Второй анализ безопасности, стабильности и отказоустойчивости (SSR2)

Основные положения и обзор

Основные положения

Настоящий отчет является предварительным проектом выводов и рекомендаций группы по анализу SSR2. Есть ряд вопросов, над которыми группа по анализу SSR2 продолжает работать, но в целом она считает, что достигнут этап, когда комментарии общественности внесли бы полезный и крайне необходимый вклад в подготовку итогового отчета.

В частности, RT SSR2 хотела бы узнать ваше мнение о следующем:

- выводы и рекомендации;
- какая часть ICANN (например, Правление, корпорация ICANN или сообщество ICANN) должна выполнять каждую рекомендацию;
- какие показатели целесообразнее всего использовать, чтобы сделать каждую рекомендацию измеримой, избегая при этом избыточных решений;
- какой приоритет следует отдать каждой рекомендации;
- какие дополнительные отчеты или материалы группа по анализу должна, по вашему мнению, рассмотреть до завершения работы над рекомендациями (см. вики-страницу SSR2,[1] где перечислены уже рассмотренные группой материалы, в том числе «справочные материалы», «информационные материалы» и «вопросы и ответы»).

В соответствии с установленной процедурой проведения проверок сообществу также будут предоставлены дополнительные возможности прокомментировать итоговый отчет SSR2.

Обзор

Введение

[Будет добавлено в итоговый отчет.]

Справочная информация

[Будет добавлено в итоговый отчет.]

Задачи

Согласно Уставу корпорации ICANN (раздел 4.6(c))[2] «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 оказывают прямое влияние на систему уникальных идентификаторов интернета и/или на которые прямо влияет указанная выше система, координированием которой занимается ICANN («Анализ SSR»)».

[1] Вики-страница группы по анализу SSR2 ICANN, https://community.icann.org/display/SSR/SSR2+Review.

[2] «Устав Интернет-корпорации по присвоению имен и номеров», ICANN, в редакции от 28 ноября 2019 года, https://www.icann.org/resources/pages/governance/bylaws-en.

А именно:

> *ii. Вопросы, оценкой которых может заниматься рабочая группа по анализу SSR («Рабочая группа по анализу SSR»), включают в себя, помимо прочего, следующее:*
>
> A. *физическую и сетевую безопасность, стабильность и отказоустойчивость в контексте координирования системы уникальных идентификаторов интернета;*
> B. *соответствие применимой концепции плана по обеспечению безопасности в случае непредвиденных обстоятельств для систем уникальных идентификаторов интернета;*
> C. *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 должна оценивать 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.*

Рекомендации SSR2 — сводная информация

Группа по анализу SSR2 привела все рекомендации SSR2 в соответствие со стратегическим планом ICANN на 2021–2025 годы[3], а также со своими целями и задачами. В отчете указаны соответствующие задачи, на выполнение которых направлены отдельные рекомендации; RT SSR2 исключила из настоящего отчета все рекомендации, которые не были четко согласованы со стратегическим планом.

Все рекомендации RT SSR2 соответствуют стратегическому плану корпорации ICANN и поэтому считаются высокоприоритетными.

3 «Стратегический план ICANN на 2021–2025 финансовые годы», последняя редакция от 29 марта 2019 года, https://www.icann.org/public-comments/strategic-plan-2018-12-20-en.

№	Рекомендация	Исполнитель	Приоритет
1	**Завершить выполнение всех соответствующих рекомендаций SSR1**		Высокий
2	**Рекомендация 9 SSR1 — Системы управления информационной безопасностью и сертификаты безопасности** 2.1. Корпорация ICANN должна составить дорожную карту своих проверок безопасности и мероприятий по сертификации, соответствующих отраслевым стандартам, в том числе определить сроки прохождения каждой сертификации и указать области, где требуется постоянное совершенствование. 2.2. Корпорация ICANN должна составить план сертификации и установить требования к обучению должностных лиц организации, отслеживать процент выполнения работ, обосновать свой выбор и документально отразить, как сертификаты соответствуют стратегии безопасности и управления рисками корпорации ICANN. 2.3. Корпорация ICANN также должна обосновать свой выбор, продемонстрировав его соответствие стратегии безопасности и управления рисками. 2.4. Корпорация ICANN должна внедрить систему управления информационной безопасностью и пройти сторонний аудит. 2.5. Чтобы воспользоваться преимуществами режима сертификации и аудита, корпорация ICANN должна пройти сторонний аудит и сертификацию в соответствии с отраслевыми стандартами безопасности и должна оценить варианты сертификации согласно общепринятым международным стандартам (например, ITIL, ISO 27001, SSAE-18) в контексте своих функциональных обязанностей.		Высокий
3	**Рекомендации 12,15 и 16 SSR1 — Стратегия и концепция SSR, показатели и раскрытие информации об уязвимостях** 3.1. Корпорация ICANN должна четко и публично решать вопросы безопасности (с учетом операционной безопасности, например, после введения моратория и анонимизации информации, если это необходимо) и продвигать передовые методы обеспечения безопасности среди всех сторон, связанных договорными обязательствами. 3.2. Корпорация ICANN должна также зафиксировать в принятом на основе консенсуса документе передовыеметоды работы в области SSR, установить четкие, измеримые и отслеживаемые цели, а затем реализовать эти методы в контрактах, соглашениях и меморандумах о взаимопонимании. 3.3. Корпорация ICANN должна внедрить слаженный процесс раскрытия информации об уязвимостях. Информация о		Высокий

	проблемах, связанных с SSR, должна незамедлительно раскрываться и доводиться до сведения соответствующих доверенных сторон (например, тех, кто пострадал или должен исправить данную проблему), в частности, когда какая-либо из сторон, связанных договорными обязательствами, допустила нарушение или корпорация ICANN получила сведения об обнаружении значительных уязвимостей. 3.4. Корпорация ICANN должна разработать четкий коммуникационный план для информирования сообщества и своевременно составлять регулярные (как минимум ежегодные) отчеты, содержащие анонимные показатели процесса раскрытия информации об уязвимостях. Эти коммюнике должны содержать сведения, добросовестно раскрываемые в соответствии с согласованным сообществом процессом, и анонимные показатели.		
4	**Рекомендации 20 и 22 SSR1 — Транспарентность бюджета и бюджетирование SSR в новых gTLD** 4.1. Там, где это возможно (на контрактной основе) и оправдано с точки зрения усилий (т. е. более 10% деятельности, описанной в статье бюджета), ICANN должна повысить транспарентность бюджета подразделений корпорации ICANN, имеющих отношение к реализации концепции безопасности, стабильности и отказоустойчивости систем идентификаторов (IS-SSR) и выполнению функций, касающихся SSR, в том числе связанных с созданием новых gTLD.		Средний
5	**Рекомендация 27 SSR1 — Управление рисками** 5.1. Концепция управления рисками ICANN должна быть централизованной и стратегически скоординированной. 5.2. Корпорация ICANN должна четко сформулировать свою концепцию рисков и стратегически согласовать ее с требованиями и целями организации, определив соответствующие показатели успеха и порядок оценки этих показателей корпорацией ICANN. 5.3. ICANN должна предоставить сообществу централизованный доступ к информации, относящейся к управлению рисками. Эта информация должна регулярно (как минимум ежегодно) обновляться для отражения текущей картины угроз.		Высокий
6	**Ввести должность ответственного за стратегию и тактику безопасности и управление рисками** 6.1. Корпорация ICANN должна ввести должность ответственного за стратегию и тактику безопасности и управление рисками в сфере внутренней безопасности организации, а также во внешней системе глобальных идентификаторов.		Высокий

	6.2. Корпорация ICANN должна нанять на эту должность специалиста соответствующей квалификации и выделить достаточные для выполнения указанных обязанностей бюджетные средства. 6.3. Это должностное лицо должно управлять отделом безопасности корпорации ICANN и контролировать взаимодействие персонала во всех областях, влияющих на безопасность. 6.4. Это должностное лицо также должно регулярно отчитываться перед Правлением и сообществом ICANN. 6.5. Это должностное лицо будет заниматься поиском путей и решением проблем, разрабатывая стратегию и осуществляя комплексные программы для внесения значительных улучшений. 6.6. Кроме того, это должностное лицо должно участвовать в любых затрагивающих вопросы безопасности переговорах при заключении корпорацией ICANN договоров (например, в каналах поставок аппаратного и программного обеспечения и при заключении связанных с ними соглашений об уровне обслуживания), утверждая все договорные условия, имеющие отношение к безопасности.		
7	**Дальнейшее развитие концепции управления рисками в области безопасности** 7.1. Корпорация ICANN должна четко сформулировать свою концепцию управления рисками в области безопасности и стратегически согласовать ее с требованиями и целями организации. 7.2. Корпорация ICANN должна определить соответствующие показатели успеха и порядок оценки этих показателей. RT SSR2 подробно обосновала необходимость этого в дополнительных комментариях, относящихся к рекомендации 9 SSR1 (см. выше раздел «Рекомендация 9 SSR1 — Системы управления информационной безопасностью и сертификаты безопасности» в настоящем отчете). 7.3. Корпорация ICANN должна: 7.3.1. Принять и внедрить ISO 31000 «Управление рисками», а также подтвердить и сертифицировать соблюдение этого стандарта с привлечением соответствующих независимых аудиторов.[4] Результаты деятельности по управлению рисками следует учитывать при определении планов и средств обеспечения бесперебойной деятельности и аварийного восстановления. 7.3.2. Регулярно обновлять перечень рисков в области безопасности и использовать его для определения приоритетов и направлений деятельности корпорации ICANN. Корпорация ICANN должна сообщать об обновлении этого перечня и своей методологии оценки рисков в области безопасности. Результаты такой работы		Высокий

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

	следует отражать в плане BC/DR и Системе управления информационной безопасностью (ISMS). 7.3.3. Назначить специальное должностное лицо, отвечающее за управление рисками в области безопасности, которое подчиняется начальнику службы безопасности, как указано в рекомендации «Должность начальника службы безопасности».		
8	**Разработать план обеспечения бесперебойной деятельности на основе ISO 22301** 8.1. 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».[5] 8.2. ICANN должна зафиксировать важность целесообразных и приемлемых сроков для BC и DR с учетом срочности восстановления полной функциональности. 8.3. Для операций с открытыми техническими идентификаторами (PTI) (функции IANA, включая все соответствующие системы, которые способствуют обеспечению безопасности и стабильности DNS, а также управлению корневой зоной) корпорация ICANN должна разработать общий подход к обеспечению непрерывности обслуживания в тесном сотрудничестве с Консультативным комитетом системы корневых серверов (RSSAC) и операторами корневых серверов. 8.4. Корпорация ICANN должна опубликовать материалы (например, сводную информацию), подтверждающие наличие у нее планов и средств обеспечения бесперебойной деятельности. Для проверки соблюдения требований при реализации итоговых планов обеспечения бесперебойной деятельности следует привлечь независимого аудитора.		Высокий
9	**Обеспечить целесообразность, осуществимость и тщательное документирование плана аварийного восстановления.** 9.1. Корпорация ICANN должна обеспечить, чтобы план DR для операций PTI (функций IANA) охватывал все уместные системы, способствующие безопасности и стабильности DNS, а также управление корневой зоной и соответствовал стандарту ISO 27031 *«Принципы готовности информационно-коммуникационных технологий к бесперебойной деятельности».* Корпорация ICANN должна разработать этот план в тесном сотрудничестве с RSSAC и операторами корневых серверов.		Высокий

[5] ISO 22301:2019 «Безопасность и отказоустойчивость. Системы менеджмента непрерывности бизнеса. Требования», https://www.iso.org/standard/75106.html.

	9.2. 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 «*Принципы готовности информационно-коммуникационных технологий к бесперебойной деятельности*». 9.3. У корпорации ICANN должен быть план аварийного восстановления, разработанный в течение двенадцати месяцев после принятия Правлением ICANN этих рекомендаций по созданию как минимум третьего центра для аварийного восстановления (в дополнение к площадкам в Лос-Анджелесе и Калпепере), а именно за пределами США, их территорий и североамериканского региона, в том числе план реализации. 9.4. Корпорация ICANN должна опубликовать сводную информацию о своих общих планах и средствах аварийного восстановления. Для проверки соблюдения требований при реализации этих планов DR корпорации ICANN следует привлечь независимого аудитора.		
10	**Улучшить концепцию определения степени соблюдения требований регистраторами и регистратурами** 10.1. Создать концепцию показателей эффективности для оценки уровня соблюдения регистраторами и регистратурами своих обязательств в отношении WHOIS (включая недостоверность данных) и других элементов, влияющих на злоупотребления, безопасность и отказоустойчивость, как указано в результатах анализа RDS/WHOIS2 и CCT.[67] 10.2. Выделить отдельную статью бюджета для группы должностных лиц отдела по контролю исполнения договорных обязательств, которым поручено активно тестировать и оценивать или заказывать тестирование и оценку согласованных показателей SLA в рамках управления эффективностью. 10.3. Изменить статью о продлении срока действия SLA с «автоматического продления» на периодическое продление на четыре года, предусмотрев оговорку о пересмотре (в период пересмотра будет рассматриваться уровень соблюдения регистраторами и регистратурами и показателей эффективности и в случае очевидного несоблюдения требований будут даваться рекомендации по включению требований, направленных на усиление безопасности и отказоустойчивости).		Высокий

6 Группа ICANN по анализу RDS-WHOIS, «Анализ службы каталогов регистрационных данных (RDS)-WHOIS2: итоговый отчет», 3 сентября 2019 года, https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf.

7 «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.

	10.4. Кроме того, Правление ICANN должно взять на себя ответственность за успешное завершение [8]EPDP, принятие и реализацию политики в области WHOIS в течение года после опубликования этого отчета.		
11	**Возглавить усилия по доработке определений, относящихся к злоупотреблениям, и обеспечить подготовку отчетности в соответствии с этими определениями.** 11.1. Правление ICANN должно приложить усилия, направленные на минимизацию двусмысленности формулировок и достижение универсально приемлемого соглашения о злоупотреблениях, SSR и угрозах безопасности в своих контрактах со сторонами, связанными договорными обязательствами, и планах реализации. 11.2. Корпорация и Правление ICANN должны безотлагательно выполнить обязательства, относящиеся к SSR (наряду с рекомендациями по результатам анализа CCT и RDS/WHOIS2), на основе текущих, проверенных сообществом определений злоупотреблений[9]. 11.3. Параллельно Правление ICANN должно привлечь внимание сообщества к доработке (и применению) определения злоупотребления DNS, а также утвердить дополнительный термин и меняющееся внешнее определение «угрозы безопасности» — термина, используемого в проекте ICANN Платформа отчетности о случаях злоупотребления доменами (DAAR) и GAC (в пекинском коммюнике[10] и для Спецификации 11[11]), а также в международных конвенциях, таких как Конвенция по киберпреступности и связанные с ней «Пояснительные		Высокий

8 Организация поддержки доменов общего пользования ICANN, «Ускоренный процесс формирования политики GNSO (EPDP) с целью подготовки рекомендаций по проекту политики в отношении Временной спецификации для регистрационных данных в gTLD для рассмотрения Правлением ICANN», 1 мая 2019 года, https://www.icann.org/public-comments/epdp-recs-2019-03-04-en.

9 В самом отчете по CCT есть определения как злоупотребления DNS, так и злоупотребления в области безопасности DNS, и в сноске 11 на стр. 8 с одобрением упомянуты определения, содержащиеся в документе персонала ICANN под названием «Меры защиты от злоупотребления DNS» от 18 июня 2016 года. Рабочая группа сообщества по вопросам политики борьбы со злоупотреблениями при регистрации (RAP) в 2010 году «на основе консенсуса сформулировала определение злоупотребления», которое гласит: «Злоупотребление — 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 планам законного использования, если цель использования была раскрыта». (Это определение упомянуто с одобрением в сноске 287 на стр. 88 итогового отчета по CCT)

10 Правительственный консультативный комитет ICANN, «Рекомендации GAC: Коммюнике по результатам заседаний на ICANN46 в Пекине», последняя редакция от 11 апреля 2013 года, https://gac.icann.org/contentMigrated/icann46-beijing-communique.

11 ICANN, «Соглашение об администрировании домена верхнего уровня», https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm.

	примечания» [12]— для использования совместно с определением злоупотребления DNS в корпорации ICANN.[13] 11.4. Правление ICANN должно поручить SSAC и PSWG в сотрудничестве с экспертами в области электронных преступлений и злоупотреблений доработать определение злоупотребления DNS с учетом процессов и определений, содержащихся в Конвенции по киберпреступности.		
12	**Создать законные и целесообразные механизмы доступа к данным WHOIS** 12.1. Правление ICANN должно создать законные и целесообразные механизмы доступа проверенных сторон, например правоохранительных органов, к данным WHOIS. 12.2. Правлению ICANN следует взять на себя ответственность и обеспечить незамедлительное завершение реализации корпорацией ICANN Временной спецификации для регистрационных данных в gTLD.		Высокий
13	**Повысить полноту и полезность программы «Платформа отчетности о случаях злоупотребления доменами»** 13.1. Правление ICANN и корпорация ICANN должны в сотрудничестве с организациями сообщества ICANN и сторонними организациями, которые занимаются борьбой со злоупотреблениями, повысить полноту и полезность DAAR, чтобы улучшить как измерение показателей, так и отчетность о злоупотреблениях доменами. 13.1.1. Корпорация ICANN должна указывать в публикуемых отчетах DAAR регистратуры и регистраторов, чьи домены в наибольшей степени способствуют злоупотреблениям согласно методологии DAAR. 13.1.2. Корпорация ICANN должна сделать доступными исходные данные для DAAR через программу ICANN «Открытые данные» и установить приоритетность элементов *«daar»* и *«daar-summarized»* в инвентаре информационных активов ODI[14] для незамедлительного доступа сообщества. 13.1.3. Корпорация ICANN должна публиковать отчеты, которые содержат данные в пригодных для машинного считывания форматах, в дополнение к графическим данным, представленным в текущих отчетах. 13.1.4. Корпорация ICANN должна оказывать содействие Правлению и всем группам интересов, группам заинтересованных сторон и консультативным комитетам в		Высокий

[12] Совет Европы, «Конвенция по киберпреступности», ETS № 185, стр. 7, 23 ноября 2001 года, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[13] См. примечание 50.

[14] См. документ https://www.icann.org/en/system/files/files/odi-data-asset-inventory-spreadsheet-11jun18-en.csv опубликованный офисом CTO: https://www.icann.org/public-comments/odi-datasets-metadata-2018-06-11-en.

	интерпретации результатов DAAR, включая помощь в определении деятельности по формированию политики и консультативной деятельности, которая будет способствовать предотвращению и смягчению последствий злоупотребления доменными именами.		
14	**Обеспечить возможность тщательного количественного анализа взаимосвязи между платежами за регистрацию доменов и признаками угроз безопасности и злоупотреблений** 14.1. Корпорация ICANN должна собирать, анализировать и публиковать данные о ценах, чтобы обеспечить возможность дальнейших независимых исследований и отслеживания взаимосвязи между ценообразованием и злоупотреблениями.		Высокий
15	**Улучшить контракты с регистраторами и регистраторами, чтобы стимулировать борьбу со злоупотреблением DNS** 15.1. Корпорация ICANN должна сделать требования SSR обязательным условием продления контракта или базового соглашения со сторонами, связанными договорными обязательствами, включая соглашение об администрировании домена верхнего уровня (базовое и индивидуальные) и RAA. Такие требования контракта должны включать положения, устанавливающие пороги злоупотреблений (например, 3% от всех регистраций), при превышении которых будет происходить автоматическая отправка уведомлений отделом по контролю исполнения договорных обязательств, и более высокий порог (например, 10% от всех регистраций), при достижении которого ICANN будет считать, что регистраторы и регистратуры нарушили свои обязательства по соглашениям. В отчете группы по анализу CCT также рекомендован этот подход.[15] 15.2. Корпорации ICANN следует ввести условие договора, которое позволяло бы расторгнуть договор в случае «участия в серии» злоупотреблений (как в разделе 5.5.2.4 «СРОК ДЕЙСТВИЯ, РАСТОРЖЕНИЕ И УРЕГУЛИРОВАНИЕ СПОРОВ» соглашения об аккредитации регистраторов в редакции от 2013 года)[16]. 15.3. Чтобы поддержать рассмотрение таких поправок к договорам, корпорация ICANN должна: 15.3.1. Обеспечить доступ сторон, имеющих законные цели, к регистрационным данным через договорные обязательства и строгие механизмы контроля их соблюдения.		Высокий

[15] См. рекомендации 14, 15 и 16 в документе «Конкуренция, потребительское доверие и потребительский выбор: итоговый отчет», https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[16] «Соглашение об аккредитации регистраторов в редакции от 2013 года», ICANN, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

	15.3.2. Установить и контролировать соблюдение единых требований к Централизованной службе файлов корневой зоны, обеспечивающих постоянный доступ к данным для исследований в области SSR. 15.3.3. Привлекать к сотрудничеству ccTLD и ccNSO, чтобы способствовать борьбе со злоупотреблением DNS и угрозами безопасности в ccTLD. 15.3.4. Правление, сообщество и корпорация ICANN должны сотрудничать с ccNSO для повышения качества отслеживания данных и отчетности, для оценки злоупотребления DNS и угроз безопасности в ccTLD, а также для разработки плана ccNSO, направленного на поддержку усилий ccTLD по дальнейшему сокращению объемов злоупотребления DNS и смягчению угроз безопасности. 15.3.5. Незамедлительно ввести требование к службам RDAP сторон, связанных договорными обязательствами, внести в белый список адресное пространство корпорации ICANN и установить процесс проверки других организаций, которых службы RDAP сторон, связанных договорными обязательствами, будут вносить в белый список для предоставления доступа без ограничений по скорости. 15.4. В более долгосрочной перспективе Правлению ICANN следует предложить GNSO инициировать процесс принятия новой политики и новых соглашений со сторонами, связанными договорными обязательствами, существенно улучшающих меры по борьбе со злоупотреблением DNS и смягчению угроз безопасности, включая изменения RDAP и сведений о владельцах доменов, стимулирование соответствующих усилий сторон, связанных договорными обязательствами, создание концепции показателей эффективности, а также институционализацию обучения и сертификации сторон, связанных договорными обязательствами, и ключевых заинтересованных сторон.		
16	**Создание ценовых стимулов для сторон, связанных договорными обязательствами, направленных на сокращение количества злоупотреблений и смягчение угроз безопасности** 16.1. Корпорация ICANN должна стимулировать противодействие злоупотреблениям и угрозам безопасности путем внесения в договоры следующих изменений: 16.1.1. Стороны, связанные договорными обязательствами, в портфеле которых процент доменных имен, используемых для злоупотреблений, меньше конкретного значения (например, 1%) (по данным коммерческих провайдеров или DAAR), должны получить скидку при уплате сборов (например, сокращение размера текущих сборов или увеличение текущего операционного сбора за каждое доменной имя и предоставление скидки регистратору).		Высокий

	16.1.2. Регистраторы должны получать скидку за каждое доменное имя, зарегистрированное проверенным владельцем домена, до целесообразного порогового значения. 16.1.3. Освобождать от необходимости уплаты сборов RSEP, когда в заявках RSEP четко указано, каким образом сторона, связанная договорными обязательствами, намерена бороться со злоупотреблением DNS, и предварительно одобрять все заявки регистратур в рамках RSEP, где разрешается в поле EPP на уровне регистратуры указывать, что эти доменные имена находятся под управлением проверенного владельца домена. 16.1.4. Возвращать сборы, взимаемые с регистраторов и регистратур за домены, которые были идентифицированы как используемые для злоупотребления или создающие угрозы безопасности и удалены в течение соответствующего срока после регистрации (например, в течение 30 дней после регистрации домена). 16.2. Учитывая, что все стороны (корпорация ICANN, стороны, связанные договорными обязательствами, и другие важные заинтересованные стороны, такие как регистратуры, регистраторы, поставщики услуг сохранения конфиденциальности и регистрации через доверенных лиц, а также интернет-провайдеры) должны понимать, каким образом можно точно измерить, отследить, выявить и идентифицировать злоупотребление DNS, корпорации ICANN следует институционализировать обучение и сертификацию всех сторон в областях, определенных на основе DAAR и других источников данных о распространенных злоупотреблениях **[ссылка будет добавлена]** и надлежащих мерах по их предотвращению. Обучение должно охватывать в качестве отправной точки: автоматическое отслеживание номеров жалоб и обработка жалоб; ежеквартальные/ежегодные публичные отчеты о жалобах и принятых мерах; анализ.		
17	**Создать центральный портал для сообщений о злоупотреблениях** 17.1. Корпорация ICANN должна создать и поддерживать центральный портал для жалоб на злоупотребление DNS, который обеспечивает автоматическую пересылку всех сообщений о злоупотреблениях соответствующим сторонам. Эта система использовалась бы исключительно для получения данных, на выход поступали бы только сводные данные и метаданные. Такую систему должны в обязательном порядке использовать все gTLD; при этом следует предложить ccTLD присоединиться. Ответы необходимо сделать общедоступными для поиска и включать в годовые отчеты (в полном виде или посредством ссылки). Кроме того, отчеты должны быть доступны (например, по электронной почте) не участвующим ccTLD.		Высокий

18	**Обеспечить беспристрастность и эффективность работы ICANN по контролю исполнения обязательств** 18.1. Корпорация ICANN должна проводить независимую проверку деятельности отдела по контролю исполнения договорных обязательств, чтобы он придерживался высоких стандартов. 18.2. Правление ICANN должно наделить этот отдел полномочиями реагирования на жалобы и требовать, чтобы он инициировал расследования и обеспечивал выполнение договорных обязательств лицами, способствующими и подстрекающими к системным злоупотреблениям, как определено в SLA. Эти дополнительные полномочия могут включать поддержку поэтапных действий по эскалации принудительных мер и надлежащие осуществимые меры, которые корпорация ICANN может принять в ответ на невыполнение требования об устранении нарушения обязательств в указанные сроки. 18.3. Отдел ICANN по контролю исполнения договорных обязательств должен, по умолчанию, использовать SLA для контроля и отчетности, осуществлять четкие и эффективные процессы, полностью информировать заявителя, оценивать степень удовлетворенности и в максимальном объеме раскрывать информацию.		Высокий
19	**Обновление обработки неправомерно присвоенных имен** 19.1. Корпорация ICANN должна опираться на текущую деятельность по расследованию типовых случаев регистрации имен, вводящих в заблуждение, в сотрудничестве с исследователями и заинтересованными сторонами, при наличии такой возможности. 19.2. Когда регистрация вводящего в заблуждение имени поднимается до уровня неправомерного присвоения имени, корпорация ICANN должна включать этот вид злоупотреблений в свои отчеты DAAR и разработать политику и рекомендации по передовой практике противодействия. 19.3. Корпорация ICANN должна публиковать на портале количество жалоб на неправомерное присвоение имен в форме, позволяющей независимым третьим сторонам анализировать, смягчать и предотвращать вред от использования таких доменных имен. 19.4. Корпорация ICANN должна обновить действующее «Руководство по внедрению IDN-доменов» **[ссылка будет добавлена]**, чтобы включить раздел об именах, содержащих товарные знаки, использующих создание цепочки TLD и (трудно обнаруживаемые) опечатки. Кроме того, ICANN должна на контрактной основе обеспечить соблюдение «Руководства по внедрению IDN-доменов» для gTLD и рекомендовать ccTLD сделать то же самое.		Высокий

20	**Завершить разработку регрессивного тестирования DNS** 20.1. Корпорация ICANN должна завершить разработку пакета для регрессивного тестирования DNS.[17] 20.2. Корпорация ICANN должна обеспечить возможность реализации и поддержки функционального тестирования различных конфигураций и версий программного обеспечения.		Высокий
21	**Выполнить рекомендации из документов SAC063 и SAC073 и установить формальные процедуры обновления ключа** 21.1. Корпорация ICANN должна выполнить рекомендации из документов SAC063 и SAC073, чтобы обеспечить SSR процесса обновления ключа KSK. 21.2. Корпорация ICANN должна установить формальную процедуру, опирающуюся на формальный инструмент и язык моделирования [18]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, FSM) для общественного обсуждения; отзывы сообщества должны быть приняты во внимание. 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 можно было использовать извлеченные уроки для корректировки процесса. 21.3. 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.		Высокий
22	**Установить базовые методы обеспечения безопасности для операторов и функционирования корневых серверов** 22.1. Корпорация ICANN в тесном сотрудничестве с RSSAC и другими заинтересованными сторонами должна включить в состав модели управления RSS, предложенной в		Высокий

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

18 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)

	документе RSSAC037, базовые методы обеспечения безопасности для операторов и функционирования корневых серверов, чтобы минимизировать риски RSS, связанные с работой корневых серверов. Эти передовые методы должны охватывать управление изменениями, процедуры верификации и процедуры проверки работоспособности. 22.2. Корпорация ICANN также должна разработать соответствующие KPI для оценки реализации этих передовых методов и требований и обеспечить ежегодную публичную отчетность о соблюдении этих KPI операторами корневых серверов (RSO) и другими соответствующими сторонами, включая корпорацию ICANN. 22.3. Корпорация ICANN должна задокументировать стратегии повышения безопасности корневого сервера, находящегося под управлением ICANN (IMRS), широко известного как корневой сервер L, и должна рекомендовать другим RSO поступить аналогичным образом. 22.4. Корпорация ICANN должна обеспечить использование для IMRS процесса раскрытия информации об уязвимостях (не обязательно публичного), отчетов по вопросам безопасности, связи с исследователями и советов или рекомендаций RSSAC, где это применимо.		
23	**Ускорить внедрение RZMS нового поколения** 23.1. ICANN и PTI должны ускорить внедрение новых мер безопасности RZMS, касающихся аутентификации и авторизации запрошенных изменений. 23.2. Корпорация ICANN должна как можно скорее начать общественное обсуждение изменений политики RZMS.		Высокий
24	**Составить список статистических данных и показателей, отражающих рабочее состояние систем уникальных идентификаторов.** 24.1. Корпорация ICANN должна составить список статистических данных и показателей, отражающих рабочее состояние (например, доступность и скорость отклика) каждого вида источников данных об уникальных идентификаторах, таких как служба, связанная с корневой зоной, реестры IANA и все службы gTLD, входящие в сферу компетенции корпорации ICANN. 24.2. Корпорация ICANN должна опубликовать каталог этих служб, массивов данных и показателей на одной странице своего сайта, например, в рамках платформы для открытых данных. 24.3. ICANN должна публиковать сводки этих данных за каждый год и за более длительные периоды, запрашивать отзывы общественности об этих сводках и учитывать такие отзывы для улучшения будущих отчетов. 24.4. Для обоих наборов KPI корпорация ICANN должна составлять сводки как за предыдущий год, так и за более		Средний

	длительный период, запрашивать и публиковать сводку отзывов сообщества о каждом отчете и учитывать такие отзывы для улучшения будущих отчетов.		
25	**Обеспечить постоянную возможность централизованного доступа к данным файлов зон** 25.1. Сообщество ICANN и корпорация ICANN должны предпринять шаги, обеспечивающие своевременный доступ к CZDS, а также к другим данным, без лишних препятствий для запрашивающих данные лиц. 25.2. Корпорация ICANN должна выполнить четыре рекомендации, сформулированные в документе SSAC 97:[19] *«Рекомендация 1: SSAC рекомендует Правлению ICANN предложить персоналу ICANN рассмотреть возможность изменения системы CZDS для решения проблемы, вызванной тем, что по умолчанию срок подписки истекает автоматически, например, разрешив автоматическое продление подписки по умолчанию. При этом можно предусмотреть вариант, позволяющий оператору регистратуры отказаться от значения по умолчанию для каждого подписчика, что заставит выбранного подписчика повторно подать заявку по истечении текущего срока. CZDS должна по-прежнему позволять операторам регистратур в любой момент напрямую отказать проблемному подписчику в доступе.* *Рекомендация 2: SSAC рекомендует Правлению ICANN предложить персоналу ICANN при проведении последующих раундов создания новых gTLD обеспечить изменение соглашения о подписке на CZDS сообразно изменениям, внесенным в результате выполнения рекомендации 1.* *Рекомендация 3: SSAC рекомендует Правлению ICANN предложить персоналу ICANN заняться поиском путей сокращения количества жалоб в связи с проблемами доступа к файлу корневой зоны и своевременного устранения проблем, которые явились поводом для жалоб.* *Рекомендация 4: SSAC рекомендует Правлению ICANN предложить персоналу ICANN обеспечить точность и*		Высокий

[19] 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.

	открытость отчетов о доступе к файлу корневой зоны и статистики запросов к веб-интерфейсу службы WHOIS в соответствии с четко определенными стандартами, которые соблюдаются всеми операторами регистратур gTLD. Показатель доступа к файлу корневой зоны (ZFA) необходимо уточнить в кратчайшие сроки.		
26	**Задокументировать, улучшить и протестировать процессы EBERO** 26.1. Корпорация ICANN должна публично задокументировать процессы EBERO, включая точки принятия решений, действия и исключения. Документ должен описывать взаимозависимые элементы для каждого решения, действия и исключения. 26.2. По возможности, корпорация ICANN должна автоматизировать эти процессы и ежегодно их тестировать. 26.3. Корпорация ICANN должна публично проводить «дымовое» тестирование EBERO с заранее установленной периодичностью, используя план тестирования, которые заранее согласован со сторонами, связанными с ICANN договорными обязательствами, чтобы обеспечить отработку всех ветвей исключения и опубликовать результаты. 26.4. Корпорации ICANN следует улучшить этот процесс, разрешив провайдеру услуг временного депонирования данных gTLD отправлять депонированные данные напрямую провайдеру EBERO.		Высокий
27	**Обновить DPS и достичь консенсуса в отношении будущих обновлений алгоритма DNSKEY** 27.1. Сотрудники PTI должны обновить DPS, чтобы способствовать смене алгоритма цифровой подписи, включая ожидаемый переход от алгоритма цифровой подписи RSA к алгоритму ECDSA или к будущим пост-квантовым алгоритмам, которые увеличат отказоустойчивость DNS, сохранив или повысив при этом степень безопасности. 27.2. 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.		Средний
28	**Подготовить отчет о периодичности измерения доменных коллизий и предложить решение**		Средний

	28.1. Корпорация ICANN должна представить результаты, которые позволят определить характер и частоту доменных коллизий и возникающие в результате этого проблемы. Сообщество ICANN должно внедрить решение до следующего раунда создания gTLD. 28.2. Корпорация ICANN должна содействовать этому процессу, организовав независимое исследование доменных коллизий, дождаться полного завершения этого исследования и принять, учесть при реализации или отклонить каждую из итоговых рекомендаций. Используя понятие «независимое» исследование RT SSR2 подразумевает, что корпорация ICANN должна обеспечить проверку выводов группы по оценке исследования и отчета, выполненного рабочей группой проекта по анализу доменных коллизий (NCAP) SSAC, сторонами, не имеющими финансовой заинтересованности в расширении пространства TLD. 28.3. Корпорация ICANN должна разрешить сообществу сообщать о случаях доменных коллизий. Для этих сообщений, которые следует включить в состав показателей отчетности перед сообществом, необходимо предусмотреть надлежащую обработку данных, требующих особенного внимания, и предотвращение угроз безопасности.		
29	**Сосредоточить внимание на конфиденциальности, измерении SSR и совершенствовании политики на основе результатов этих измерений** 29.1. Корпорация ICANN должна отслеживать и регулярно сообщать о влиянии на конфиденциальность таких технологий, как DoT (DNS по TLS) и DoH (DNS по HTTPS). 29.2. Соответственно, согласованная политика и соглашения корпорации ICANN с операторами регистратур и регистраторами должны содержать положения, отражающие такие требования, но гарантирующие при этом отсутствие фрагментации DNS из-за необходимости выполнения минимальных требований, регламентирующих сбор, хранение, временное депонирование, передачу и отображение 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. 29.3. Корпорация ICANN должна: 29.3.1. Создать специализированные подразделения в рамках функции по контролю исполнения договорных обязательств, в центре внимания которых будут находиться требования и принципы конфиденциальности (такие как ограничение сбора, классификация данных, определение целевого назначения и меры безопасности при раскрытии) и которые могут способствовать удовлетворению потребностей правоохранительных органов в процессе развития концепции RDAP.		Высокий

	29.3.2. Отслеживать изменение и развитие законов о конфиденциальности (например, CCPA и законов о защите информации, позволяющей установить личность (PII)) и обеспечивать соответствие политики и процедур корпорации ICANN требованиям соответствующих законов и нормативных актов в отношении сохранения конфиденциальности и защиты информации, позволяющей установить личность.[20] 29.3.3. Разработать и обновлять политику защиты информации, позволяющей установить личность. Эта политика должна быть доведена до сведения всех лиц, участвующих в обработке личной информации. Следует принять технические и организационные меры для надлежащей защиты PII. 29.3.4. Проводить периодическую проверку соблюдения политики конфиденциальности регистраторами, чтобы убедиться в наличии у них, как минимум, процедур для устранения нарушений конфиденциальности. 29.4. DPO корпорации ICANN также должен нести ответственность за PII во внешней DNS. DPO должен давать руководящие указания менеджерам и заинтересованным сторонам в отношении обязанностей и процедур, а также следить за важными техническими разработками и сообщать о них.		
30	**Оставаться в курсе научных исследований в области SSR и использовать эту информацию при обсуждении политики** 30.1. 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, IEEE S&P, а также конференции по оперативной безопасности APWG, M3AAWG и FIRST, и публиковать для сообщества ICANN отчет, в котором обобщаются последствия публикаций, имеющих отношение к работе корпорации ICANN или сторон, связанных договорными обязательствами. 30.1.1. Эти отчеты должны содержать 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.		Средний

[20] Группе по анализу известно о хартии корпорации ICANN, в которой описан ее подход к взаимодействию с правительствами https://www.icann.org/en/system/files/files/proposed-org-engagement-govt-standards-charter-25feb19-en.pdf и Отчете о законодательных инициативах (Системе отслеживания) https://www.icann.org/legislative-report-2019. Однако мы хотели бы добиться более пристального внимания к конфиденциальности и защите данных.

	30.1.2. В состав этих отчетов также должны входить рекомендации о проведении дополнительных исследований для подтверждения результатов коллегиальных научных выводов, описание того, какие данные потребуются для выполнения дополнительных рекомендуемых исследований, и как ICANN может способствовать получению доступа к таким данным, например, CZDS.		
31	**Уточнить последствия внедрения технологии DNS-по-HTTP для SSR** 31.1. Корпорация ICANN должна заказать независимое исследование последствий внедрения технологии DoH для SSR, а также влияния будущей роли IANA в экосистеме интернета. Ожидается, что в результате этого все заинтересованные стороны смогут понять последствия указанных изменений в области SSR, а также диапазон альтернатив (или отсутствие таковых), которые доступны различным заинтересованным сторонам для оказания влияния на будущее.		Высокий

Указания будущим группам по анализу SSR — выводы

Чтобы будущим группам по анализу SSR было проще выполнить оценку, RT SSR2 постарается сформулировать свои рекомендации в соответствии с критериями SMART: везде, где это возможно, рекомендации будут *конкретными, измеримыми, назначаемыми, актуальными и отслеживаемыми*. RT SSR2 считает, что более четкие и ориентированные на действия рекомендации упростят процесс реализации, отслеживания и оценки при следующем анализе SSR. RT SSR2 включила дополнительную информацию о своем процессе и методологии выполнения задач, сформулированных в мандате RT SSR2, в «Приложение C:Процесс и методология».