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

Из итогового отчета группы по анализу SSR2

22 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.

[7] См. https://www.qualtrics.com/.