPDP для улучшения безопасности на основе доказательств

15.1. После создания временной спецификации (см. рекомендацию SSR2 № 14: «Создать временную спецификацию для улучшения безопасности на основе доказательств») корпорации ICANN следует организовать поддерживаемый персоналом EPDP для выработки политики борьбы со злоупотреблениями. Для определения численности и распределения волонтеров EPDP, представляющих сообщество ICANN, следует использовать в качестве образца устав группы по EPDP в области Временной спецификации для регистрационных данных в gTLD.[97]

[97] ICANN, «Устав группы по PDP», последняя редакция страницы от 23 июля 2018 года, 12–14: https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter.

15.2. EPDP должен опираться на фундамент определений CCWG, предложенный в рекомендации SSR2 № 10.2. Эта концепция политики должна определять соответствующие контрмеры и действия по исправлению положения для различных типов злоупотреблений, временные рамки для действий сторон по договору, таких как сроки сообщения о злоупотреблениях / отчета об ответах, а также меры по обеспечению соблюдения договорных обязательств ICANN в случае нарушения политики. Корпорация ICANN должна настаивать на праве прекращать действия контрактов в случае систематической практики укрывательства злоупотреблений со стороны любой стороны, связанной контрактом. Результат должен включать механизм обновления каждые два года контрольных показателей и договорных обязательств, связанных со злоупотреблениями, с использованием процесса, который не займет более 45 рабочих дней.

Рекомендации SSR2 № 14 и 15 можно будет считать выполненными, когда у отдела по контролю исполнения договорных обязательств ICANN будут средства для принятия надлежащих мер, если стороны, связанные договорными обязательствами, не реагируют на неправильное использование DNS, в частности, когда во всех соответствующих контрактах и соглашениях будут обязательства по борьбе со злоупотреблениями.

Рекомендации SSR2 № 14 и 15 можно будет считать действенными, если отдел по контролю исполнения договорных обязательств ICANN будет использовать эти средства для устранения вопиющих нарушений политики сторонами, связанными договорными обязательствами.

Ожидаемый результат выполнения рекомендаций SSR2 № 14 и 15 состоит в том, чтобы наделить отдел по контролю исполнения договорных обязательств ICANN полномочиями бороться со злостными нарушителями, когда речь идет о неправильном использовании DNS, для борьбы с которым, по утверждению сотрудников этого отдела ICANN, у них нет надлежащих средств.

Эти рекомендации требуют действий со стороны корпорации ICANN и сообщества ICANN и направлены на выработку политики. Цели этих рекомендации достижимы, но корпорация ICANN сможет выполнить их только со временем.

4. Координирующая роль в области защиты конфиденциальности и данных

Конфиденциальность — это постоянно прогрессирующая проблема из-за постоянно растущего объема сбора и анализа данных третьими сторонами (в дополнение к традиционным государственным учреждениям), а также из-за меняющегося законодательства о конфиденциальности. Группа по анализу SSR2 пришла к выводу, что корпорация ICANN была не настолько предусмотрительна, как того требовала меняющаяся ситуация, о чем свидетельствуют несоответствия в данных, доступных в RDS.[98]

На сайте ICANN растет число веб-страниц без указания даты, на которых обсуждаются различные аспекты конфиденциальности регистрационных данных. Отсутствие

[98] См. раздел E.2.b.i. «Регистрационные данные» и раздел E.2.b.ii. «Централизованная служба файлов корневой зоны» в настоящем отчете.

временных меток не позволило группе по анализу провести осмысленное исследование истории корпорации ICANN в данной области.[99] По состоянию на октябрь 2020 года сайт RDS и соответствующая документация также устарели и не содержат ни актуальных документов сообщества, ни ссылок на них. На сайте ICANN есть несколько веб-страниц на тему RDS, но на них отсутствуют перекрестные ссылки. Текущая веб-страница RDS на сайте ICANN последний раз обновлялась в 2017 году и, следовательно, там нет ссылок на текущие меры Временной спецификации или состояние дел с EPDP.[100] Группа по анализу считает, что отсутствие информации и последовательности на сайте является отражением отсутствия ясности и последовательности в вопросах конфиденциальности у самой корпорации ICANN.

В разделе E.2.b.i. «Регистрационные данные» группа по анализу также указала на необходимость сбалансировать транспарентность и подотчетность регистрационных метаданных доменных имен в свете различных правил соблюдения конфиденциальности, таких как GDPR. Обеспечив последовательность на собственном сайте, а также в согласованной политике и договорах с операторами регистратур и регистраторами, корпорация ICANN поможет обеспечить безопасное управление и защиту при сборе, хранении, временном депонировании, передаче и отображении регистрационных данных, в состав которых входят контактные данные владельца домена, контактных лиц по административным и техническим вопросам, а также техническая информация, имеющая отношение к доменному имени.

Рекомендация SSR2 № 16: Требования к конфиденциальности и RDS

16.1. Корпорация ICANN должна размещать на своем сайте согласованные перекрестные ссылки, чтобы предоставлять связную и легко доступную информацию обо всех действиях — прошлых, настоящих и запланированных, — в области конфиденциальности и управления данными, с особым вниманием к информации, касающейся RDS.

16.2. Корпорация ICANN должна создать специализированные группы в рамках функции по контролю исполнения договорных обязательств, которые понимают требования и принципы сохранения конфиденциальности (такие как ограничение сбора, классификация данных, указание цели использования и меры безопасности при раскрытии) и могут способствовать удовлетворению потребностей правоохранительных органов в рамках концепции RDS по мере исправления и принятия сообществом этой концепции (см. также рекомендацию SSR2 № 11: Решение проблем с доступом к данным CZDS).

16.3. Корпорация ICANN должна проводить периодическую проверку соблюдения политики конфиденциальности регистраторами, чтобы убедиться в наличии у них процедур для устранения нарушений конфиденциальности.

---

[99] Примеры: https://whois.icann.org/en/privacy-and-proxy-services, https://whois.icann.org/en/privacy, https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law и https://www.icann.org/rdap. Примечание: Кажется, что всем этим страницам много лет, и на некоторых внизу есть примечание: «17 мая 2018 года Правление ICANN утвердило Временную спецификацию для регистрационных данных в gTLD. Данная страница проверяется и будет обновлена с учетом Временной спецификации».

[100] ICANN, «О WHOIS», последняя редакция — июль 2017 года: https://whois.icann.org/en/about-whois.

Эту рекомендацию можно будет считать выполненной, если действия корпорации ICANN в отношении конфиденциальности и управления ею в RDS будут должным образом задокументированы, а специально выделенные внутренние ресурсы корпорации ICANN позволят ей идти в ногу с текущей передовой практикой и требованиями законодательства в этой области.

Эту рекомендацию можно будет считать действенной, когда корпорация ICANN будет постоянно применять передовые методы работы и демонстрировать постоянное соблюдение требований законодательства в области обработки и конфиденциальности данных.

F. Дополнительные вопросы, вызывающие озабоченность в связи с глобальной системой DNS и касающиеся SSR

Группа по анализу SSR2 признает, что корпорация ICANN — всего лишь одна из многих организаций в экосистеме DNS. С другой стороны, корпорация ICANN входит в число тех, у кого есть уникальная возможность влиять и направлять действия, связанные с SSR, в масштабе всей экосистемы. В данном разделе предлагаются конкретные рекомендации относительно областей, в которых корпорация ICANN может улучшить свои практические методы и политику для себя и для всей глобальной DNS. Внедряя передовой опыт при управлении IMRS, распространяя совместный вклад исследователей, предлагая инструменты для тестирования и анализа, а также принимая другие возможные меры, обсуждаемые в этом разделе, корпорация ICANN может предпринять шаги как для улучшения своих собственных действий в области SSR, так и для помощи другим в понимании путей улучшения их деятельности.

1. Доменные коллизии

Хотя корпорация ICANN предоставляет подробные материалы и обучение по вопросу доменных коллизий, отсутствуют ограничения на использование владельцами доменов для частной зоны уникальных идентификаторов, вступающих в конфликт с идентификаторами общедоступной зоны. Группа по анализу SSR2 считает недавно завершенное и опубликованное исследование (далее именуемое исследованием NCAP 2019 года) шагом в правильном направлении для устранения нежелательных доменных коллизий.[101] Однако при проведении этого исследования не учитывалась сохраняющаяся потребность в механизмах обнаружения незарегистрированных конфликтов имен, как злонамеренных, так и случайных. В ходе исследования также был сделан вывод о том, что доменные коллизии уже давно не изучаются (с 2017 года), а сокращение числа зарегистрированных коллизий рассматривалось как признак работоспособности существующих механизмов.[102] С другой стороны, авторитетное исследование в 2016 году

[101] Карен Скарфоне, «Управление рисками доменных коллизий среди доменных имен верхнего уровня: выводы по итогам исследования Проект анализа доменных коллизий (NCAP)», ICANN OCTO, 27 мая 2020 года: https://www.icann.org/en/system/files/files/managing-risks-tld-2-name-collision-07may20-en.pdf.
[102] Тот же источник, 43.

показало, что последний раунд создания gTLD заметно усугубил проблему доменных коллизий.[103] Уменьшение количества доменных коллизий, зарегистрированных с помощью традиционных механизмов отчетности, не означает отсутствия таких коллизий. Напротив, характер доменных коллизий мог измениться таким образом, что позволяет им ускользать из поля зрения этих традиционных механизмов. В последние годы также сократился темп делегирования новых gTLD, что могло еще больше повлиять на абсолютное количество зарегистрированных доменных коллизий.[104]

Хотя в отчете, подготовленном по заказу ICANN в 2014 году (далее именуемом отчетом о первой фазе) во избежание потенциальных коллизий между доменными именами была предложена концепция управляемого прерывания, эта концепция никогда не тестировалась применительно к новым сценариям атак с использованием доменной коллизии.[105] Например, SSAC дал следующую рекомендацию: «*Вместо единого периода контролируемого прерывания ICANN следует ввести скользящие периоды прерывания, перемежающиеся с периодами нормальной работы, чтобы вовлеченные системы конечных пользователей могли продолжать работу в течение 120-дневного тестового периода, что позволит сократить риск катастрофических последствий для бизнеса*».[106] Авторы отчета о первой фазе сделали ряд своих выводов на основании отсутствия электронных писем и телефонных звонков от владельцев доменов второго уровня, что не обеспечивает адекватного отражения сложности этой проблемы.[107] В отчете о первой фазе также обсуждалось несколько альтернативных подходов к концепции управляемого прерывания, включая использование ловушек для хакеров, DNAME и подходы «строка-строка», но эти подходы никогда не рассматривались в контексте их реализации.[108] Группа по анализу SSR2 приходит к заключению, в противовес авторам отчета о первой фазе, что доменные коллизии все еще остаются проблемой, требующей дальнейшего изучения и устранения.

Рекомендация SSR2 № 17: Измерение доменных коллизий

17.1. Корпорация ICANN должна создать концепцию, которая позволит определить характер и частоту доменных коллизий и возникающие в результате этого проблемы. Эта концепция должна включать метрики и механизмы для измерения степени, в которой управляемое прерывание является успешным для выявления и устранения доменных коллизий. Это может поддерживаться механизмом, обеспечивающим защищенное раскрытие экземпляров доменных коллизий. Эта концепция должна позволять надлежащую обработку конфиденциальных данных и угроз безопасности.

---

[103] Ци Альфред Чен, Эрик Остервейл, Мэтью Томас и З. Морли Мао. «MitM-атаки с использованием доменной коллизии: анализ причин и оценка уязвимостей в эпоху новых gTLD». Симпозиум IEEE по безопасности и конфиденциальности (SP) 2016 года (май 2016 года), 675-690. doi:10.1109/sp.2016.46.

[104] ICANN, сайт Программы New gTLD: https://newgtlds.icann.org/en/program-status/statistics.Примечание: по состоянию на 12 декабря 2020 года в обработке остаются только 9 заявок на gTLD из первоначальных 1930.

[105] ICANN, «Отчет о первой фазе — снижение риска коллизий в пространстве имен DNS», 6 июля 2014 года, 6, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf; ICANN, «Рамочный план действий в случаях доменных коллизий», 30 июля 2014 года, 2-3, https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf.

[106] SSAC ICANN, «SAC066: Комментарий SSAC по отчету JAS о первой фазе — снижение риска коллизий в пространстве имен DNS», 6 июня 2014 года, 4: https://www.icann.org/en/system/files/files/sac-066-en.pdf.

[107] Отчет о первой фазе — снижение риска коллизий в пространстве имен DNS, 22: https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf.

[108] Тот же источник.

17.2. Сообщество ICANN должно разработать четкую политику для предотвращения и разрешения доменных коллизий, связанных с новыми gTLD, и реализовать эту политику до следующего раунда создания gTLD. Корпорация ICANN должна обеспечить, чтобы оценка этой политики проводилась сторонами, не имеющими финансовой заинтересованности в расширении gTLD.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN разработает концепцию для получения результатов, которые характеризуют характер и частоту доменных коллизий и возникающие в результате проблемы, путем определения показателей и разработки механизмов для измерения степени успешности механизма управляемого прерывания.

Эту рекомендацию может будет считать действенной, если у корпорации ICANN и сообщества появится возможность выявлять доменные коллизии, принимать меры и, в конечном итоге, минимизировать их существование, а также реагировать на изменение сценариев доменных коллизий.

Эта рекомендация должна быть выполнена до начала следующего раунда создания gTLD.

2. Исследования и брифинги

В настоящее время в научно-исследовательском сообществе наблюдается огромная активность в решении вопросов SSR на уровнях именования, маршрутизации и адресации. Сообщество ICANN может воспользоваться этой деятельностью и опытом в качестве информационной основы при разработке политики и технологий, которые значительно снизят ущерб экосистеме в области SSR. Однако не предусмотрено функций, которые позволяли бы самой корпорации ICANN и сообществу, которое она обслуживает, оставаться в курсе этих событий.

Рекомендация SSR2 № 18: Информационное обеспечение дебатов по вопросам политики

18.1. Корпорация ICANN должна следить за событиями в научном сообществе, уделяя особое внимание конференциям по вопросам исследования сетей и безопасности, включая по крайней мере ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, Симпозиум IEEE по безопасности и конфиденциальности, а также конференции по оперативной безопасности и FIRST, и публиковать для сообщества ICANN отчет, в котором обобщаются последствия публикаций, имеющих отношение к работе корпорации ICANN или сторон, связанных договорными обязательствами.[109]

[109] Ссылки на конференции: ACM CCS <https://dl.acm.org/conference/ccs>, ACM Internet Measurement Conference <https://www.sigcomm.org/events/imc-conference>, Usenix Security <https://www.usenix.org/conferences>, CCR <https://www.ccrsummit.com/>, SIGCOMM <https://www.sigcomm.org/>, Симпозиум IEEE по безопасности и конфиденциальности <https://www.ieee-security.org/index.html>, FIRST <https://www.first.org/>. Примечание: Чтобы выполнить эту рекомендацию, предлагается наладить контакты с организаторами (председателями комитетов по разработке технических программ, организаторами руководящих групп и т. д.) и запрашивать у них дайджесты мероприятий и/или ежегодно приглашать членов комитетов этих конференций на одно из мероприятий сообщества ICANN для ознакомления с соответствующими дайджестами. При таком подходе к выполнению рекомендации корпорация ICANN сохраняла бы полученные материалы в архивном отчете.

18.2. Корпорация ICANN должна обеспечить, чтобы эти отчеты содержали важные соображения, которые могут повлиять на рекомендации относительно действий, в том числе изменений в договорах с регистратурами и регистраторами, способных смягчить, предотвратить или устранить вред потребителям и инфраструктуре в области SSR, указанный в рецензируемой научной литературе.

18.3. Корпорация ICANN должна обеспечить, чтобы эти отчеты также содержали рекомендации по дополнительным исследованиям для подтверждения результатов экспертной оценки, описание данных, которые потребуются сообществу для проведения дополнительных исследований, и сведения о том, какую помощь может предложить корпорация ICANN для организации доступа к таким данным через посредника, например через CZDS.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN создаст и будет поддерживать общедоступный архив дайджестов или результатов различных конференций, посвященных исследованиям сетей и безопасности.

Эту рекомендацию можно будет считать действенной, когда информация, поступающая от исследовательского сообщества по вопросам, связанным с SSR, станет более доступна лицам, принимающим решения по вопросам политики.

3. Испытательная платформа DNS

Поскольку экосистема DNS уже велика и продолжает расти, крайне важно постоянно поддерживать и контролировать пакет регрессионных тестов и испытательную платформу для анализа поведения и взаимодействия в DNS. Группа по анализу SSR2 пришла к выводу, что текущая работа OCTO над испытательной платформой DNS после ее завершения в достаточной мере решит эту проблему.[110] Группа по анализу также полагает, что поддержка и обслуживание этой испытательной платформы (наряду с использованием полученных результатов и выводов) является требованием корпорации ICANN.

Своевременное завершение работ и обслуживание этой испытательной платформы позволят сообществу ICANN тестировать и исследовать поведение резолверов, что имеет решающее значение для обеспечения целостности и глобальной доступности DNS.

Рекомендация SSR2 № 19: Полная разработка набора тестов регрессии DNS

19.1. Корпорация ICANN должна завершить разработку пакета для тестирования резолверов DNS.

19.2. Корпорация ICANN должна обеспечить возможность продолжения реализации и поддержки функционального тестирования различных конфигураций и версий программного обеспечения.

[110] «Испытательная платформа для резолверов», репозиторий GitHub ICANN, https://github.com/icann/resolver-testbed.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN завершит разработку общедоступного пакета тестов для выполнения сообществом тестирования и исследования поведения резолверов.

Эту рекомендацию можно будет считать действенной при наличии пакета тестов с ежегодным циклом обновления, который помогает обеспечить целостность и глобальную доступность DNS.

4. Проблемы с корневой зоной и регистратурами

A. Обновление ключа

Ключ для подписания ключей (KSK) DNSSEC корневой зоны был обновлен 11 октября 2018 года впервые с момента создания ключа зоны, которая заведомо не может быть криптографически проверена (DURZ).[111] Во время процесса обновления ключа было много споров и поступило много призывов проанализировать детали этого обновления.[112] Одним из результатов изучения данного вопроса группой по анализу SSR2 стало понимание того, что для безопасного и успешного обновления ключа в составе процедуры должны быть правильно функционирующие ветви обработки исключений.[113] Корпорация ICANN отложила обновление ключа на год, чтобы выполнить измерения и развеять опасения. В сообществе ICANN уже началось обсуждение сроков и процедуры будущих операций обновления ключа, в том числе рассмотрение потенциальных новых сложностей, например обновлений алгоритма.[114] Соответственно, корпорация ICANN открыто призвала направлять комментарии по процессу очередного запланированного обновления ключа KSK.[115]

В связи с крайней важностью средств обеспечения безопасности, основой для которых является (и будет являться) подписание корневой зоны с помощью DNSSEC, решающее значение для обеспечения безопасности, стабильности и отказоустойчивости процесса, посредством которого при обновлении ключа KSK корневой зоны обеспечивается сохранение средств защиты DNSSEC, имеет поддающийся формальной проверке анализ

[111] ICANN, «Первое обновление ключа KSK прошло успешно», 15 октября 2018 года: https://www.icann.org/news/announcement-2018-10-15-en.

[112] ICANN, «Недавнее обновление ключа KSK: итоги и дальнейшие действия», блог ICANN, 30 января 2018 годаhttps://www.icann.org/news/blog/the-recent-ksk-rollover-summary-and-next-steps; Мориц Мюллер, Мэтью Томас, Дуэйн Весселс, Уэс Хардакер, Тэджун Чанг, Виллем Тороп и Роланд ван Рейсвейк-Дейдж, «Верти, верти, верти свой корень:комплексный анализ первого в истории обновления ключа KSK DNSSEC корневой зоны», октябрь 2019 года: https://dl.acm.org/doi/10.1145/3355369.3355570.

[113] Стенограмма пленарного заседания SSR2 № 97 — утреннее заседание, 17 января 2020 года, 35: https://community.icann.org/x/HJkzBw.

[114] Отчет персонала о результатах общественного обсуждения: Предложение об изменении процедуры обновления ключа KSK корневой зоны, 7 августа 2020 года: https://www.icann.org/en/system/files/files/report-comments-proposal-future-rz-ksk-rollovers-07aug20-en.pdf.Примечание: комментарии поступили от компании Japan Registry Services, Группы интересов коммерческих пользователей ICANN, Группы некоммерческих заинтересованных сторон ICANN, Консультативного комитета системы корневых серверов ICANN, Консультативного комитета по безопасности и стабильности ICANN и нескольких физических лиц.

[115] «Предложение об изменении процедуры обновления ключа KSK корневой зоны», 1 ноября 2019 года: https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en.

этого процесса.[116] При формальном моделировании процесса используется методология и/или среда программирования для определения каждой задачи в процессе, оценки ее выполнения (успех, неудача, прочее и т. д.) и определения последующих действий в зависимости от результатов. Подобные спецификации процессов продемонстрировали свою полезность в сложных процессах человеческого общения, включая безопасность при проведении выборов, безопасность медицинских процессов и многое другое.[117] В этих случаях задачи людей (в социуме) сложны и моделируются с помощью формальных языков спецификации процессов, а критические (и жизненно-важные) решения и последствия моделируются символически и формально отслеживаются. Такое моделирование позволяет давать количественные предписания и прогнозы относительно целесообразных действий и возможных результатов выбора, исключительных ситуаций и успешного выполнения.[118] По сравнению с выборами и медицинскими процессами, обновление ключа KSK корневой зоны DNS представляет собой легко управляемую площадку, для которой безопасность и правильность работы имеют глобальное значение.

Рекомендация SSR2 № 20: Официальные процедуры обновления ключей

20.1. Корпорация ICANN должна установить формальную процедуру, опирающуюся на формальный инструмент и язык моделирования процессов, чтобы определить детали будущих обновлений ключа, включая точки принятия решений, ветви обработки исключений, полный поток управления и т. д. Проверка процесса обновления ключа должна предусматривать опубликование программной процедуры (например, программы, системы с конечным числом состояний (FSM)) для общественного обсуждения, и корпорация ICANN должна учесть отзывы сообщества. У процесса на каждом этапе должны быть эмпирически проверяемые критерии приемлемости, которые должны соблюдаться для продолжения процесса. Этот процесс должен подвергаться пересмотру не реже самого обновления ключа (то есть с той же периодичностью), чтобы корпорация ICANN могла использовать извлеченные уроки для корректировки процесса.

20.2. Корпорация ICANN должна создать группу заинтересованных сторон с участием соответствующего персонала (из корпорации ICANN или сообщества) для периодического проведения деловых игр по окончании процесса обновления ключа KSK корневой зоны.

---

[116] Эрик Остервейл, «Терминарх кибербезопасности:используйте его, пока он жив».*IEEE, журнал «Безопасность и конфиденциальность»* 18, № 4 (2020 год): 67–70.

[117] Леон Дж. Остервейл, Мэтт Бишоп, Хизер Конбой, Хонг Фан, Борислава И. Симидчиева, Джордж Аврунин, Лори А. Кларк и Шон Пайзерт, «Итеративный анализ для улучшения ключевых свойств особо важных процессов с активным участием человека: пример безопасности выборов», журнал ACM Transactions on Privacy and Security (TOPS), выпуск. 20, № 2, май 2017 года, стр. 5:1-31. (UM-CS-2016-012); Лори А. Кларк, Яо Чен, Джордж С. Аврунин, Бин Чен, Рэйчел Кобли, Ким Фредерик, Элизабет А. Хеннеман и Леон Дж. Остервейл, «Программирование процессов для обеспечения медицинской безопасности: анализ ситуации с переливанием крови», издание Software Process Workshop, стр. 347–359, Springer, Берлин, Гейдельберг, 2005 год.

[118] Итеративный анализ для улучшения ключевых свойств особо важных процессов с активным участием человека: пример безопасности выборов, Леон Дж. Остервейл, Мэтт Бишоп, Хизер Конбой, Хонг Фан, Борислава И. Симидчиева, Джордж Аврунин, Лори А. Кларк, Шон Пайзерт (Iterative Analysis to Improve Key Properties of Critical Human-Intensive Processes: An Election Security Example, Leon J. Osterweil, Matt Bishop, Heather Conboy, Huong Phan, Borislava I. Simidchieva, George Avrunin, Lori A. Clarke, Sean Peisert), журнал ACM Transactions on Privacy and Security (TOPS), выпуск. 20, № 2, май 2017 года, стр. 5:1-31. (UM-CS-2016-012).

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN разработает формальный процесс и процедуру проверки процесса обновления ключа после каждого обновления и когда корпорация ICANN начнет проводить регулярные теоретические учения для тестирования и ознакомления участников с процессом обновления ключа.

Эту рекомендацию можно будет считать действенной, если появится возможность формальной проверки SSR процесса, посредством которого при обновлении ключа KSK корневой зоны обеспечивается сохранение средств защиты DNSSEC.

Эта рекомендация должна выполняться при каждом обновлении ключа.

B. Управление изменениями корневой зоны

Группа по анализу SSR2 обратила внимание на успехи PTI в реализации механизмов, снижающих возможность манипулирования данными TLD и корневой зоны.[119] Для управления корневой зоной используется технологическая система управления метками TLD в корневой зоне, называемая системой управления корневой зоной (RZMS). В рамках этого рабочего процесса применяется консервативный подход к управлению изменениями, поскольку каждое изменение требует проверки несколькими сторонами.[120]

Несмотря на то, что нет известных проблем безопасности и стабильности, связанных с неправильным использованием RZMS, существует возможность обычных кибератак в процессе аутентификации всех сторон, участвующих в рабочем процессе RZMS. Для общения с операторами TLD сейчас используются электронные письма с незашифрованным текстом, а для доступа к системе простая комбинация имени пользователя и пароля. Проверка подлинности запросов на изменение должна быть более строгой и предусматривать многофакторную аутентификацию (MFA) и безопасную связь (например, шифрование) при использовании электронной почты.

Сотрудники отдела выполнения функций IANA сейчас занимаются созданием RZMS нового поколения, в которой модель авторизации будет существенно переработана.[121] RZMS нового поколения должна содержать надежную и безопасную модель аутентификации и авторизации для подачи и утверждения запросов, а также дополнительные функциональные возможности, которые повысят безопасность и стабильность глобальной системы DNS, в том числе следующие:

- Обеспечение целостности и подлинности запросов на изменение данных TLD.
- Использование защищенных каналов связи на всех уровнях, включая управление запросами.
- Устойчивость к возможным обманным действиям с использованием авторитативных DNS-серверов корневой зоны и зон TLD.
- Быстрое реагирование на запросы на удаление (удаление записей NS или DS).

---

[119] Сообщение Дженнифер Брайс, отправленное группе по анализу SSR2 через лист рассылки, 27 марта 2019 года, Тема: Ответы касательно SSR DNS,https://mm.icann.org/pipermail/ssr2-review/2019-March/001569.html.

[120] Имена и номера интернета (IANA), «Процесс запроса на изменение корневой зоны», источник проверен 8 декабря 2020 года: https://www.iana.org/help/root-zone-process.

[121] PTI, «Заседание членов ccNSO — Обновление функций IANA, относящихся к именам», ICANN 60, 31 октября 2017 года, слайды 11–14: https://ccnso.icann.org/sites/default/files/field-attached/presentation-pti-members-31oct17-en.pdf.

- Рассмотрение (включая оценку комитетами SSAC и RSSAC и процесс общественного утверждения) дополнительных автоматизированных технических проверок и процедур для быстрого устранения проблем, которые могут повлиять на бесперебойное функционирование DNS TLD.
- Рассмотрение комитетами SSAC и RSSAC реализации RFC 8078 и соответствующих обновлений для автоматического обслуживания якорей доверия при делегировании DNSSEC (CDS/CDNSKEY).122

Хотя корпорация ICANN уже объявила о разработке и внедрении новой системы RZMS с более строгими требованиями к безопасности каналов связи, группа по анализу SSR2 не обнаружила никаких сведений о том, когда корпорация ICANN планирует ввести эту новую систему в эксплуатацию.

Рекомендация SSR2 № 21: Повышение безопасности связи с операторами TLD

21.1. Корпорация ICANN и PTI должны ускорить внедрение новых мер безопасности для RZMS в отношении аутентификации и авторизации запрашиваемых изменений и предоставить операторам TLD возможность воспользоваться этими мерами безопасности, в частности, MFA и шифрованной электронной почтой.

Эту рекомендацию можно будет считать выполненной, когда у корпорации ICANN и PTI будет RZMS нового поколения с надежной и безопасной моделью аутентификации и авторизации для подачи и утверждения запросов, а также дополнительными функциональными возможностями, которые повысят безопасность и стабильность глобальной системы DNS.

Эту рекомендацию можно будет считать действенной, если корпорация ICANN за счет усовершенствованных процедур управления идентификационной информацией снизит вероятность возникновения проблем для безопасности и стабильности, связанных с неправильным использованием RZMS.

C. Данные корневой зоны и реестры IANA

Реестры IANA содержат важные параметры, которые указаны в документах RFC, подготовленных Инженерной проектной группой интернета (IETF), Инженерной исследовательской группой интернет-технологий (IRTF) и в рамках независимого потока.[123] Доступность и целостность этих реестров параметров имеют первостепенное значение и должны быть четко продемонстрированы сообществу с помощью формальных ключевых показателей эффективности (KPI). В настоящее время показатели доступности услуг, предоставляемых корпорацией ICANN, недоступны сообществу. Заинтересованным сторонам такая информация необходима для оценки аспектов SSR этих услуг в динамике по времени.

[122] О. Гудмундссон и П. Воутерс, «Управление записями DS из родительской зоны через CDS/CDNSKEY», RFC 8078, DOI 10.17487/RFC8078, марта 2017 года: <https://www.rfc-editor.org/info/rfc8078>.
[123] IANA, «Регистрационные процедуры для протоколов», 3 января 2020 года: https://www.iana.org/help/protocol-registration.

Корпорация ICANN также может счесть создание KPI для корневой зоны DNS (включая DNSSEC, доступность, целостность, злоупотребления и т. д.) наиболее эффективным способом измерения, отслеживания и передачи сообществу сведений о динамике данных, касающихся корневой зоны.

Полезными KPI могут оказаться, в частности:

- Задержка распространения изменений корневой зоны по зеркалам.
- Корневая зона DNS (включая DNSSEC, доступность, целостность и т. д.), чтобы третьи стороны могли отслеживать различные аспекты SSR.
- Показатели, демонстрирующие размер, рост и состав реестров IANA, а также доступность этих реестров в глобальной сети.

Рекомендация SSR2 № 22: Измерение качества услуг

22.1. Для каждой службы, находящейся в сфере управления корпорации ICANN, включая корневую зону и службы, связанные с gTLD, а также реестры IANA, корпорация ICANN должна создать список статистических данных и показателей, отражающих рабочее состояние (например, доступность и скорость реагирования) этой службы, и опубликовать каталог этих служб, наборов данных и показателей на одной странице сайта icann.org, например, на странице Платформы для открытых данных. Корпорация ICANN должна произвести измерения для каждой из этих услуг в виде сводных данных как за предыдущий год, так и в долгосрочном плане (для иллюстрации базового поведения).

22.2. Корпорация ICANN должна ежегодно запрашивать у сообщества отзывы об этих показателях. Эти отзывы следует рассматривать, публично резюмировать после каждого отчета и включать в последующие отчеты. Данные и связанные с ними методологии, используемые для измерения результатов этих отчетов, следует архивировать и делать общедоступными, чтобы способствовать воспроизводимости.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN определит показатели рабочего состояния доступных сообществу служб, которые поддерживает корпорация ICANN.

Эту рекомендацию можно будет считать действенной, как только сообщество увидит, что транспарентность деятельности корпорации ICANN в области SSR повысилась.

D. Шифрование DNS

Группа по анализу SSR2 изучила две темы в области шифрования DNS. Во-первых, группа исследовала переход от алгоритма RSA к алгоритму эллиптической криптографии для подписей DNSSEC. Во-вторых, группа исследовала необходимость перехода к алгоритму постквантовой цифровой подписи.[124] Чтобы идти в ногу с достижениями в области традиционных вычислительных технологий, размер ключей RSA должен со временем увеличиваться. В качестве альтернативы DNSSEC может перейти от RSA к эллиптической криптографии (ECC), которая обеспечивает такую же безопасность с меньшими по размеру открытыми ключами и подписями. Кроме того, есть опасение, что изобретение крупномасштабного квантового компьютера позволит взламывать как RSA,

[124] Подробнее об исследованиях группы см. «Приложение G: Криптография».

так и ECC. Прежде чем появится крупномасштабный квантовый компьютер, DNSSEC необходимо перевести на квантово-безопасный алгоритм. У корпорации ICANN и PTI нет положений в DPS, предусматривающих такой переход.

Корпорация ICANN — не единственная организация, которой нужно принять во внимание ожидаемые достижения в области криптографии. Группы, занимающиеся разработкой отраслевых стандартов, также готовятся к постквантовому будущему. Самым известным направлением деятельности является проект постквантовой криптографии NIST, который в сотрудничестве с исследователями из разных стран мира ведет разработку новых криптографических примитивов, неуязвимых для атак со стороны квантовых компьютеров.[125] Можно ожидать, что на осуществление этого проекта уйдет еще несколько лет, прежде чем итоговые алгоритмы будут готовы к стандартизации, но он, безусловно, идет полным ходом.

Между тем исследователи сходятся во мнении, что в постквантовую эру безопасность будет обеспечена с помощью подписей на основе хэш-функций. Оперативная рабочая группа по исследованию интернета (IRTF) определила эти алгоритмы подписи в своей исследовательской группе Crypto Forum (CFRG), используя небольшие закрытые и открытые ключи с низкими вычислительными затратами.[126] Однако подписи имеют довольно большой размер, а закрытый ключ позволяет создать только конечное количество подписей. Эти две особенности делают подписи на основе хэш-функций нежелательными в среде DNSSEC.

В документации корпорации ICANN не учитывается необходимость замены текущего алгоритма. Следовательно, корпорация ICANN не готова к ожидаемым достижениям в области алгоритмов криптографических ключей цифровых подписей.

Рекомендация SSR2 № 23: Обновление алгоритма

23.1. Специалисты PTI должны обновить Заявление о практике использования DNSSEC (DPS), чтобы предусмотреть смену алгоритма цифровой подписи, в том числе ожидаемый переход от алгоритма цифровой подписи RSA к другим алгоритмам или к будущим постквантовым алгоритмам, которые обеспечивают такие же или более высокие показатели безопасности и сохранение или повышение отказоустойчивости DNS.

23.2. Поскольку обновление алгоритма DNSKEY корневой зоны — очень сложный и требующий особого внимания процесс, PTI следует сотрудничать с другими партнерами по корневой зоне и мировым сообществом при подготовке согласованного плана будущего обновления алгоритма DNSKEY корневой зоны с учетом уроков, извлеченных из первого обновления KSK в 2018 году.

Эту рекомендацию можно будет считать выполненной, когда PTI обновит DPS, чтобы обеспечить смену алгоритма цифровой подписи, и разработает согласованный план будущих обновлений алгоритма DNSKEY корневой зоны.

[125] Национальный институт стандартов и технологий (NIST), Лаборатория информационных технологий, Центр ресурсов компьютерной безопасности, «Постквантовая криптография», создано 03 января 2017 года, обновлено 23 ноября 2020 года: https://csrc.nist.gov/projects/post-quantum-cryptography.
[126] IRTF, Исследовательская группа Crypto Forum: https://irtf.org/cfrg.

Эту рекомендацию можно будет считать действенной, если корпорация ICANN подготовится к использованию более современных алгоритмов для подписания ключей, включая любое увеличение длины ключа и сроков обновления ключа.

5. Резервный оператор регистратуры (EBERO)

Провайдер EBERO выступает в качестве особого компонента инфраструктуры аварийного восстановления и играет важную роль в предоставлении необходимых систем и операционных мощностей, принимая на себя выполнение всех важнейших функций прекратившей работу регистратуры gTLD.

Провайдера EBERO привлекается на временной основе при возникновении опасности того, что оператор регистратуры gTLD окажется не в состоянии выполнять важнейшие функции регистратуры.[127] Этот процесс обеспечивает доступность функций оператора gTLD, обеспечивает защиту владельцев доменов и создает дополнительный уровень защиты DNS. Как указано в различных широко известных стандартах, таких как ISO 22301, руководство по передовой практике требует, чтобы процессы аварийного восстановления регулярно тестировались (см. рекомендацию SSR2 № 7: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления).

Группе по анализу SSR2 не удалось проверить, координировала ли корпорация ICANN необходимое сквозное тестирование всего процесса EBERO, описанного в документе «Руководство по единому порядку переноса данных — версия 3».[128] Корпорация ICANN и поставщики услуг EBERO протестировали отдельные компоненты этого процесса (для одного теста использовался домен .doosan, а для второго — .mtpc), причем последний тест был проведен в 2017 году.[129] Группа по анализу SSR2 нашла результаты этих тестов в материалах заседаний, а не на какой-либо отдельной веб-странице ICANN.[130] Группа по анализу признает, что подробности сквозного тестирования процесса EBERO выходят за рамки проверки SSR; однако возможность убедиться, что такие тесты проводились, и ознакомиться с их результатами имеет важное значение в контексте транспарентности для сообщества.

Также стоит отметить, что, хотя процессы EBERO задокументированы в Руководстве по единому порядку переноса данных, данный документ было чрезвычайно трудно найти, поскольку это составная часть соглашения с EBERO.

---

[127] ICANN, «Резервный оператор регистратуры», дата не указана: https://www.icann.org/resources/pages/ebero-2013-04-02-en.

[128] ICANN, «Соглашение с резервным оператором регистратуры», август 2019 года: https://www.icann.org/en/system/files/files/cira-ebero-15aug19-en.pdf.Примечание: см. Приложение B — Единый порядок переноса данных.

[129] ICANN, отчет о проверке EBERO, презентация на Tech Day ICANN55, 7 марта 2016 года: https://meetings.icann.org/en/marrakech55/schedule/mon-tech/presentation-ebero-07mar16-en.pdf; Кевин Мэрфи «Второй резервный оператор регистратуры проверен на недействующем домене-бренде», Domain Incite, 27 апреля 2017 года: http://domainincite.com/21724-second-emergency-registry-tested-with-dead-dot-brand.

[130] Франциско Ариас, «Проверки EBERO», презентация на Tech Day ICANN60, 30 октября 2017 года: https://ccnso.icann.org/sites/default/files/field-attached/presentation-ebero-exercises-30oct17-en.pdf.

Рекомендация SSR2 № 24: Повышение транспарентности и сквозного тестирования процесса EBERO

24.1. Корпорация ICANN должна координировать сквозное тестирование всего процесса EBERO через заранее определенные промежутки времени (не реже одного раза в год), используя план тестирования, который содержит наборы данных, используемые для тестирования, последовательность выполнения и крайние сроки, и заранее согласовывается со сторонами, связанными с ICANN договорными обязательствами, чтобы обеспечить проверку всех ветвей обработки исключений и опубликовать результаты.

24.2. Корпорация ICANN должна упростить поиск Руководства по единому порядку переноса данных, опубликовав ссылки на сайте EBERO.

Эту рекомендацию можно будет считать выполненной, когда корпорация ICANN будет координировать ежегодное сквозное тестирование всего процесса EBERO, предоставляя общедоступную документацию с его результатами.

Эту рекомендацию можно будет считать действенной, если корпорации ICANN удастся подтвердить, что процесс EBERO функционирует должным образом, защищая владельцев доменов и обеспечивая дополнительный уровень защиты DNS.

Приложение A. Дополнительные предложения

В процессе проверки группа по анализу SSR2 обратила внимание на несколько областей, в которых изменения повысят эффективность работы и возможности будущих групп по анализу. Хотя эти вопросы выходят за рамки мандата группы по анализу, мы надеемся, что корпорация ICANN рассмотрит нижеследующие предложения в качестве вклада в проведение будущих проверок. Они перечислены в порядке приоритета.

Предложение № 1

Корпорации ICANN следует реализовать функцию онлайн-отслеживания хода выполнения каждой рекомендации каждой группы по анализу. Благодаря обеспечению наглядности всего процесса выполнения рекомендации в режиме реального времени, все сообщество сможет наблюдать за деталями выполнения и направлять отзывы обо всех недостатках. Чтобы добиться желаемой транспарентности и наглядности, требуется более высокая детализация планов выполнения и прогресса, как сегодня можно увидеть на веб-страницах, посвященных выполнению рекомендаций CCT.[131] Группа по анализу SSR2 считает, что рекомендация № 1 не потребовалась бы, если бы указанная функция была предусмотрена для выполнения рекомендаций группы по анализу SSR1. Кроме того, опираясь на концепцию куратора выполнения рекомендаций CCT, корпорация ICANN должна предоставлять ежеквартальные отчеты членам группы по анализу, которая подготовила рекомендации, чтобы они регулярно сообщали, приводит ли выполнение рекомендаций к ожидаемым результатам. Это также позволит избежать вопросов от следующей группы по анализу, когда она будет оценивать выполнение рекомендаций. Группа по анализу SSR2 считает, что процесс оценки рекомендаций группы по анализу SSR1 был бы простым, если бы такая функция существовала до начала работы группы по анализу SSR2.

Предложение № 2

Чтобы избежать недопонимания и несбывшихся ожиданий, корпорации ICANN следует разработать четкий задокументированный процесс получения ресурсов для групп по анализу на договорной основе, в том числе этапы и моменты одобрения группой по анализу. Каждой группе по анализу потребуется технический писатель, поэтому корпорация ICANN должна предоставить группе по анализу такого специалиста, начиная с самого первого собрания группы.

Предложение № 3

Чтобы способствовать исследованию сразу после окончания периода общественного обсуждения и «*удовлетворить растущие потребности в инклюзивности, подотчетности и транспарентности*», как указано в стратегической задаче 2.1, группа по анализу SSR2 предлагает корпорации ICANN создать лист рассылки для объявлений о периодах общественного обсуждения. В настоящее время бывает довольно трудно найти

[131] ICANN, «Принятые рекомендации Группы по анализу конкуренции, потребительского доверия и потребительского выбора (CCT-RT) — план выполнения рекомендаций и дальнейшие действия», источник проверен 19 декабря 2020 года: https://www.icann.org/public-comments/cct-rt-implementation-plan-2019-09-11-en.

информацию об общественном обсуждении. Принятие этого предложения послужит повышению осведомленности подписчиков на лист рассылки о периодах общественного обсуждения без дополнительных усилий. Наличие таких сообщений позволит членам будущих групп по анализу и другим заинтересованным лицам без труда находить информацию с помощью доступных инструментов поиска в почтовом архиве.

Группа по анализу SSR2 предлагает, чтобы корпорация ICANN отправляла в этот лист рассылки по крайней мере три сообщения за период общественного обсуждения. Первое сообщение следует отправить в начале периода общественного обсуждения, и оно должно содержать постоянный URL-адрес соответствующего проекта документа. Второе сообщение следует отправить сразу после закрытия периода общественного обсуждения, и оно должно содержать постоянный URL-адрес совокупности представленных комментариев. Третье сообщение должно указывать, был ли достигнут консенсус, и если да, то оно должно содержать постоянный URL-адрес итогового документа. Другие сообщения, например о продлении периода общественного обсуждения, также могут принести пользу. Кроме того, группа по анализу SSR2 предлагает, чтобы корпорация ICANN создала веб-страницу со списком всех объявлений о сборе комментариев, содержащую ссылки на страницы с соответствующими документами.

Предложение № 4

Чтобы обеспечить транспарентное обсуждение вопросов безопасности, корпорации ICANN следует рассмотреть возможность создания открытой платформы обеспечения доступности, целостности и безопасности информации для обмена сведениями о безопасности и злоупотреблениях, чтобы сделать информацию более динамичной и повысить оперативность ее раскрытия.

Приложение B. Определения и аббревиатуры

Определения

Оценка такого рода требует одинакового понимания важнейших терминов, относящихся к этому анализу. Группа по анализу SSR2 с самого начала использовала в своей работе следующие определения:[132]

- Злоупотребление: См. «неправильное использование DNS» ниже
- Компрометация рабочей электронной почты (BEC): вид мошенничества, направленного против компаний, где учетные записи электронной почты сотрудников подделываются либо компрометируются для совершения мошеннических банковских переводов.
- Ботнет: сеть компьютеров, зараженных вредоносным ПО и контролируемых как группа без ведома владельцев этих компьютеров.
- Мошенничество с цифровыми сертификатами: злоумышленник взламывает центр сертификации (ЦС), чтобы создать и получить поддельные сертификаты для проведения дальнейших атак; злоумышленник также может использовать поддельные сертификаты для аутентификации под именем другого человека или системы или для подделки цифровых подписей.
- Распределенная атака типа «отказ в обслуживании» (DDoS): злонамеренная попытка нарушить работу целевого сервера, службы или сети путем подавления целевого объекта или окружающей его инфраструктуры потоком сетевого трафика из нескольких (распределенных) источников.
- Неправильное использование DNS: умышленное использование универсальных идентификаторов, предоставленных DNS, не по назначению с целью создания инфраструктуры киберпреступности и отправки пользователей на сайты, позволяющие совершать другие виды преступлений, такие как эксплуатация детей, нарушение прав на интеллектуальную собственность и мошенничество.
- Система доменных имен (DNS): DNS — это распределенная онлайн-служба базы данных, которая переводит легко запоминающиеся доменные имена в числовые адреса интернет-протокола (IP-адреса); например, DNS преобразует www.icann.org в 192.0.34.65 (спецификация содержится в RFC 1034 и 1035).
- Концепция безопасности, стабильности и отказоустойчивости систем идентификаторов (IS-SSR): периодически обновляемый документ где «описаны роль и рамки компетенции ICANN как организации, поддерживающей единый, всемирный и функционально совместимый интернет, а также проблемы, стоящие перед системами уникальных идентификаторов интернета».
- Вредоносное ПО: программное обеспечение, созданное специально для нарушения работы, повреждения или несанкционированного доступа к компьютерной системе.
- Фишинг: мошенническая попытка получить конфиденциальную информацию путем отправки электронного сообщения от имени заслуживающей доверия организации.
- Программа-вымогатель: вредоносное ПО, предназначенное для блокировки доступа к компьютерной системе до выплаты некоторой денежной суммы.

[132] ICANN, «Роль и круг обязанностей в области SSR», источник проверен 27 декабря 2019 года: https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en.

- Отказоустойчивость: способность системы уникальных идентификаторов эффективно выдерживать и переносить атаки злоумышленников и прочие деструктивные события без нарушения или приостановки обслуживания.
- Мошенничество: фальсификация реального бизнеса или инвестиционной возможности, предназначенная для наживы.
- Безопасность: способность защищать уникальные идентификаторы интернета и предотвращать их неправомерное использование.
- Угроза безопасности: к числу наиболее серьезных угроз безопасности относятся фишинг, мошенничество, вредоносное ПО, программы-вымогатели, спам, DDoS-атаки, мошенничество с цифровыми сертификатами и ботнеты.
- Спам: нежелательная массовая рассылка сообщений по электронной почте.
- Стабильность: способность обеспечивать ожидаемое функционирование системы идентификаторов и доверие к ней со стороны пользователей уникальных идентификаторов.
- Уникальные идентификаторы: техническая миссия ICANN включает содействие в координации распределения уникальных идентификаторов интернета на общем уровне: а именно, доменных имен верхнего уровня, выделяемых региональным интернет-регистратурам блоков адресов интернет-протокола (IP-адресов) и номеров автономных систем (AS), а также параметров протокола в соответствии с указаниями IETF.

Аббревиатуры

- AS: автономная система
- BC: непрерывность бизнеса
- CISO: директор по информационной безопасности
- CSO: директор по безопасности
- CZDS: Централизованная служба файлов корневой зоны
- DAAR: Платформа отчетности о случаях злоупотребления доменами
- DNS: система доменных имен
- DNSSEC: расширения безопасности DNS (согласно спецификации в RFC 4033, RFC 4034 и RFC 4035)
- DoH: DNS по HTTPS
- DoT: DNS по TLS
- DPS: заявление о практике использования DNSSEC
- DR: восстановление работоспособности после аварии
- DURZ: зона, которая заведомо не может быть криптографически проверена
- EBERO: резервный оператор регистратуры
- EPDP: ускоренный процесс формирования политики
- FSM: конечный автомат
- gTLD: домен верхнего уровня общего пользования
- GNSO: Организация поддержки доменов общего пользования
- HTTP: протокол передачи гипертекста
- HTTPS: протокол защищенной передачи гипертекста
- IANA: Администрация адресного пространства интернета
- IETF: Инженерная проектная группа интернета
- IMRS: корневой сервер, находящийся под управлением ICANN
- IP: интернет-протокол
- IRTF: Инженерная исследовательская группа интернет-технологий
- Концепция IS-SSR: концепция безопасности, стабильности и отказоустойчивости систем идентификаторов интернета
- ISMS: система управления информационной безопасностью

- ISO: Международная организация по стандартизации
- ITIL: библиотека ИТ-инфраструктуры
- KSK: ключ для подписания ключей
- NCAP: проект анализа доменных коллизий
- NIST: Национальный институт стандартов и технологий США
- OCTO: офис технического директора
- PII: личные данные
- PTI: Организация по открытым техническим идентификаторам
- RDS: служба каталогов регистрационных данных
- RAA: соглашение об аккредитации регистраторов
- RAPWG: Рабочая группа по политике в сфере противодействия злоупотреблениям при регистрации
- RDAP: протокол доступа к регистрационным данным
- RSSAC: Консультативный комитет системы корневых серверов
- SADAG: статистический анализ неправильного использования DNS в gTLD
- SMART: конкретный, измеримый, назначаемый, актуальный и отслеживаемый
- SOP: стратегический и операционный планы
- SSAC: Консультативный комитет по безопасности и стабильности
- SSAE: положение о стандартах аттестационных проверок
- SSR: безопасность, стабильность и отказоустойчивость
- SSR1: первый процесс проверки SSR
- SSR2: второй процесс проверки SSR
- TLS: защита транспортного уровня

Приложение C. Процесс и методология

Процесс и методология рассмотрения рекомендаций SSR1

В основе описанного ниже процесса оценки, которому следовала группа по анализу SSR2, лежат брифинги и обсуждения с персоналом корпорации ICANN, ответственным за выполнение рекомендаций, систематическое изучение значительного количества соответствующих документов ICANN и составленных корпорацией ICANN отчетов о выполнении рекомендаций, а также дополнительные исследования и собеседования.[133] Кроме того, для взаимодействия с соответствующими заинтересованными сторонами сообщества группа воспользовалась информационными заседаниями на открытых конференциях ICANN в Барселоне и Кобе. По возможности оценка была как количественной, так и качественной, в зависимости от конкретной рекомендации.

Многие рекомендации SSR1 носили общий характер и не содержали конкретики. У группы по анализу SSR2 не было полномочий на доступ к внутренней работе ICANN и ее анализ, поэтому корпорации ICANN было предложено предоставить членам группы по анализу SSR2 свои планы выполнения и доказательства успешного выполнения рекомендаций. Как в самих рекомендациях, так и в предоставленной корпорацией ICANN документации отсутствовали KPI и целевые показатели, измеримые задачи и планы выполнения. Это затрудняло измерение или отслеживание выполнения рекомендаций. Кроме того, формулировки некоторых рекомендаций оставляли возможность для различного толкования. Иногда это приводило к тому, что понимание рекомендации группой SSR2 отличалось от ее понимания персоналом корпорации ICANN.

Чтобы проинформировать о том, как были выполнены рекомендации SSR1, персонал корпорации ICANN предоставил группе в 2017 году первоначальные ответы, касающиеся выполнения каждой рекомендации. Персонал ICANN перечислил веб-страницы или документы, организовал доклады представителей различных отделов корпорации ICANN, а также в течение девяти месяцев проводил для группы брифинги на тему рекомендаций. Группа также изучила довольно много справочных документов, представляющих интерес для данной проверки. Группа провела собеседования с персоналом корпорации ICANN, запросила дополнительную информацию и использовала вклад соответствующих заинтересованных сторон и собственные исследования для выполнения дополнительного анализа, где это было необходимо.

Получив от корпорации ICANN ответы на поставленные вопросы и завершив исследования и комплексную проверку в меру своих возможностей, группа подготовила во второй половине 2018 года предварительные оценки выполнения каждой рекомендации, которые обсуждались в интернете, на еженедельных телеконференциях группы и во время очных совещаний. Группа отредактировала текст по мере необходимости и утвердила выводы и результаты по каждой рекомендации SSR1, чтобы включить их в проект отчета группы SSR2 наряду с утвержденными протоколами консенсуса группы и возражениями меньшинства, когда они имели место.

После обсуждения в интернете и на телеконференциях, а также после нескольких циклов доработки, группа решила структурировать свой проект оценки в соответствии с

[133] Вики-страница группы по анализу SSR2 ICANN: https://community.icann.org/display/SSR/SSR2+Review. См. В частности информационные материалы и материалы брифингов.

описанной ниже методологией, в которой основное внимание уделено выполнению задачи, актуальности и необходимой дальнейшей работе:

1. Что было сделано для выполнения рекомендации?
2. Была ли рекомендация выполнена полностью?
3. Привело ли ее выполнение к ожидаемым результатам?
4. Как проводилась оценка?
5. Сохраняет ли рекомендация свою актуальность?
6. Если да, какая дополнительная работа необходима? Если нет, почему?

Первый вопрос касается того, что было сделано корпорацией ICANN для выполнения рекомендации. В ответе на второй вопрос дается оценка группой степени выполнения на «дату полного выполнения», указанную персоналом. Команда обнаружила много рекомендаций, которые, по-видимому, были выполнены лишь частично или планы их выполнения вообще отсутствовали. В этих случаях группа определила конкретные области для улучшения. В некоторых случаях было сложно установить четкие предварительные условия и цели, необходимые для успешного выполнения, из-за отсутствия планов выполнения, документации и показателей эффективности. Третий вопрос касается того, привело ли выполнение рекомендации к ожидаемым результатам и в какой степени. Четвертый вопрос касается того, как группа SSR2 проводила оценку. Читатели могут проследить, какие документы и другие доказательства были рассмотрены группой по каждой рекомендации. Кроме того, на основании пятого вопроса группа оценила актуальность каждой рекомендации в 2018 году. Наконец, группа приняла решение о том, требуют ли текущие обстоятельства дополнительной работы по выполнению этой рекомендации, что затем легло в основу набора собственных рекомендаций группы SSR2.

Процесс и методология оценки SSR ICANN, SSR DNS и будущих задач

Группа по анализу SSR2 провела ряд собеседований с персоналом корпорации ICANN.[134] Вопросы касались полноты и эффективности используемых в корпорации ICANN процессов обеспечения безопасности, а также эффективности концепции безопасности корпорации ICANN.

Группа по анализу SSR2 организовала конкретный процесс подтверждения результатов и выработки рекомендаций для рассмотрения ICANN, включающий следующее:

- Рассмотрение, анализ и обобщение соответствующей документации.
- Проведение исследований в выявленных проблемных областях.
- Проведение соответствующих собеседований по мере необходимости.
- Составление сводного документа с обоснованиями, выводами и рекомендациями.

Рабочий поток 2 был сосредоточен на проблемах SSR внутри самой корпорации ICANN, тогда как рабочий поток 3 был сосредоточен на SSR глобальных систем идентификаторов: глобальной DNS, баз данных номеров IANA (распределение IP и ASN) и реестрах протокола IANA. Группа по анализу особо рассмотрела отчеты и другие данные о рисках, угрозах и

[134] Вики-страница группы по анализу SSR2 ICANN: https://community.icann.org/display/SSR/SSR2+Review. См. В частности материалы брифингов.

неправильном использовании DNS, а затем сопоставила полученные данные с соответствующими компонентами, процедурами и принципами политики ICANN.
В рамках рабочего потока 4, касающегося будущих проблем для SSR, группа по анализу SSR2 рассмотрела текущие исследования неправильного использования DNS, влияние постоянного увеличения видов и количества устройств в DNS, новые технологии, выявленные в других рабочих потоках проблемные области, способные оказать влияние в будущем, а также официально используемые в ICANN методы анализа и смягчения угроз. Группа по анализу SSR2 признала, что этот рабочий поток зависит от новых тем в других зависимых областях. В частности, помимо общеизвестных проблем, в рамках этого рабочего потока изучалась возможность столкнуться с другими конкретными проблемами стабильности и отказоустойчивости DNS применительно к SSR ICANN и SSR DNS.

Приложение D. Выводы, относящиеся к рекомендациям SSR1

Данный раздел содержит подробную оценку каждой рекомендации SSR1. Здесь рассматриваются конкретные меры по их выполнению и соответствующие проблемы, а также соображения группы касательно дальнейшей работы. Группа по анализу SSR2 обратила внимание на следующие неоднократно возникающие проблемы:

1. Отсутствуют индикаторы, показатели и цели, которые позволили бы сообществу и корпорации ICANN отслеживать и понимать ситуацию и собственную деятельность в сфере безопасности.

2. Отсутствуют доступные для всеобщего ознакомления факты, определения и процедуры, что препятствует наблюдению за деятельностью в области SSR. Это приводит к отсутствию ясности в отношении того, какая деятельность осуществляется, когда, кем и как.

3. Отсутствует проверка сообществом и подотчетность, что лишает сообщество ICANN возможности вносить свой вклад по вопросам SSR.

4. В настоящее время у корпорации ICANN нет всеобъемлющей стратегии, конкретных целей или четкой и всесторонней политики в области SSR. В отсутствие конструктивной стратегии в области SSR и интегрированного управления безопасностью и рисками (например, политики, процедур, стандартов, базовых показателей, руководящих принципов) обязанности, связанные с SSR, не возлагаются, а их выполнение не измеряется и не отслеживается, что приводит к недостаточной транспарентности и подотчетности.

Рекомендация SSR1 № 1

«ICANN должна опубликовать единое, четкое и последовательное заявление о своем круге обязанностей по обеспечению SSR и выполнению ограниченной технической миссии. ICANN должна получить и учесть комментарии общественности, чтобы это заявление было принято на основе консенсуса».

Заключение SSR2: Эта рекомендация остается актуальной, поскольку она была частично выполнена, но не был достигнут в полной мере ожидаемый эффект от наличия основанного на консенсусе, четкого и последовательного заявления, описывающего круг обязанностей корпорации ICANN в области SSR и техническую миссию.

Обоснование:

- Группа обнаружила, что такое заявление существует и корпорация ICANN обновила его под влиянием проверки сообщества (но больше не поддерживает).[135] Несмотря

[135] «Роль и круг обязанностей в области SSR», https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en; Группа по анализу безопасности, стабильности и отказоустойчивости DNS — проект отчета: отчет о результатах общественного обсуждения», последняя редакция от 18 мая 2012 года: http://www.icann.org/en/system/files/files/report-comments-ssr-rt-draft-report-18may12-en.pdf.

на наличие этого заявления и его четких определений «безопасности, стабильности и отказоустойчивости», использование этих определений остается непоследовательным. В ходе разговоров с членами группы, имеющими доступ к тексту соглашений корпорации ICANN с различными сторонами, связанными договорными обязательствами, выяснилось, что в соглашениях корпорации ICANN используются другие определения понятий «безопасность» и «стабильность».[136]

- Не были представлены показатели, позволяющие оценить, привело ли выполнение рекомендации к ожидаемым результатам в виде предоставления четкой и последовательной информации о круге обязанностей в области SSR и границах технической миссии. Учитывая различные способы использования термина «SSR» в ICANN, выполнение рекомендации не привело к единому определению, как ожидала группа по анализу SSR1.

Рекомендация SSR1 № 2

«Определение и пути реализации круга обязанностей ICANN по обеспечению SSR и выполнению ограниченной технической миссии следует пересматривать для сохранения консенсуса и содействия получению предложений от сообщества. Этот процесс должен регулярно повторяться, возможно, во взаимосвязи с циклом будущих проверок SSR».

Заключение SSR2: Эта рекомендация остается актуальной и не была полностью выполнена. Не был достигнут ожидаемый эффект от регулярного общественного анализа круга обязанностей корпорации ICANN в области SSR и соответствующей технической миссии.

Обоснование:

- Группа по анализу SSR2 не нашла свидетельств того, что проводится регулярный анализ круга обязанностей в сфере SSR. Начиная с 2013 года, отсутствует возможность комментировать заявление о круге обязанностей и миссии.

Рекомендация SSR1 № 3

«После опубликования согласованного заявления о своем круге обязанностей по обеспечению SSR и выполнению ограниченной технической миссии ICANN должна использовать во всех материалах единообразную терминологию и описания из данного заявления».

Заключение SSR2: Эта рекомендация все еще актуальна, но не была полностью выполнена. Ожидаемый эффект от использования в материалах по SSR согласованной терминологии и набора описаний не был достигнут.

См. рекомендацию SSR2 № 13: Повышение транспарентности и подотчетности сообщений о нарушениях. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

[136] См. также раздел 7.3 базового соглашения для новых gTLD https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html по сравнению с определениями безопасности и стабильности, используемыми корпорацией ICANN: https://www.icann.org/groups/ssac

Обоснование:

- В июле 2013 года в блоге была опубликована доступная всему сообществу статья, где представлен список используемых корпорацией ICANN терминов в области безопасности; однако эти определения, похоже, не всегда последовательно включаются в другие документы, имеющие отношение к SSR.[137]
- В отчете персонала корпорации ICANN по этой рекомендации указано, что персонал постоянно будет добавлять важные термины в общедоступный глоссарий корпорации ICANN в рамках стратегического и операционного плана (SOP); по мере развития деятельности в области SSR терминология и описания будут обновляться в рамках SOP. Однако глоссарий (найденный в вышеупомянутой статье) не обновлялся с февраля 2014 года.

Рекомендация SSR1 № 4

«ICANN должна документально оформить и четко определить характер своих взаимоотношений в сфере SSR в рамках сообщества ICANN, чтобы создать единую отправную точку для понимания взаимозависимости между организациями».

Заключение SSR2: Эта рекомендация остается актуальной, но не была полностью выполнена. Намеченный эффект от предоставления открытого и транспарентного ресурса, описывающего взаимоотношения корпорации ICANN в области SSR, не был достигнут.

См. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Персонал корпорации ICANN составил для группы по анализу SSR2 документ, в котором отслеживаются роли и обязанности ICANN, связанные с SSR, и перечисляются все организации, с которыми у корпорации ICANN когда-либо были официальные отношения.138 Этот документ содержит конкретные ссылки на документы, лежащие в основе таких взаимоотношений в каждом случае, и описание аспектов SSR, касающихся этих отношений. Однако многие ссылки, перечисленные в этом документе, не работают. В документе часто упоминаются аспекты отношений SSR со статусом «неизвестно».

Рекомендация SSR1 № 5

«ICANN должна использовать определение своих взаимоотношений в сфере SSR для сохранения эффективных рабочих схем и для демонстрации того, как с помощью этих отношений достигается каждая цель в сфере SSR.»

Заключение SSR2: Эта рекомендация все еще актуальна, но не была полностью выполнена. Группе по анализу не удалось определить, достигла ли корпорация ICANN предполагаемого воздействия эффективных рабочих схем применительно к обеспечению достижения каждой цели в области SSR.

---

[137] ICANN, статья «Терминология ICANN в сфере безопасности», последняя редакция от 8 июля 2013 года: https://www.icann.org/news/blog/icann-s-security-terminology.

[138] «Отношения в сфере SSR», ICANN, 23 января 2017 года: https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf.

См. рекомендацию SSR2 № 3: Повышение транспарентности бюджета, связанного с SSR. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Группа ожидала, что концепция IS-SSR будет содержать информацию о том, как ключевые взаимоотношения, указанные в рекомендации SSR1 № 4, используются для достижения целей в области SSR; однако такая информация не является легкодоступной.[139]
- Группе SSR2 не хватало информации, чтобы оценить конструктивность рабочих отношений.

Рекомендация SSR1 № 6

«ICANN должна опубликовать документ с подробным описанием функций и обязанностей SSAC и RSSAC, чтобы четко разграничить деятельность этих двух групп. ICANN должна стремиться к выработке единого мнения по данному вопросу в обеих группах с учетом истории и обстоятельств их создания. ICANN должна обсудить аспекты обеспечения обеих групп надлежащими ресурсами, в соответствии с возложенными на них обязанностями».

Заключение SSR2: Эта рекомендация все еще актуальна, но не была выполнена. Корпорация ICANN не достигла ожидаемого эффекта от четкого определения функций SSAC и RSSAC для всех заинтересованных сторон.

Обоснование:

- Функции и обязанности SSAC и RSSAC зафиксированы в документе.[140] Однако этот общедоступный документ по-прежнему помечен как «ПРОЕКТ НА РАССМОТРЕНИИ». Похоже, что работа над этой рекомендацией была начата, однако завершилась без рассмотрения результатов организационных проверок SSAC и RSSAC. Даже если консенсус и был достигнут, группе по анализу SSR2 не удалось найти итоговый документ.
- Документ составлен на основе Устава ICANN, действовавшего до передачи координирующей роли в исполнении функций IANA. Разделы Устава, где описаны SSAC и RSSAC, в основном не претерпели изменений, но RSSAC теперь непосредственно отвечает за реагирование «на запросы Правлением информации или мнения». Обновление не устранило возможность пересечения функций и обязанностей SSAC и RSSAC в Уставе ICANN:

  > *«Роль SSAC состоит в консультировании сообщества и Правления ICANN по вопросам, связанным с безопасностью и целостностью систем распределения имен и адресов интернета;*
  >
  > *Роль RSSAC состоит в консультировании сообщества и Правления ICANN по вопросам, связанным с функционированием, администрированием, безопасностью и целостностью системы корневых серверов интернета».*

[139] Тот же источник.

[140] ICANN, «ПРОЕКТ НА РАССМОТРЕНИИ: Функции и обязанности Консультативного комитета по безопасности и стабильности и Консультативного комитета системы корневых серверов ICANN», 5 марта 2015 года: https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf.

Рекомендация SSR1 № 7

«ICANN должна на основе своей текущей концепцию SSR сформулировать четкий список задач и установить приоритеты для своих инициатив и видов деятельности в соответствии с этими задачами».

Заключение SSR2: Эта рекомендация остается актуальной и была частично выполнена. Ожидаемый эффект от наличия четких, публично рассмотренных целей SSR и соответствующих усилий по установлению приоритетов не был достигнут.

См. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками, и рекомендацию SSR2 № 3: Повысить транспарентность бюджета, связанного с SSR. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:

- Сведения о деятельности в области SSR регулярно предоставляются в рамках стратегических и операционных планов (SOP), в том числе в регулярных отчетах ICANN по управлению портфелем проектов и ежеквартальных отчетах по SSR.[141] SOP составлялись на основе концепции IS-SSR, которая определяет приоритеты, цели и действия в области SSR. Однако разработка этой концепции прекращена, вследствие чего возникает вопрос: каким образом в планах SOP отражается деятельность в области SSR. Неясно, какова процедура обновления документов, относящихся к SSR, поскольку последняя редакция концепции IS-SSR была опубликована в 2016 году.[142]
- Концепция IS-SSR давала сообществу возможность высказывать свое мнение при определении стратегии в сфере SSR. Корпорация ICANN прекратила работу над этой концепцией, что недопустимо ограничивает возможность сбора мнений всех групп заинтересованных сторон сообщества ICANN о подходе корпорации ICANN к деятельности по обеспечению SSR.
- По-видимому, стратегическое планирование по вопросам безопасности, стабильности и отказоустойчивости сосредоточено в руках офиса технического директора (OCTO), и с учетом наличия SOP группа по анализу подтвердила, что планирование деятельности в сфере SSR осуществляется на уровне OCTO. Однако уровень детализации и планирования, предусмотренный в этой рекомендации, не предполагает публичного обсуждения с равным участием всех заинтересованных сторон корпорации ICANN.

Рекомендация SSR1 № 8

«ICANN должна продолжить уточнение задач своего стратегического плана, в частности, задачи сопровождения и поддержания работоспособности DNS. Необходимо обеспечить полную согласованность концепции и стратегического плана».

Заключение SSR2: Хотя эта рекомендация на сегодняшний день сохраняет свою актуальность и была частично выполнена, ее выполнение не привело к ожидаемому

[141] ICANN, «Стратегический план ICANN на 2021–2025 финансовые годы», дата не указана: https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf; Дейв Писцителло «Отчеты о деятельности по обеспечению SSR систем идентификаторов», блог ICANN, последняя редакция от 21 января 2015 года: https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

[142] ICANN, Концепция IS-SSR на 2015–2016 ФГ: https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

результату, который заключается в обеспечении более четкой связи между стратегией обеспечения SSR и операционной деятельностью.

См. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками, и рекомендацию SSR2 № 3: Повысить транспарентность бюджета, связанного с SSR. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:

- Документы, доступные на главной странице выполнения рекомендаций по итогам SSR1, указывают на то, что руководящие указания по SSR отражены и рассмотрены в соответствующих отчетах, стратегиях и процедурах.[143] Однако в имеющихся отчетах недостаточно информации о деятельности в области SSR и не хватает подробностей, касающихся реализации и выполнения мероприятий по обеспечению SSR.
- В стратегическом и операционном планах не указываются виды деятельности, приоритеты и расходы, связанные с обеспечением SSR. Важно отметить, что предусмотренные SSR1 механизмы были заменены другими организационными и процедурными инструментами, что усложняет как оценку, так и выполнение рекомендаций.

Рекомендация SSR1 № 9

«ICANN должна оценить возможности сертификации соответствия своих эксплуатационных обязанностей общепринятым международным стандартам (например, ITIL, ISO и SAS-70). ICANN должна опубликовать четкий оперативный план такой сертификации».

Заключение SSR2: Эта рекомендация остается актуальной. Группе по анализу SSR2 не удалось определить, была ли эта рекомендация полностью выполнена и был ли достигнут ожидаемый эффект, поскольку в исходной рекомендации отсутствовала необходимая конкретная информация о том, какую сертификацию или сертификаты следует получить корпорации ICANN и о том, какие конечные цели преследовались.

См. рекомендацию SSR2 № 4: Улучшить процессы и процедуры управления рисками, и рекомендацию SSR2 № 5: Соблюдать требования к соответствующим системам управления информационной безопасностью и сертификатам безопасности. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:

- В результате собеседований с персоналом корпорации ICANN было установлено, что корпорация ICANN получила несколько сертификатов для IANA, например, прошла сертификацию SOC2/3 для системы KSK корневой зоны, сертификацию SOC2 для систем обслуживания и назначения регистратур и SysTrust для внедрения DNSSEC на корневом уровне.144 Помимо деятельности, относящейся к функциям IANA, корпорация ICANN составляет отчеты на основе концепций непрерывного совершенствования в области информационных технологий и кибербезопасности,

[143] Главная вики-страница выполнения рекомендаций по итогам SSR1, последняя редакция от 22 августа 2017 года: https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home.

[144] См. рабочий документ «Вопросы и ответы SSR2», дата не указана, 6: https://community.icann.org/pages/viewpage.action?pageId=64076120.

проводит ежегодный финансовый аудит, выполняет ежегодную самооценку и проверку документации EFQM, а также консультируется со специалистами, чтобы способствовать оценке и улучшению качества работы.145
- По полученным от корпорации ICANN сведениям, весь персонал, занимающийся вопросами информационной безопасности, прошел обучение по программам SANS.146
- По полученным от корпорации ICANN сведениям, результаты внутреннего аудита передаются только Правлению ICANN.147
- Группе по анализу SSR2 не удалось найти ни одного документа, который можно было бы использовать в качестве дорожной карты сертификации процесса SSR, что делает невозможным рассмотрение этого вопроса сообществом.

Рекомендация SSR1 № 10

«ICANN не должна прекращать усилий, направленных на обеспечение соблюдения сторонами своих договорных обязательств, и должна выделить адекватные ресурсы для выполнения этой функции. ICANN также должна разработать и внедрить имеющий более четкую структуру процесс мониторинга проблем соблюдения обязательств и проведения расследований».

Заключение SSR2: Эта рекомендация остается актуальной и не была полностью выполнена. Намеченный эффект от использования адекватных ресурсов для контроля за соблюдением договоров и разработки непрерывного структурированного процесса мониторинга соблюдения не был достигнут.

См. рекомендацию SSR2 № 8: Обеспечить и продемонстрировать представление общественных интересов на переговорах со сторонами, связанными договорными обязательствами, и рекомендацию SSR2 № 9: Осуществлять мониторинг и контроль соблюдения обязательств. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:
- Оценка базируется на общедоступной информации (например, опубликованной на странице отчетов отдела по контролю исполнения договорных обязательств), а также на информации из отчета персонала ICANN, в котором были представлены доказательства выполнения рекомендации.[148] Регулярная публичная отчетность о деятельности по контролю за соблюдением требований предусмотрена в составе стратегического и операционного планов (SOP) корпорации ICANN. У корпорации ICANN есть специальная общедоступная страница для отчетов о соблюдении договорных обязательств, где ежемесячно, ежеквартально и ежегодно публикуются данные; за текущий 13-месячный период для запроса доступны десять различных отчетов; а также показатели и данные, напрямую запрашиваемые различными

[145] Тот же источник, 24.

[146] Тот же источник, 11.

[147] Тот же источник, 6.

[148] Отчет о выполнении рекомендаций SSR1 представлен здесь: https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2 (слайды 28–30); материалы брифинга SSR2-RT, относящиеся к данной рекомендации, представлены здесь: https://community.icann.org/download/attachments/66085372/SSR1%20Compliance%20Briefing%20June%202017%20v3.pdf?version=2&modificationDate=1499814488000&api=v2.

рабочими группам. В настоящее время в рамках работы по обеспечению соблюдения обязательств действует ряд программ аудита и информирования. После проверки SSR1 корпорация ICANN ввела новые должности, чтобы гарантировать выполнение целей и задач в этой области.

- Механизмы подачи и рассмотрения жалоб были обновлены путем переноса на сайт корпорации ICANN, автоматизации и запуска инструмента обработки массовых жалоб. Кроме того, персонал ICANN сообщил, что был проведен опрос для оценки удовлетворенности.[149] Корпорация ICANN начала проверку качества для обнаружения недостоверных данных в RDS. Отчеты о достоверности данных RDS составляются с момента получения в 2012 году соответствующей рекомендации группы по анализу WHOIS.
- В отчетах о соблюдении договорных обязательств за 2017 и 2016 годы мало фактов, свидетельствующих о принятии принудительных мер для обеспечения SSR, хотя базовое соглашение об администрировании нового gTLD (июль 2017 года) содержит конкретные обязательства сторон в отношении безопасности и стабильности и может способствовать дальнейшему выполнению рекомендаций.150 Группе по анализу SSR2 неясно, каким образом выполняется задача корпорации ICANN по сокращению масштабов и последствий злоупотреблений при регистрации и злонамеренного поведения за счет принятия мер по обеспечению соблюдения требований или других инициатив. Большинство вопросов, рассмотренных в отчете персонала о выполнении рекомендаций SSR1, относится к WHOIS. Кроме того, в соглашении об аккредитации регистраторов (RAA 2013) недостаточно четко сформулированы права корпорации ICANN обеспечивать в принудительном порядке соблюдение обязательств регистраторами, деятельность которых создает угрозу для услуг регистраторов и регистратур, DNS или интернета.
- Корпорация ICANN ежемесячно составляет отчеты о своей работе по обеспечению соблюдения обязательств, однако неясно, в каком объеме при этом решаются вопросы SSR.151

Рекомендация SSR1 № 11

«ICANN должна доработать и внедрить меры по обеспечению успеха новых gTLD и ускоренного ввода IDN-доменов, которые прямо относятся к задачам программ в сфере SSR, включая средства измерения эффективности механизмов предотвращения неправильного использования системы доменных имен».

Заключение SSR2: Эта рекомендация остается актуальной, но измерить степень ее выполнения невозможно. Хотя меры по противодействию неправильному использованию доменных имен были приняты, невозможно определить, привели ли эти меры к сокращению объемов использования доменов для злоупотреблений и в какой степени.

Картина DNS изменилась с тех пор, как первая группа по анализу SSR представила свои рекомендации, в частности, в результате расширения пространства новых gTLD. Однако рекомендация сделать аспекты SSR ключевым показателем успеха в управлении

[149] См. «Выполнение рекомендации SSR № 10» в сводном отчете о выполнении рекомендаций SSR1: https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2.

[150] ICANN, 31 июля 2017 года: https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf.

[151] См. «Отчеты о показателях эффективности деятельности отдела ICANN по контролю исполнения договорных обязательств»: https://features.icann.org/compliance/dashboard/report-list.

пространством DNS остается столь же, если не в больше степени, актуальной сегодня, как и в 2011 году.

См. рекомендацию SSR2 № 8: Обеспечить и продемонстрировать представление общественных интересов на переговорах со сторонами, связанными договорными обязательствами; рекомендацию SSR2 № 12: Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку, и рекомендацию SSR2 №13: Повысить транспарентность и подотчетность в области сообщений о нарушениях. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:

- Группе по анализу SSR2 не удалось найти ни одного документа с описанием критериев успеха, включая показатели эффективности механизмов противодействия неправильному использованию доменных имен, который был бы согласован с сообществом. Отсутствие измеримых критериев было также отмечено в недавнем отчете и рекомендациях группы по анализу CCT.[152]
- Спецификация 11 нового соглашения об администрировании домена верхнего уровня содержит существенные обязательства регистратур в области SSR, в том числе обязательство периодически проводить технический анализ того, не используются ли домены в TLD для создания угроз безопасности, таких как фарминг, фишинг, вредоносное ПО и ботнеты, и регулярно составлять статистические отчеты. Именно такие обязательства входят в состав типового соглашения об администрировании нового gTLD с начала приема заявок в 2012 году. У корпорации ICANN есть диаграмма соблюдения обязательств, но она измеряет количество жалоб по категориям.[153] Эти данные по-прежнему сложно отслеживать, поскольку отчетность размещена на нескольких страницах.

Рекомендация SSR1 № 12

«ICANN должна работать с сообществом над выявлением передовых практических методов в области SSR и поддерживать внедрение таких методов через договора, соглашения и меморандумы о взаимопонимании, а также другие механизмы».

Заключение SSR2: Рекомендация SSR1 № 12 не была полностью выполнена и остается особенно актуальной сегодня. Полезный эффект от выявления и внедрения передовой практики в области SSR не был достигнут.

См. рекомендацию SSR2 № 8: Обеспечить и продемонстрировать представление общественных интересов на переговорах со сторонами, связанными договорными обязательствами, и рекомендацию SSR2 № 9: Осуществлять мониторинг и контроль соблюдения обязательств. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

[152] Отчет группы по анализу CCT, 9: https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[153] См. «Отчеты отдела ICANN по контролю исполнения договорных обязательств о проделанной работе»: https://features.icann.org/compliance; «Отчеты о показателях эффективности деятельности отдела по контролю исполнения договорных обязательств»: https://features.icann.org/compliance/dashboard/report-list.

Обоснование:

- Спецификация 11 нового соглашения об администрировании домена верхнего уровня (RA) содержит существенные обязательства регистратур в области SSR. Обязательства, предусмотренные в этом RA, входят в состав типового соглашения об администрировании нового gTLD с начала приема заявок в 2012 году. Однако корпорация ICANN, по-видимому, не оценивала степень эффективности этих положений с точки зрения достижения целей рекомендации SSR1 № 12.
- Отчет под названием «Методология предотвращения атак на систему идентификаторов» датирован февралем 2017 года. В документе сформулированы предложения, подготовленные (как утверждается) «*экспертами по безопасности системы идентификаторов самой ICANN и всего сообщества*».[154] Тем не менее, неясно, какой процесс использовался при разработке передовой практики, изложенной в этом документе. В сопроводительном документе отсутствуют доказательства интеграции этой передовой практики в соглашения корпорации ICANN. В отчете нет сведений о работе до 2017 года.
- В отчете о методологии предотвращения атак на систему идентификаторов содержится неисчерпывающий перечень таких атак. Хотя после февраля 2017 года были заключены или обновлены некоторые соглашения, спецификации и меморандумы о взаимопонимании, никакие положения именно этого документа никогда не включались в состав соглашений со сторонами, связанными договорными обязательствами.
- Страница указателя ресурсов ICANN по вопросам безопасности не обновлялась с 2014 года.[155]
- В ходе проверки SSR2 не было обнаружено свидетельств того, что персонал периодически информирует SO/AC о передовой практике или предлагает выявить дополнительные передовые методы.
- В отчете персонала по этой рекомендации SSR1 указано, что работа с Комитетом по интернет-политике Антифишинговой рабочей группы (APWG), направленная на публикацию рекомендаций по защите веб-приложений и разработке ресурсов для повышения осведомленности в вопросах безопасности, завершена. От APWG поступил рекомендательный документ «Что делать, если ваш сайт взломан фишерами», но он был подготовлен до SSR1. Похоже, что на сайте ICANN отсутствует свод рекомендаций по защите веб-приложений и разработке ресурсов для повышения осведомленности в вопросах безопасности, хотя имеется отчет о 4-м глобальном симпозиуме по стабильности, безопасности и отказоустойчивости DNS, проведенном в Пуэрто-Рико в 2012 году.[156]

Рекомендация SSR1 № 13

«ICANN должна стимулировать разработку и опубликование всеми организациями поддержки рекомендованных практических методов в сфере SSR для своих членов».

[154] Лиза Файфер и Дэвид Писцителло, «Методология предотвращения атак на систему идентификаторов», информационный документ ICANN, 13 февраля 2017 года: https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf.

[155] Указатель ресурсов ICANN по вопросам безопасности, последняя редакция от 8 августа 2014 года: https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en.

[156] «Стабильность, безопасность и отказоустойчивость DNS», отчет о 4-м глобальном симпозиуме, ICANN и APWG, 25 октября 2012 года: https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf.

Заключение SSR2: Эта рекомендация остается актуальной, но не была выполнена. Ожидаемый эффект от наличия регулярного процесса публикации организациями поддержки (SO) передовой практики в сфере SSR для своих членов не был достигнут.

См. рекомендацию SSR2 № 8: Обеспечить и продемонстрировать представление общественных интересов на переговорах со сторонами, связанными договорными обязательствами, и рекомендацию SSR2 № 9: Осуществлять мониторинг и контроль соблюдения обязательств. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:

- По мнению корпорации ICANN, работа над этой рекомендацией носит постоянный характер, и отчеты о ней отражаются в SOP. Персонал ICANN контактирует со всеми SO и AC, чтобы способствовать выявлению и публикации материалов на странице репозитория передового опыта. Корпорация ICANN также сообщает, что на основе планов SOP ее персонал занимается различными видами постоянной деятельности, направленной на поощрение повсеместного использования передовой практики в сфере SSR. Группе по анализу SSR2 не удалось найти ни свидетельств того, что корпорация ICANN вела эту информационную работу, ни свидетельств того, что SO опубликовали для своих членов рекомендации по передовой практике в сфере SSR.
- Персонал корпорации ICANN сообщил, что ему неизвестно о каких-либо недавних шагах, призванных стимулировать создание организациями поддержки и консультативными комитетами репозиториев передового опыта для опубликования информации, относящейся к SSR, и заявил следующее: «*вполне вероятно, что информация от 2012 года на сайте ccTLD может быть самым последним примером опубликования информации на тему SSR организацией поддержки*».[157] Более того, персонал сообщил, что только ccNSO в настоящее время публикует передовые методы в сфере SSR для своих членов.

Рекомендация SSR1 № 14

«ICANN должна обеспечить неуклонное развитие своей информационно-разъяснительной деятельности в сфере SSR для сохранения ее актуальности, своевременности и целесообразности».

Заключение SSR2: Эта рекомендация остается актуальной, но не выполнена, и поэтому не достигнут желаемый эффект в виде повышения своевременности, актуальности и уместности информационно-разъяснительной деятельности ICANN, связанной с SSR.

См. рекомендацию SSR2 № 18: Информационное обеспечение дебатов по вопросам политики. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Интерфейс взаимодействия напрямую не решал вопрос «развития» информационной деятельности для сохранения ее актуальности.[158] Вместо этого при выполнении рекомендации основное внимание было уделено сообщениям о том, какие

[157] Вики-страница SSR2, документы и проекты группы по анализу, «Таблица рекомендаций SSR1», дата не указана, 26: https://community.icann.org/pages/viewpage.action?pageId=64076120.

[158] ICANN, Интерфейс взаимодействия, источник проверен 13 декабря 2020 года: https://features.icann.org/events-near-you.

мероприятия проводятся в произвольный момент времени. Поскольку не был сделан упор на развитие самой деятельности, рекомендация не выполнена.

Рекомендация SSR1 № 15

«ICANN должна действовать как координатор ответственного раскрытия и распространения информации об угрозах DNS и методах их смягчения».

Заключение SSR2: Эта рекомендация остается актуальной и не была полностью выполнена. Хотя процесс существует «на бумаге», невозможно оценить его функциональность и эффективность.

См. рекомендацию SSR2 № 8: Обеспечить и продемонстрировать представление общественных интересов на переговорах со сторонами, связанными договорными обязательствами; рекомендацию SSR2 № 12: Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку, и рекомендацию SSR2 №13: Повысить транспарентность и подотчетность в области сообщений о нарушениях. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:

- Хотя корпорация ICANN внедрила процесс раскрытия уязвимостей, нет никакой общедоступной статистики или другой информации о том, как часто этот процесс запускался.
- Корпорация ICANN создала Программу раскрытия уязвимостей для общедоступных активов ICANN.159 Когда в корпорацию ICANN поступают уведомления об уязвимостях инфраструктуры DNS, корпорация ICANN (когда это возможно) передает эту информацию ответственным третьим сторонам. Однако ответственность за устранение любой уязвимости на своей платформе (платформах) несет эта третья сторона.
- С 2013 года ни один из отчетов по IS-SSR не содержит статистических данных или показателей, относящихся к раскрытию информации. По опубликованным материалам невозможно определить, применялась ли когда-либо методология раскрытия уязвимостей и работоспособна ли она. Нет данных, даже в анонимной форме, о деятельности корпорации ICANN как координатора уязвимостей, а также о ее работе по координации действий в чрезвычайных ситуациях и кризисному управлению, связанному с SSR.

Рекомендация SSR1 № 16

«ICANN не должна прекращать своих усилий, направленных на расширение участия сообщества и его вклада в процесс разработки концепции обеспечения SSR. ICANN также должна создать процесс более регулярного получения предложений от других участников экосистемы».

Заключение SSR2: Эта рекомендация остается актуальной и была выполнена лишь частично. Учитывая отсутствие доказательств того, что текущая информационная деятельность привела к расширению участия сообщества, нельзя считать, что достигнут ожидаемый эффект от этой рекомендации.

[159] ICANN, «Процесс обработки уведомлений об уязвимостях в онлайн-службах корпорации ICANN», источник проверен 13 декабря 2020 года: https://www.icann.org/vulnerabilities.

См. рекомендацию SSR2 № 8: Обеспечить и продемонстрировать представление общественных интересов на переговорах со сторонами, связанными договорными обязательствами; рекомендацию SSR2 № 12: Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку, рекомендацию SSR2 №13: Повысить транспарентность и подотчетность в области сообщений о нарушениях, и рекомендацию SSR2 № 18: Информационное обеспечение дебатов по вопросам политики. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:

- Постоянное участие в деятельности соответствующих сообществ позволило достичь цели «участие», однако не удалось определить, каким образом поступающие предложения «регулярно» учитываются. Эта рекомендация предусматривает более активное участие общественности в инициативах по обеспечению SSR, включая создание концепций и годовых отчетов. Эта рекомендация не привела к очевидным изменениям подхода к созданию концепции IS-SSR и годовых отчетов.
- В настоящее время ведется работа по информированию сообществ, у которых есть связи с корпорацией ICANN, что позволяет достичь цели «участие». Однако рекомендация требует охвата новых сообществ, занимающихся вопросами SSR.
- Нет доказательств того, что текущая информационная деятельность привела к расширению участия сообщества.
- В рекомендации конкретно предлагается создать процесс более регулярного получения предложений от других участников экосистемы. Соответственно, окончательный отчет о состоянии дел с выполнением этой рекомендации SSR1 представляется неуместным.160
- В отчете о выполнении рекомендации говорится, что персонал «поддерживает различные инициативы отдела безопасности по наращиванию потенциала».161 Группе по анализу SSR2 не удалось определить, приведут ли эти инициативы по наращиванию потенциала к более широкому участию в разработке концепций IS-SSR и каким образом это произойдет, поскольку корпорация ICANN больше не обновляет концепции IS-SSR.
- Группе по анализу SSR2 не удалось выяснить в общедоступных источниках, каковы были инициативы по наращиванию потенциала и когда они проводились.

Рекомендация SSR1 № 17

«ICANN должна создать более структурированный внутренний процесс демонстрации связи различных видов деятельности и инициатив с конкретными стратегическими целями, задачами и приоритетами концепции обеспечения SSR».

Заключение SSR2: Эта рекомендация остается актуальной. Из-за отсутствия отслеживаемых индикаторов невозможно определить состояние дел с выполнением этой рекомендации на основе общедоступных материалов. Ожидаемый эффект от рекомендации не был достигнут, поскольку корпорация ICANN больше не поддерживает концепцию SSR.

[160] ICANN, Отчет о выполнении рекомендаций по итогам проверки SSR, июнь 2015 года: https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf.
[161] Тот же источник, 7.

См. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- В отчете о выполнении этой рекомендации указано, что результаты выполнения рекомендации SSR1 № 2 использовались как руководство по выполнению рекомендации SSR1 № 17. Однако рекомендации SSR1 № 2 и № 17 преследуют разные цели. В рекомендации SSR1 № 2 предлагается проводить регулярные консультации с общественностью для определения видов деятельности и круга обязанностей, связанных с SSR, тогда как рекомендация SSR1 № 17 предполагает, что инициативы в области SSR будут связаны с конкретными стратегическими целями, задачами и приоритетами. Результаты выполнения рекомендации SSR1 № 2 не соответствуют требованиям рекомендации SSR1 № 17.
- В последнем годовом отчете, рассмотренном SSR2 (2018 ФГ), перечислено восемнадцать отдельных инициатив на финансовый год, а затем описано, как эти инициативы связаны с общей миссией офиса CTO и общим стратегическим планом ICANN. Годовой план также содержит ссылки на отчеты о деятельности, в которых описывается работа, выполненная за отчетный период (шесть месяцев).
- Связь между годовым отчетом по SSR и стратегическим планом ICANN не ясна. Кроме того, в стратегическом плане не упоминаются годовые отчеты по SSR и почти не упоминается деятельность, связанная с SSR. Группе по анализу SSR2 не удалось на основе общедоступных материалов определить, существует ли более структурированный внутренний процесс демонстрации связи различных видов деятельности и инициатив с конкретными стратегическими целями, задачами и приоритетами концепции IS-SSR. Однако в разделе последнего годового отчета, где представлен перечень ежегодных инициатив, сделана попытка увязать их со стратегическим планом ICANN.
- В других рекомендациях SSR1 делается попытка согласовать и интегрировать деятельность ICANN в области SSR с общим стратегическим планом. Результат выполнения рекомендации SSR1 № 17 никак нельзя считать созданием структурированного и легко проверяемого внутреннего процесса.

Рекомендация SSR1 № 18

«ICANN должна проводить ежегодный оперативный анализ прогресса в реализации концепции обеспечения SSR и включать этот анализ в состав компонентов концепции обеспечения SSR на следующий год».

Заключение SSR2: Эта рекомендация остается актуальной. Группе по анализу SSR2 не удалось найти никаких доказательств того, что существует процесс внутреннего или публичного анализа, приводящий к регулярному обновлению концепции IS-SSR. Поэтому группа не может определить, достигнуты ли намеченные результаты этой рекомендации.

См. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- В рекомендации SSR1 № 18 предлагается рекурсивный подход, при котором анализ деятельности за предыдущий год влияет на решения относительно будущих инициатив.

Группа по анализу SSR2 не обнаружила фактов, свидетельствующих о наличии неформального или недокументированного внутреннего процесса или публичного ежегодного процесса операционного анализа реализации концепции IS-SSR.

Рекомендация SSR1 № 19

«ICANN должна ввести процесс, позволяющий сообществу отслеживать реализацию концепции обеспечения SSR. Информация должна предоставляться с достаточной степенью детализации, позволяющей сообществу следить за выполнением корпорацией ICANN своих обязательств в отношении SSR».

Заключение SSR2: Эта рекомендация остается актуальной. Из-за отсутствия конкретики или «достаточной ясности» эта рекомендация не поддается количественному анализу во всей полноте. Ожидаемый эффект от выполнения данной рекомендации не достигнут, поскольку сообщество по-прежнему не может отслеживать деятельность, связанную с SSR, в разумные сроки, на открытой и транспарентной основе.

См. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Корпорация ICANN сообщает, что в ежегодно публикуемой концепции IS-SSR[162] отслеживается прогресс в выполнении мероприятий, которые были запланированы в предыдущем году. Кроме того, регулярные отчеты по управлению проектом, операционные планы и бюджеты считаются инструментами, предоставляющими подробную информацию о деятельности в сфере SSR. Однако публикация годовой концепции IS-SSR на сайте, похоже, не служит цели информирования сообщества и не позволяет отслеживать реализацию этой концепции. Сроки публикации документов по реализации сильно отстают от самой реализации, что не позволяет сообществу отслеживать действия, связанные с SSR.
- Более того, похоже, что группа по анализу SSR1 привела в качестве примера механизма, позволяющего отслеживать деятельность в сфере SSR, информационную панель, которая была создана для выполнения одной из рекомендаций ATRT. Однако нет никаких свидетельств того, что такая информационная панель доступна сообществу или общественности применительно к деятельности, связанной с SSR.

Рекомендация SSR1 № 20

«ICANN должна повысить транспарентность информации об организационной структуре и бюджетных средствах, связанных с реализацией концепции обеспечения SSR и выполнением функций в области SSR».

Заключение SSR2: Эта рекомендация остается актуальной и была частично выполнена. Предполагаемый эффект от повышения транспарентности информации об организационной структуре и бюджетных средствах, касающихся SSR, не был достигнут.

См. рекомендацию SSR2 № 3: Повысить транспарентность бюджета, связанного с SSR. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

[162] Архив документов IS-SSR: https://www.icann.org/ssr-document-archive.

Обоснование:

- Цикл процесса планирования ICANN заключает в себе три элемента: стратегический план, пятилетний план операционной деятельности и годовой план операционной деятельности и бюджет.[163] Этот цикл завершается отчетом о достижениях и ходе работ. Теперь в рамках Фазы I, как описано в отчетах о выполнении рекомендаций SSR1 на вики-сайте, предусмотрено предоставление общедоступных сведений о планах, бюджетах и мероприятиях, связанных с SSR (согласно рекомендации SSR1 № 2); это увязано с концепцией IS-SSR ICANN и информирует о деятельности и расходах в области SSR.[164] Периодические отчеты о деятельности в области SSR дополняют эту общедоступную информацию.[165] Осуществляется Фаза II для определения механизмов предоставления более подробной общедоступной информации о связанных с SSR бюджетах и расходах в разных отделах ICANN. В настоящее время общедоступную информацию по этой теме за 2018 ФГ можно найти на вики-странице, которая посвящена выполнению рекомендации № 20.[166]
- Персонал также составлял отчеты о мероприятиях, в которых отражались ресурсы и бюджетные средства, использованные для организации этого мероприятия.[167] По состоянию на март 2020 года отчеты о мероприятиях не публиковались. Шаблон для общедоступной версии таких отчетов можно найти на вики-странице, которая посвящена выполнению рекомендации № 20.
- Годовая отчетность о деятельности в сфере SSR включается в документы концепций и годовые отчеты. В бюджетных документах есть очень обобщенные статьи расходов на деятельность, связанную с SSR. Та же самая деятельность, похоже, не отражается в регулярных отчетах ICANN по управлению проектами. В отчете о выполнении рекомендации говорится, что ICANN «*интегрирует концепцию обеспечения SSR и отчеты о деятельности и расходах в области SSR в состав концепции и процесса планирования, чтобы предоставлять общедоступную информацию о планах, бюджетах и мероприятиях, связанных с SSR*».[168] Однако, как отмечалось в рекомендации SSR1 № 19, система управления портфелем ICANN и информационная панель проекта KPI предлагают очень мало информации, позволяющей сообществу отслеживать деятельность в сфере SSR.
- В утвержденном бюджете на 2018 ФГ есть три профильные области, относящиеся к SSR: Развитие идентификаторов; Безопасность, стабильность и отказоустойчивость идентификаторов интернета; Техническая репутация. Только для первых двух (Развитие идентификаторов и SSR идентификаторов интернета) предусмотрены отдельные бюджеты на уровне портфеля; детали этих бюджетов не приводятся. В отчете персонала о выполнении рекомендации также указано, что ICANN *«определит механизмы предоставления более подробной общедоступной*

[163] «Процесс планирования в ICANN»: https://www.icann.org/resources/pages/governance/planning-en.

[164] Главная страница выполнения рекомендаций по итогам проверки SSR1: https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home.

[165] Отчеты о деятельности по обеспечению SSR систем идентификаторов: https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

[166] Выполнение рекомендаций по итогам проверки SSR1, рекомендация № 20, последняя редакция от 18 сентября 2018 года: https://community.icann.org/display/SSR/Rec+%2320.

[167] Отчеты о деятельности по обеспечению SSR систем идентификаторов: https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

[168] См. обновления отчета о выполнении рекомендации SSR1 № 20: https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2.

информации о связанных с SSR бюджетах и расходах в разных отделах ICANN», что предполагает дополнительную работу по выполнению этого аспекта рекомендации.

Рекомендация SSR1 № 21

«ICANN должна создать более структурированный внутренний процесс для демонстрации связи решений по организационной структуре и бюджетным средствам с концепцией обеспечения SSR, включая лежащий в основе анализ издержек и выгод».

Заключение SSR2: Эта рекомендация остается актуальной и была частично выполнена. Это не дало ожидаемого результата — открытого и транспарентного процесса принятия бюджетных решений в области SSR.

См. рекомендацию SSR2 № 3: Повышение транспарентности бюджета, связанного с SSR. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- В отчете персонала о выполнении этой рекомендации упоминаются три результата:
  - Интеграция концепции IS-SSR и отчетов в состав концепции и процесса планирования для предоставления общедоступной информации о планах, бюджетах и мероприятиях, связанных с SSR.
  - Определение механизмов предоставления более подробной общедоступной информации о связанных с SSR бюджетах и расходах в разных отделах ICANN.
  - Изучение отчетов о мероприятиях, в которых отражаются ресурсы и бюджетные средства, использованные для организации мероприятия.
- В отчете персонала особо упоминается шаблон отчета для публикации информации, относящейся к бюджету и ресурсам на проведение мероприятий в области безопасности.[169] Согласно отчету персонала, такой отчет будет публиковаться ежегодно, начиная с 2018 финансового года. Изучение страниц, посвященных SSR, на сайте ICANN указывает на то, что такой отчет не публиковался. Годовая отчетность о деятельности в сфере SSR включается в документы концепций и годовые отчеты. В бюджете есть очень обобщенные статьи расходов на деятельность, связанную с SSR. Однако та же самая деятельность, похоже, не отражается в регулярных отчетах ICANN по управлению проектами. Это наблюдение совпадает с выводами SSR1 по рекомендации SSR1 № 20. Кроме того, отчеты о влиянии мероприятий в сфере SSR на бюджет и ресурсы, по-видимому, никогда не составлялись, а шаблон для содействия в подготовке такой отчетности, похоже, недоступен для публичного рассмотрения или комментариев.
- Процесс планирования ICANN гарантирует, что запланированные и предусмотренные в бюджете мероприятия, в том числе связанные с SSR, определяются конкретными целями. Не планировалось запрашивать комментарии общественности относительно шаблона, используемого для публикации более подробной общедоступной информации о бюджетах и расходах, связанных с SSR. В настоящее время этот шаблон, по-видимому, заменен годовым отчетом за финансовый год.

[169] Выполнение рекомендаций по итогам проверки SSR1, рекомендация № 20: https://community.icann.org/display/SSR/Rec+%2320.

Рекомендация SSR1 № 22

«ICANN должна публиковать, постоянно контролировать и обновлять документацию по организационной структуре и бюджетным ресурсам, необходимым для управления различными аспектами SSR параллельно с вводом новых gTLD.»

Заключение SSR2: Эта рекомендация остается актуальной и была частично выполнена. Выполнение рекомендации не позволило в полной мере достичь ожидаемого эффекта.

См. рекомендацию SSR2 № 3: Повысить транспарентность бюджета, связанного с SSR. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Общедоступная информация о связанных с SSR бюджетах и расходах в разных отделах ICANN за 2018 ФГ была опубликована здесь: https://community.icann.org/x/DqNYAw. Этот отчет обновляется ежегодно и охватывает прямые затраты, возникающие в результате деятельности, необходимой для выполнения функций по обеспечению SSR, прямые затраты на совместно используемые ресурсы и затраты на вспомогательные функции, выделенные для SSR. В этом отчете отсутствует разбивка финансирования, ресурсов или другой деятельности в разрезе Программы New gTLD.
- Корпорация ICANN также изучила возможные механизмы предоставления более подробной общедоступной информации о связанных с SSR бюджетах и расходах в разных отделах ICANN. Однако в шаблоне для этой общедоступной информации не выделены мероприятия или бюджеты в области SSR, связанные с Программой New gTLD.
- Совершенно очевидно, что организационная структура и бюджет для решения вопросов SSR, связанных с деятельностью группы программы создания новых gTLD, были предоставлены через отдел безопасности, но также отражены в бюджете и организационной структуре Программы New gTLD (например, Комиссия по вопросам стабильности DNS, EBERO, другие этапы процесса и так далее). По-видимому, намеченным результатом выполнения этой рекомендации должно было стать улучшение количества и качества информации об организационной структуре и бюджете для реализации концепции IS-SSR и выполнения функций по обеспечению SSR в рамках Программы New gTLD.
- В архиве документов ICANN по концепции IS-SSR нет ни одного документа, относящегося конкретно к Программе New gTLD. В концепции от 30 сентября 2016 года gTLD упоминаются дважды: один раз в Модуле A как тенденция в экосистеме интернета и второй раз в Модуле B как часть общего стратегического плана ICANN. В концепции обеспечения SSR на 2014 ФГ, опубликованной в марте 2013 года, Программа New gTLD снова упоминается как «тенденция» и движущая сила политики GNSO. За исключением этого, Программа New gTLD упоминается только в разделе, посвященном выполнению рекомендаций SSR1.

Рекомендация SSR1 № 23

«ICANN должна предоставить надлежащие ресурсы рабочим группам и консультативным комитетам, занимающимся вопросами SSR, в соответствии с возложенными на них обязанностями. ICANN также должна в обязательном порядке создать такие условия, в которых рабочие группы и консультативные комитеты

смогут принимать объективные решения без какого-либо внутреннего или внешнего давления».

Заключение SSR2: Эта рекомендация остается актуальной и была частично выполнена. Предполагаемый эффект заключался в том, чтобы у рабочих групп и консультативных комитетов появилась возможность выполнять свои мандаты объективным образом, без внешнего или внутреннего давления, и не поддается измерению.

См. рекомендацию SSR2 № 3: Повысить транспарентность бюджета, связанного с SSR. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Корпорация ICANN предоставляет персонал технической поддержки ICANN для оказания комитетам SSAC и RSSAC помощи в подготовке документов. В бюджете корпорации ICANN предусмотрено некоторое финансирование для поддержки SSAC и RSSAC в проведении заседаний (в частности, расходы на проезд, проживание в гостинице и питание); в качестве примера для группы по анализу SSR2 корпорация ICANN привела бюджет на 2015 год.[170] Вспомогательное финансирование никогда не было связано или обусловлено какой-либо официальной оценкой эффективности, результатов или удовлетворенности. По мнению ICANN, это обеспечивает надлежащую независимость. На практике неясно, как рабочие приоритеты RSSAC или SSAC определяются или оцениваются ICANN или сообществом, что создает пробел в подотчетности, а также делает невозможной оценку наличия у них ресурсов, «соответствующих возложенным на них обязанностям». Исходный отчет SSR1 содержал следующий текст, относящийся к этой рекомендации:
  «В ходе обсуждений с SSAC выяснилось, что иногда этот комитет испытывает давление и вынужден давать ответ по конкретной проблеме в крайне ограниченные сроки. Это приводит к сокращению времени анализа проблем и более целенаправленным рекомендациям. Очевидно, что иногда при анализе непосредственных рисков сроки исследовательской работы сжимаются. Это неизбежно. Однако целесообразно обеспечить правильное планирование, предоставляя SSAC и RSSAC как можно больше времени для проведения высококачественных исследований и формулирования выводов».

  Это наблюдение перекликается с обстоятельствами и опасениями последних двух лет, особенно в контексте обновления ключа KSK в октябре 2018 года, когда SSAC изо всех сил старался ответить в кратчайшие сроки на просьбы о предоставлении рекомендаций, в отсутствие необходимых полноценных данных или исследований.[171] Скорее всего, выделяемая SSAC доля бюджета ICANN недостаточна, учитывая множество широко распространенных и новых проблем в сфере SSR, а также ожидания, что SSAC предоставит рекомендации, для подготовки которых необходимы исследования или обобщение результатов предыдущих исследований. Кроме того, нынешняя структура SSAC несовместима с «высококачественной исследовательской работой», поскольку члены комитета — это группа «волонтеров», в основном

[170] ICANN, «Утвержденный операционный план и бюджет на 2015 ФГ», 1 декабря 2014 года, 77-78: https://www.icann.org/en/system/files/files/adopted-opplan-budget-fy15-01dec14-en.pdf.
[171] ICANN, «Первое обновление ключа KSK прошло успешно», 15 октября 2018 года: https://www.icann.org/news/announcement-2018-10-15-en.

являющихся представителями отрасли, участие которых оплачивается их работодателями. Соответственно, этот комитет не «свободен от внешнего давления».
- Отсутствие показателей и мониторинга успеха или неудачи Программы New gTLD указывает на то, что этот подход с участием многих заинтересованных сторон не «свободен от внешнего давления». Используя показатели из отчета группы по анализу CCT о неправильном использовании DNS в новых gTLD, нельзя сделать вывод, что Программа New gTLD была успешной с точки зрения CCT. Такое исследование полностью соответствует функциям и обязанностям отдела безопасности ICANN (см. рекомендацию SSR1 № 24). Сама ICANN не проводила и не финансировала подобное мероприятие, вероятно, из-за слишком сильного внешнего противодействия исследованиям такого рода в области SSR.
- В документе о рабочих процедурах SSAC не упоминается о противодействии внешнему и внутреннему давлению, за исключением раздела 2.1.2 «Отказ от участия и возражения». Это означает, что каждый член и комитет в целом самостоятельно улаживают конфликты интересов, а все обсуждения конфиденциальны по соображениям безопасности.[172] То же самое верно для RSSAC и RZERC, но в этих двух случаях структура комитетов такова, что каждый человек представляет заинтересованную сторону.
- В некоторых из этих консультативных комитетов, занимающихся вопросами SSR, неизменно отсутствуют важные заинтересованные стороны (например, жертвы неправильного использования идентификаторов, научные работники, представители правоохранительных органов, политики).

Рекомендация SSR1 № 24

«ICANN должна четко сформулировать устав, функции и обязанности своей службы безопасности».

Заключение SSR2: Эта рекомендация остается актуальной и была частично выполнена. Ожидаемый эффект от наличия четко сформулированного устава, функций и обязанностей службы безопасности не был достигнут.

См. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:
- По состоянию на 2018 год главная служба безопасности отсутствует. Тем не менее, работающая в офисе технического директора (OCTO) группа специалистов по SSR занимается внешними вопросами SSR, имеющими отношение к ICANN, CIO и сотрудники группы занимаются внутренними вопросами безопасности, а исследовательская группа OCTO рассматривает будущие риски и возможности в сфере SSR в рамках ограниченного круга обязанностей ICANN.173 На веб-странице этой группы в общих чертах описана ее миссия и приводятся ссылки на страницу

[172] Консультативный комитет по безопасности и стабильности ICANN, «Рабочие процедуры SSAC, версия 5.1», 27 февраля 2019 года, 10: https://www.icann.org/en/system/files/files/operational-procedures-27feb18-en.pdf.
[173] Офис технического директора (OCTO) ICANN, источник проверен 27 декабря 2019 года: https://www.icann.org/octo.

«деятельности» в области SSR.[174] Отсутствуют формулировки, определяющие «устав», «функции» или «обязанности» этой группы. Группа SSR2 предполагает, что перечисленные на этой странице виды деятельности ICANN считает функциями и обязанностями OCTO в области SSR:

- Активное взаимодействие с сообществами специалистов в области безопасности, в том числе безопасности эксплуатации и общественной безопасности, для сбора и обработки данных, указывающих на (неизбежные) угрозы функционированию DNS или служб регистрации доменов («экосистеме DNS»).
- Содействие или участие вместе с указанными сообществами в мероприятиях по обеспечению готовности к угрозам для защиты или смягчения угроз экосистеме DNS.
- Исследование или анализ данных для лучшего понимания состояния и степени работоспособности экосистемы DNS.
- Координирование подготовки отчетов о выявлении уязвимостей DNS (https://www.icann.org/vulnerability-disclosure.pdf).
- Предоставление экспертных знаний в предметной области для наращивания потенциала ccTLD и сообществ специалистов по общественной безопасности в решении вопросов, относящихся к экосистеме DNS, включая DNSSEC, злоупотребление или неправильное использование инфраструктуры или операций DNS.
- Помощь в ведении деятельности по управлению рисками для экосистемы DNS.
- Участие вместе со специалистами отдела ICANN по глобальному взаимодействию с заинтересованными сторонами в глобальной работе многих заинтересованных сторон, направленной на повышение кибербезопасности и снижение киберпреступности.

- По-видимому, OCTO немногое сделал в плане анализа SSR, результаты которого доступны широкой общественности. Инициатива «Открытые данные», отчетность DAAR и проект разработки показателей работоспособности интернета представляются проектами, для которых используются только внутренние данные корпорации ICANN. Неясно, какую пользу принесла любая из перечисленных работ всему сообществу, которому призвана служить корпорация ICANN.

Рекомендация SSR1 № 25

«ICANN должна ввести механизмы выявления рисков и стратегических факторов в краткосрочной и долгосрочной перспективе в рамках своей концепции управления рисками».

Заключение SSR2: Эта рекомендация остается актуальной и была частично выполнена. Выполнение рекомендации не позволило в полной мере получить ожидаемый эффект.

См. рекомендацию SSR2 № 4: Улучшить процессы и процедуры управления рисками. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Концепция управления рисками была принята Правлением ICANN в 2013 году после получения от сообщества комментариев на конференциях ICANN50 и ICANN51. Корпорация ICANN поддерживает панель управления рисками предприятия (ERM),

[174] OCTO ICANN, «Безопасность, стабильность и отказоустойчивость системы идентификаторов интернета», источник проверен 27 декабря 2019 года: https://www.icann.org/octo-ssr.

где перечислены риски, которые необходимо отслеживать и устранять, и следует концепции управления рисками предприятия. Однако, хотя механизм уже создан, отсутствует ясность в том, как идентификация рисков влияет на соответствующие процессы и политику в области SSR.

Рекомендация SSR1 № 26

«ICANN должна уделить первостепенное внимание своевременному завершению подготовки концепции управления рисками».

Заключение SSR2: Эта рекомендация остается актуальной и была частично выполнена. Учитывая, что термин «своевременный» не позволяет понять, что именно было запланировано или приемлемо, невозможно оценить, был ли достигнут намеченный эффект.

См. рекомендацию SSR2 № 4: Улучшить процессы и процедуры управления рисками. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Концепция управления рисками была принята Правлением ICANN в 2013 году[175] после получения от сообщества комментариев на конференциях ICANN50 и ICANN51. Более подробный ответ на эту рекомендацию содержится в разделе оценки рекомендации № 27.

Рекомендация SSR1 № 27

«Концепция управления рисками ICANN должна носить комплексный характер в пределах круга обязанностей по обеспечению SSR и выполнению ограниченных миссий».

Заключение SSR2: Эта рекомендация остается актуальной. Учитывая отсутствие определения понятия «комплексный» в отчете SSR1 или показателей для оценки, группе по анализу SSR2 не удалось оценить, была ли эта рекомендация выполнена полностью. Корпорация ICANN не добилась ожидаемого результата — предоставления исчерпывающей, удобной для поиска информации о концепции управления рисками, используемой ICANN.

См. рекомендацию SSR2 № 4: Улучшить процессы и процедуры управления рисками. Это рекомендация SSR2, которая расширяет исходную рекомендацию SSR1.

Обоснование:

- Группа по анализу SSR2 обсудила, можно ли признать рекомендацию SSR1 № 27 выполненной на основе ссылок, предоставленных персоналом при ответе на различные вопросы, относящиеся к рекомендации SSR1 № 25. Однако группа по анализу SSR2 пришла к выводу, что эта рекомендация, хотя и связана с рекомендациями SSR1 № 25 и 26, отличается от них тем, что требует «комплексной» концепции. Группа по анализу SSR2 пришла к мнению, что в случае выполнения рекомендации SSR1 № 27 согласно намерениям группы по анализу SSR1, она решила бы те же проблемы, для решения которых, вероятно, были даны рекомендации SSR1 № 25 и 26.

[175] ICANN, «Отчет о концепции управления рисками для DNS», последняя редакция от 4 октября 2013 года: https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en.

- Группа по анализу SSR1 не определила, какие элементы концепции обеспечат ее «комплексный» характер и как это следует оценивать. В ходе проверки было отмечено, что эту рекомендацию должен был выполнять персонал, который больше не работает в корпорации ICANN. В связи с этим отсутствует институциональная память и полные исторические данные о том, как оценивалась «комплексность» концепции управления рисками.
- Общедоступная информация о том, как осуществляется управление рисками, была обнаружена в разрозненном виде. Например, персонал указал, что функции надзора за этой деятельностью возложены на комитет Правления по управлению рисками — группу руководителей корпорации ICANN. Кроме того, есть представители функциональных подразделений по вопросам рисков — сотрудники, представляющие каждую функцию по реализации концепции рисков, и весь персонал корпорации, который несет ответственность за риски в соответствующей сфере деятельности, занимается управлением рисками. Это демонстрирует, что функция управления рисками в корпорации ICANN не централизована и не координируется на стратегическом уровне.

Рекомендация SSR1 № 28

«ICANN не должна прекращать своего активного участия в обнаружении и устранении угроз, а также своего участия в усилиях по распространению информации об угрозах и происшествиях».

Заключение SSR2: Эта рекомендация остается актуальной и не была полностью выполнена. Несмотря на то, что корпорация ICANN взаимодействует с различными группами, содействуя обнаружению, смягчению и обмену информацией об угрозах и инцидентах, ожидаемый эффект от предоставления этой информации не только указанным группам не был достигнут.

См. рекомендацию SSR2 № 2: Ввести должность руководителя высшего звена, ответственного за стратегию и тактику обеспечения безопасности и управления рисками, рекомендацию SSR2 № 8: Обеспечить и продемонстрировать представление общественных интересов на переговорах со сторонами, связанными договорными обязательствами; рекомендацию SSR2 № 12: Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку, и рекомендацию SSR2 №13: Повысить транспарентность и подотчетность в области сообщений о нарушениях. Это рекомендации SSR2, которые расширяют исходную рекомендацию SSR1.

Обоснование:
- Группа по анализу SSR2 не нашла каких-либо общедоступных данных, свидетельствующих о том, что корпорация ICANN занимается обнаружением и устранением угроз. Корпорация ICANN по мере возможности передает полученные уведомления об уязвимостях ответственным третьим сторонам. Однако ответственность за принятие мер в связи с получением информации об угрозе или инциденте несет эта третья сторона.
- Нет никаких публичных свидетельств того, что корпорация ICANN на постоянной основе занимается обнаружением угроз или что кому-либо поручена эта функция. Однако в сообществе ICANN есть ряд групп (открытых и закрытых), которые активно занимаются обнаружением угроз, в том числе SSAC, RSSAC, TLDOPS, рабочая группа по реагированию на инциденты ccNSO и PSWG. Группа по SSR OCTO координирует свои действия с этими группами.

Приложение E. Исследовательские данные из отчетов о тенденциях неправильного использования DNS

К примерам, которые в той или иной степени связаны с DNS, относятся:

- Вредоносное ПО: С 2016 по 2018 год количество уникальных URL-адресов, признанных антивирусными программами вредоносным ПО, увеличилось более чем вдвое до 554 159 6213[176], а количество атак со стороны мобильных вредоносных программ почти удвоилось за период с 2017 по 2018 год и превысило 116 миллионов[177].
- Мошенничество с цифровыми сертификатами: APWG сообщает, что фишеры все чаще используют цифровые сертификаты, чтобы атака выглядела как обмен данными с законным сайтом для подавления механизма предупреждения об обнаружении мошенничества в браузере.[178] Из-за того, что ICANN больше не предоставляет доступ к WHOIS, у администрации центров SSL-сертификации больше нет доступа к регистрационным данным доменных имен и нет возможности использовать записи о владении доменными именами, которые корпорации ICANN поручено координировать, для проверки прав собственности на доменное имя. По данным PhishLabs, половина всех фишинговых сайтов использует шифрование SSL, что может ввести пользователей в заблуждение, заставив их думать, что использование сайта безопасно, например, из-за зеленого символа замка, который появляется в адресной строке браузера при включенном шифровании SSL. Отчасти этот прирост связан с тем, что злоумышленники добавляют на свои фишинговые сайты шифрование HTTP — метод, позволяющий обернуть функцию защиты против жертв.[179]
- Фишинг: APWG сообщила, что фишеры регистрируют доменные имена непосредственно для мошенничества, а методы фишинговых атак стали более эффективными и их труднее обнаружить.

  > «*Фишеры все чаще используют переадресацию веб-страниц как способ скрыть свои фишинговые сайты от обнаружения. Когда жертвы переходят по ссылкам в фишинговых письмах, механизм переадресации отправляет пользователя в непреднамеренное путешествие по другим сайтам, прежде чем он попадет на сам фишинговый сайт.А затем, как только жертва сообщит свои учетные данные, в результате еще большего числа переадресаций она может попасть на другой домен».*[180]

- Компрометация рабочей электронной почты: Центр интернет-преступности ФБР США сообщил об увеличении на 136% выявленных в мире за период с 2016 по 2018 год

[176] AMR, «Бюллетень безопасности Лаборатории Касперского за 2018 год: статистика», 4 декабря 2018 года: https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/.
[177] Виктор Чебышев, «Развитие вредоносного ПО для мобильных устройств в 2018 году», 5 марта 2019 года:https://securelist.com/mobile-malware-evolution-2018/89689/.
[178] APWG, «Отчет APWG о тенденциях фишинга за 3 квартал 2018 года», 11 декабря 2018 года: https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.
[179] Эллиот Фолькман, «Уже 49 процентов фишинговых сайтов используют HTTPS», блог PhishLabs, 6 декабря 2018 года: https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https.
[180] Отчет APWG о тенденциях фишинга: https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.

убытков в результате компрометации рабочей электронной почты, затронувшей все 50 штатов США и 150 стран мира. С октября 2013 по май 2018 года ФБР задокументировало многомиллиардный рост BEC, который часто связан с мошеннической регистрацией доменных имен, которые обманчиво похожи на одну из целевых сторон.[181]

- Мошенничество: Австралийская комиссия по вопросам конкуренции и защиты потребителей (ACCC) ScamWatch сообщила о почти двукратном росте убытков от мошенничества примерно за последние три года до 11,8 млн австралийских долларов в 2019 году.[182] Доменные имена, используемые для интернет-мошенничества, очень часто нарушают права на товарные знаки или названия компаний. Мошенники регистрируют эти имена в условиях минимального или нулевого контроля над объемами похожих имен, которые мошенник может зарегистрировать, и ограниченного доступа к информации, которую следователи могут использовать для идентификации преступников.
- Ботнеты: В 2017 году организация Spamhaus DBL составила список, в который вошли 50 000 доменных имен управляющих серверов ботнетов, зарегистрированных и созданных киберпреступниками с единственной целью — создать управляющий сервер ботнета. Более 25% этих доменных имен ботнетов были зарегистрированы через одного и того же регистратора Namecheap.[183] В 2018 году в список Spamhaus вошли 103 503 доменных имени управляющих серверов ботнетов, что на 106% больше. Namecheap оставался регистратором, которого чаще всего использовали для совершения злоупотреблений: количество зарегистрированных там доменных имен управляющих серверов ботнетов выросло на 220%.[184]
- Спам: Спам является предпочтительной инфраструктурой доставки для фишинга, вредоносного ПО и других угроз, связанных с DNS. Среднесуточный объем спама по состоянию на август 2019 года составил 416,04 миллиарда сообщений.[185]

> *«Независимо от того, насколько сильно меняется картина угроз, вредоносная электронная почта и спам остаются жизненно важными инструментами для злоумышленников при распространении вредоносного ПО, поскольку доставляют угрозы непосредственно в конечную точку. Применяя правильное сочетание методов социальной инженерии, таких как фишинг и вредоносные ссылки и вложения, злоумышленники могут просто сидеть сложа руки и ждать, пока ничего не подозревающие пользователи активируют свои уязвимости».*[186]

---

[181] «Компрометация рабочей электронной почты, мошенничество на 12 миллиардов долларов», Объявление государственной службы Федерального бюро расследований, 12 июля 2018 года: https://www.ic3.gov/media/2018/180712.aspx.

[182] ScamWatch, Австралийская комиссия по вопросам конкуренции и защиты потребителей: https://www.scamwatch.gov.au/about-scamwatch/scam-statistics.

[183] «Отчет Spamhaus об угрозах со стороны ботнетов за 2017 год», Spamhaus Malware Labs, последняя редакция от 8 января 2018 года: https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017.

[184] «Отчет Spamhaus об угрозах со стороны ботнетов за 2019 год», Spamhaus Malware Labs, дата не указана: https://www.spamhaustech.com/botnet-threat-report-2019/

[185] «Данные об электронной почте и спаме», Cisco Talos Intelligence Group: https://www.talosintelligence.com/reputation_center/email_rep.

[186] «Годовой отчет Cisco по кибербезопасности за 2018 год», Cisco Systems, февраль 2018 года: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.

- DDOS-атаки: Количество распределенных атак типа «отказ в обслуживании» (DDoS) выросло на 40% с середины 2017 года до середины 2018 года.[187] Максимальный масштаб DDoS-атак увеличился во всем мире на 174% в первой половине 2018 года по сравнению с аналогичным периодом 2017 года, а жертвой самой крупной из когда-либо зарегистрированных атак (1,7 Тбит/с) стал крупный североамериканский провайдер услуг в феврале 2018 года.[188] Поскольку все — от коммерческих предприятий до государственных учреждений и физической инфраструктуры общественного пользования — зависит от бесперебойной работы служб, связанных с DNS, неослабленные DDoS-атаки становятся все более опасными. DDoS-атаки также стали более сложными, и теперь чаще всего используются многовекторные атаки. Компания Verisign сообщила, что 52% атак на ее системы, зарегистрированных во втором квартале 2018 года, были многовекторными.[189] Кроме того, интернет вещей (IoT) вызывает растущую озабоченность в отношении DDoS-атак, поскольку эти подключенные устройства являются легкой мишенью и продолжают распространяться. Количество подключенных устройств составляло 27 миллиардов в 2017 году и, по прогнозам, к 2020 году достигнет 125 миллиардов.[190]

[187] «Отчет о тенденциях в области DDOS-атак за первое полугодие 2018 года», Corero Network Security, дата не указана: https://info.corero.com/report-2018-half-year-ddos-trends-report-download.html.
[188] Кевин Уэлен, «Начало терабитной эры: готовьтесь к более масштабным DDoS-атакам», 5 сентября 2018 года: https://www.netscout.com/blog/entering-terabit-era-get-ready-bigger-ddos-attacks.
[189] «Отчет о тенденциях в области DDOS-атак за второй квартал 2018 года: для 52 процентов атак одновременно использовалось несколько типов атаки», блог Verisign, последняя редакция от 27 сентября 2018 года: https://blog.verisign.com/security/ddos-protection/q2-2018-ddos-trends-report-52-percent-of-attacks-employed-multiple-attack-types/.
[190] Джон Инглиш, «Подготовка сети к интернету вещей, чтобы она соответствовала ожиданиям», блог NETSCOUT, последняя редакция от 28 февраля 2018 года: https://www.netscout.com/blog/getting-network-ready-meet-iot-expectations.

Приложение F. Данные исследований в области криптографии

Криптография на основе эллиптических кривых

Криптография на основе эллиптических кривых (ECC) — альтернатива криптографии с открытым ключом RSA, которая в настоящее время используется для DNSSEC. Этот метод основан на теории эллиптических кривых, которую можно использовать для создания более быстрых, меньших по размеру и более эффективных криптографических ключей.[191]

Заявление о практике использования DNSSEC (DPS) содержит указания по длине и обновлению ключа KSK корневой зоны. Однако в DPS ничего не сказано о процедурах изменения алгоритма цифровой подписи. Согласно последним рекомендациям Агентства национальной безопасности США рекомендуется использовать для RSA 3072 бита. По-видимому, алгоритм цифровой безопасности на основе кривых Эдвардса (EdDSA) предлагает лучшую альтернативу, чем очень большие ключи RSA.[192]

Постквантовая криптография

Большинство людей еще десять лет назад ничего не слышали о квантовых вычислениях, однако в последние годы такие вычисления привлекли широкое внимание общественности. Отчасти такой интерес возник из-за уникальной вычислительной мощности квантового компьютера. Национальная академия наук США недавно выпустила доклад «Квантовые вычисления: прогресс и перспективы», в котором сделан общий вывод о том, что сейчас самое время начать подготовку к квантово-безопасному будущему.[193]

По оценкам DigiCert, для факторизации 2048-битного ключа RSA с помощью классической вычислительной технологии потребуется несколько квадриллионов лет.[194] В будущем, если будет изобретен крупномасштабный квантовый компьютер, он сможет взломать тот же ключ намного быстрее, возможно, всего за несколько месяцев. Еще остается множество технических проблем, которые необходимо преодолеть, прежде чем удастся создать квантовый компьютер, угрожающий RSA и ECC, двум основным алгоритмам асимметричного шифрования, используемым для защиты интернета.

---

[191] См. следующие RFC для получения дополнительной информации о потенциальных новых алгоритмах для подписей DNSSEC: П. Хоффман и У. Вийнгардс, «Алгоритм цифровой подписи на основе эллиптических кривых (DSA) для DNSSEC», RFC 6605, DOI 10.17487/RFC6605, апрель 2012 года: <https://www.rfc-editor.org/info/rfc6605>; О. Сьюри и Р. Эдмондс, «Алгоритм цифровой безопасности на основе кривых Эдвардса (EdDSA) для DNSSEC», RFC 8080, DOI 10.17487/RFC8080, февраль 2017 года: <https://www.rfc-editor.org/info/rfc8080>; П. Воутерс и О. Сьюри, «Требования к реализации алгоритмов и руководство по использованию для DNSSEC», RFC 8624, DOI 10.17487/RFC8624, июнь 2019 года: <https://www.rfc-editor.org/info/rfc8624>.

[192] Воутерс и Сьюри RFC 8624: https://www.rfc-editor.org/info/rfc8624.

[193] Национальные академии наук, инженерного дела и медицины. 2019 год. Квантовые вычисления: прогресс и перспективы. Вашингтон, Издательство национальных академий: https://doi.org/10.17226/25196.

[194] Тимоти Холлебек, «DigiCert о квантовых вычислениях: доклад Национальной академии наук», блог DigiCert, 9 января 2019 года: https://www.digicert.com/blog/digicert-on-quantum-national-academy-of-sciences-report/.

Для оценки успехов в создании крупномасштабного квантового компьютера нужно отслеживать такие показатели как прирост количества физических квантовых битов или «кубитов» и частота возникновения ошибок. Частота возникновения ошибок важна, потому что значительно влияет на число физических кубитов, необходимых для создания одного логического кубита. Физические кубиты — это отдельные квантовые системы, представляющие либо ноль, либо единицу; однако физические кубиты подвержены ошибкам из-за неизбежного взаимодействия с окружающей средой даже при температурах, приближающихся к абсолютному нулю. Несколько физических кубитов могут быть объединены в один логический кубит, при этом дополнительные кубиты используются для обнаружения и исправления этих ошибок. Исследователи пока не создали ни одного логического кубита, хотя быстро продвигаются к этой цели. Как только логические кубиты станут доступны, нужно будет следить за количеством логических кубитов.

Группы, занимающиеся разработкой отраслевых стандартов, также готовятся к постквантовому будущему. Самым известным направлением деятельности является проект постквантовой криптографии NIST, который в сотрудничестве с исследователями из разных стран мира ведет разработку новых криптографических примитивов, неуязвимых для атак со стороны квантовых компьютеров.[195] Можно ожидать, что на осуществление этого проекта уйдет еще несколько лет, прежде чем итоговые алгоритмы будут готовы к стандартизации.

Между тем исследователи сходятся во мнении, что в постквантовую эру безопасность будет обеспечена с помощью подписей на основе хэш-функций. Оперативная рабочая группа по исследованию интернета (IRTF) определила эти алгоритмы подписи в своей исследовательской группе Crypto Forum (CFRG), используя небольшие закрытые и открытые ключи с низкими вычислительными затратами.[196] Однако подписи имеют довольно большой размер, а закрытый ключ позволяет создать только конечное количество подписей. Хотя такие алгоритмы уже доступны, эти две особенности делают подписи на основе хэш-функций нежелательными в среде DNSSEC.

[195] Национальный институт стандартов и технологий (NIST), Лаборатория информационных технологий, Центр ресурсов компьютерной безопасности, «Постквантовая криптография», создано 03 января 2017 года, обновлено 23 ноября 2020 года: https://csrc.nist.gov/projects/post-quantum-cryptography.
[196] IRTF, Исследовательская группа Crypto Forum: https://irtf.org/cfrg.

Приложение G. Сопоставление рекомендаций SSR2 со Стратегическим планом ICANN на 2021–2025 годы и Уставом ICANN

Соответствующие разделы Устава ICANN

Раздел 1.2.(a)(i) и 1.2 (a)(ii), а также раздел 27.1(c)(i)(B) Устава в части поддержки и совершенствования «системы управления DNS и операционной стабильности, надежности, безопасности, глобальной функциональной совместимости, отказоустойчивости и открытости DNS и интернета»,

Раздел 3.6(a) Устава — оказание Правлению содействия в обсуждении и описании «существенных последствий, если таковые имеются, принятого решения с точки зрения глобальных общественных интересов, в том числе описание существенных последствий для безопасности, стабильности и отказоустойчивости DNS».

Разделы 12.2(b) и 12.2(c) Устава — тесное сотрудничество, в частности с Консультативным комитетом по безопасности и стабильности и Консультативным комитетом системы корневых серверов, и обеспечение полного выполнения рекомендаций, принятых Правлением ICANN и корпорацией ICANN.

Приложение G-1 к Уставу — вопросы, проблемы, политика, процедуры и принципы, упоминаемые в разделе 1.1(a)(i) и касающиеся регистраторов gTLD и регистратур gTLD: «вопросы, единообразное и согласованное решение которых необходимо для обеспечения функциональной совместимости, безопасности и/или стабильности интернета, услуг регистраторов, услуг регистратур или DNS» и «безопасность и стабильность базы данных регистратуры TLD».

Соответствующие цели и задачи стратегического плана

Из стратегического плана ICANN на 2021–2025 финансовые годы.[197]

1. Укрепление безопасности системы доменных имен и системы корневых серверов DNS.

1.1 Повысить общую ответственность за поддержание безопасности и стабильности DNS за счет укрепления координации DNS в партнерстве с соответствующими заинтересованными сторонами.
1.2 Укрепить управление работой корневых серверов DNS в координации с операторами корневых серверов DNS.
1.3 Определить и устранить угрозы безопасности DNS посредством более тесного сотрудничества с поставщиками аппаратных и программных решений и услуг.

[197] Стратегический план ICANN на 2021–2025 финансовые годы: https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf.

1.4 Повысить отказоустойчивость процедуры подписания ключей корневой зоны DNS, а также услуг и процессов распределения.

2. Стратегическая цель: Повышение эффективности модели управления с участием многих заинтересованных сторон ICANN.

2.1. Укрепить процесс принятия решений в ICANN на основе принципа «снизу вверх» и модели с участием многих заинтересованных сторон, а также обеспечить эффективное и своевременное выполнение работы и разработку политик.
2.2 Поддерживать и наращивать активное, информированное и эффективное участие заинтересованных сторон.
2.3 Поддерживать и совершенствовать открытость, инклюзивность, подотчетность и транспарентность.

3. Стратегическая цель: Развитие систем уникальных идентификаторов через координацию и сотрудничество с соответствующими сторонами, чтобы продолжать удовлетворять потребности глобальной базы интернет-пользователей.

3.1 Поддерживать конкуренцию, потребительский выбор и инновации в пространстве интернета за счет повышения информированности и способствуя обеспечению готовности к универсальному принятию, реализации IDN-доменов и переходу на протокол IPv6.
3.2 Усовершенствовать анализ и реагирование на новые технологии, влияющие на безопасность, стабильность и отказоустойчивость систем уникальных идентификаторов интернета, за счет более широкого взаимодействия с соответствующими сторонами.
3.3 Продолжить выполнение и совершенствование функций IANA для обеспечения качества выполняемых операций.
3.4 Поддерживать дальнейшую эволюцию систем уникальных идентификаторов интернета в рамках следующего раунда ввода новых gTLD, для которого будет обеспечено ответственное финансирование, управление и оценка риска, а также соблюдение требований процессов ICANN.

4. Стратегическая цель: решение геополитических вопросов, влияющих на миссию ICANN по обеспечению единства и глобальной функциональной совместимости Интернета.

4.1 Определять и учитывать глобальные вызовы и возможности в рамках своих полномочий для дальнейшего развития систем раннего предупреждения, таких как отчеты корпорации CANN о глобальной законодательной и регуляторной деятельности.
4.2 Продолжать создавать альянсы в экосистеме интернета и за ее пределами для повышения осведомленности и привлечения заинтересованных сторон со всего мира к участию в осуществлении миссии и разработке политик ICANN.

5. Стратегическая цель: Обеспечение финансовой устойчивости ICANN в долгосрочной перспективе.

5.1 Реализовать пятилетний финансовый план в поддержку пятилетнего плана операционной деятельности.
5.2 Разработать надежные и воспроизводимые модели прогнозов в области финансирования.
5.3 Обеспечить управление операциями и затратами на них для оптимизации и повышения эффективности деятельности ICANN.
5.4 Обеспечить непрерывное установление, достижение и поддержание уровня резервов ICANN в соответствии со сложностями и рисками среды ICANN.

№	Рекомендация	Стратегическая цель и задача
1	Завершить выполнение всех соответствующих рекомендаций SSR1.	Стратегические цели 1, 2 и 3
2	Рекомендация SSR2 № 2: Ввести должность ответственного за стратегию и тактику безопасности и управление рисками	Стратегические цели 1, 3 и 4
3	Рекомендация SSR2 № 3: Повышение транспарентности бюджета, связанного с SSR	Стратегические цели 1, 2, 3 и 5; стратегические задачи 2.1 и 3.4
4	Рекомендация SSR2 № 4: Улучшение процессов и процедур управления рисками	Стратегические цели 1, 2, 3, 4 и 5
5	Рекомендация SSR2 № 5: Соблюдать требования к соответствующим системам управления информационной безопасностью и сертификатам безопасности	Стратегическая цель 1
6	Рекомендация SSR2 № 6: Раскрытие уязвимостей SSR и транспарентность	Стратегические цели 1, 2, 3 и 4; стратегические задачи 1.1, 1.2, 1.3 и 4.1
7	Рекомендация SSR2 № 7: Улучшение процессов и процедур обеспечения непрерывности бизнеса и аварийного восстановления	Стратегические цели 1, 3 и 4; а также стратегические задачи 1.1, 1.4 и 3.3
8	Рекомендация SSR2 № 8: Обеспечение и демонстрация представления общественных интересов в переговорах со сторонами, связанными договорными обязательствами	Стратегические цели 1 и 3; стратегические задачи 1.1, 1.2, 1.3 и 1.4
9	Рекомендация SSR2 № 9: Мониторинг и обеспечение соблюдения обязательств	Стратегические цели 1, 2 и 3; стратегическая задача 2.1
10	Рекомендация SSR2 № 10: Обеспечение ясности определений терминов, связанных со злоупотреблениями	Стратегическая цель 1
11	Рекомендация SSR2 № 11: Решение проблем с доступом к данным CZDS	Стратегическая цель 3; стратегическая задача 3.2

12	Рекомендация SSR2 № 12: Пересмотреть усилия по анализу неправильного использования DNS и отчетности, чтобы обеспечить транспарентность и независимую проверку	Стратегические цели 1, 2, 3, 4 и 5
13	Рекомендация SSR2 № 13: Повышение транспарентности и подотчетности сообщений о нарушениях	Стратегические цели 1 и 3; стратегическая задача 2.1
14	Рекомендация SSR2 № 14: Создать временную спецификацию для улучшения безопасности на основе доказательств	Стратегическая цель 1; стратегическая задача 1.1
15	Рекомендация SSR2 № 15: Запустить EPDP для улучшения безопасности на основе доказательств	Стратегическая цель 1; стратегическая задача 1.1
16	Рекомендация SSR2 № 16: Требования к конфиденциальности и RDS	Стратегические цели 1, 3 и 5
17	Рекомендация SSR2 № 17: Измерение доменных коллизий	Стратегические цели 1, 3 и 4; стратегическая задача 3.4
18	Рекомендация SSR2 № 18: Информационное обеспечение дебатов по вопросам политики	Стратегические цели 1, 3 и 4; стратегическая задача 3.2
19	Рекомендация SSR2 № 19: Полная разработка набора тестов регрессии DNS	Стратегическая цель 1; стратегические задачи 1.1, 1.2, 1.3 и 1.4
20	Рекомендация SSR2 № 20: Официальные процедуры обновления ключей	Стратегические цели 1, 2 и 4; стратегическая задача 1.4
21	Рекомендация SSR2 № 21: Повышение безопасности связи с операторами TLD	Стратегическая цель 1; стратегическая задача 3.3
22	Рекомендация SSR2 № 22: Измерение качества услуг	Стратегические цели 1, 2, 3, 4 и 5; стратегические задачи 1.1, 1.2, 2.1, 3.2, 3.4 и 4.1
23	Рекомендация SSR2 № 23: Обновление алгоритма	Стратегические цели 1 и 3
24	Рекомендация SSR2 № 24: Повышение транспарентности и сквозного тестирования процесса EBERO	Стратегическая цель 1; стратегическая задача 1.2

Приложение H. Анализ результатов общественного обсуждения

Группа по анализу SSR2 создала электронную таблицу для регистрации своих ответов на комментарии общественности и изменений, вызванных результатами общественного обсуждения. Этот файл доступен на странице Документы и проекты группы по анализу вики-сайта SSR2; его также можно загрузить напрямую по ссылкам, приведенным ниже.

Excel:
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191048/Public%20Comment%20Feedback%20-%20March%202020.xlsx

PDF:
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191042/Public%20Comment%20Feedback%20-%20March%202020.pdf

Приложение I. Информационные бюллетени

Корпорация ICANN ежеквартально публикует информационные бюллетени и ведомости расходов, а также ежемесячно публикует данные об участии и отчеты о важных этапах работы. Эти документы обеспечивают транспарентность и подотчетность сообществу в отношении использования группой по анализу своих ресурсов и времени.

В информационных бюллетенях отражается посещаемость совещаний членами группы по анализу, затраты на профессиональные услуги и командировки для участия в очных совещаниях, основные этапы работы и участие в ней.

Определения используемых понятий:

Профессиональные услуги: Утвержденный бюджет группы по анализу, выделенный на привлечение независимых экспертов, как указано в разделе 4.6(a)(iv) Устава. Группы по анализу также могут выбирать независимых экспертов и обращаться к ним за рекомендациями по мере необходимости. Задача покрытия оправданных расходов и сборов, связанных с привлечением таких экспертов при проведении анализа, как указано в настоящем разделе 4.6, в той мере, в какой эти расходы и сборы соответствуют бюджету, выделенному на анализ, ложится на ICANN. Принципы работы групп по анализу с рекомендациями экспертов и их рассмотрения приведены в стандартах работы.

Командировки: Утвержденная сумма командировочных расходов на участие членов группы по анализу в очных совещаниях. К примерам командировочных расходов, помимо прочего, относятся следующие статьи расходов: авиабилеты, проживание в гостиницах, суточные, аренда места проведения совещания, аудиовизуальная/техническая поддержка и питание. Эти затраты охватывают командировочные расходы как членов группы по анализу, так и персонала корпорации ICANN.

Поддержка со стороны корпорации ICANN: Утвержденная в составе бюджета сумма расходов на привлечение корпорацией ICANN сторонних поставщиков услуг для поддержки работы группы по анализу.

Израсходовано на текущую дату: Эти суммы включают ежеквартальные данные о финансовых средствах, израсходованных группой по анализу с начала ее работы и по состоянию на конец последнего квартала.

Выделено на услуги:
1. Командировки: Ориентировочные расходы на запланированные очные совещания.
2. Профессиональные услуги: Услуги по подписанным контрактам, которые должны быть оказаны или отфактурированы.

Как правило, это услуги сторонних подрядчиков, не являющихся сотрудниками корпорации. Итого

Итого израсходовано и выделено на текущую дату: Это сумма статей «Израсходовано на текущую дату» и «Выделено
на услуги» по состоянию на конец последнего квартала. В составе статьи «Выделено
на услуги»
не учитывается сумма «Израсходовано на текущую дату». Остаток бюджета: Это разница между суммами по статьям «Утвержденный бюджет» и «Итого израсходовано и выделено на текущую дату».
С архивами информационных бюллетеней можно ознакомиться здесь:
https://community.icann.org/x/S7zRAw.