ООО «ТЦИ»

ПОЛИТИКА УПРАВЛЕНИЯ DNSSEC

[ТЦИ-DNSSEC-1]

Версия 1.0

СЛУЖЕБНАЯ ИНФОРМАЦИЯ

№ п/п	Тип служебной информации	Служебная информация
1	Владелец документа	Начальник отдела информационной безопасности
2	Утвержден	Приказом генерального директора ООО «ТЦИ» № 09-ИБ от 01.10.2019г.
3	Дата введения	с «01» октября 2019 г. Вводится впервые.
4	Срок действия	До замены (отмены)
5	Назначение документа	Настоящий документ разработан с целью описания процедур DNSSEC, используемых ООО «ТЦИ» для подписания национальных доменов «.РФ» и «.RU», а также «.SU», «.ДЕТИ», «.TATAR».
6	Область действия	Положения настоящего Документа распространяются на всех сотрудников, вовлеченных в процесс обеспечения функционирования DNSSEC в зонах национальных доменов «.РФ» и «.RU», а также «.SU», «.ДЕТИ», «.TATAR».
7	Ответственность	Ответственность за поддержание актуальности настоящего Документа и его пересмотр, возлагается на Начальника отдела информационной безопасности. Порядок внесения изменений в Документ: 1) не подлежит периодическому пересмотру; 2) изменения вносятся при необходимости приведения в соответствие с процедурами DNSSEC, рекомендованными к реализации ICANN.

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ, ТЕРМИНЫ И ПОНЯТИЯ

Домен — область (ветвь) иерархического пространства доменных имен сети Интернет, которая обозначается уникальным идентификатором - доменным именем или именем домена.

Администрирование домена — определение *администратором домена* порядка использования домена. Право администрирования существует в силу договора о регистрации доменного имени и действует с *момента* регистрации доменного имени в течение *срока действия регистрации*.

Регистрация доменного имени — внесение в Реестр информации о доменном имени.

Делегирование домена (делегирование) — размещение и хранение информации о DNS-серверах делегируемого домена в DNS-серверах домена верхнего уровня.

Срок действия регистрации - интервал времени, устанавливаемый администратором домена верхнего уровня.

Аннулирование регистрации — исключение информации о доменном имени из Реестра.

Реестр – (синоним термина «главный реестр») - хранилище информации, выполняющее регламентированные данным документом действия с хранимой информацией.

ТЦИ – (синоним «**Технический Центр**», «**ТЦ**») – ООО «ТЦИ», обеспечивающее функционирование системы регистрации.

Система регистрации - программно-аппаратный комплекс, реализующий протоколы взаимодействия регистратора с одним и более реестрами, обеспечивающий размещение главных реестров в виде баз данных и функционирование системы адресации сети Интернет (системы DNS).

Идентификатор – уникальная последовательность символов.

Объект – структурированный набор записей в реестре, имеющий идентификатор и относящийся к определённому типу.

Атрибут объекта – поле объекта, в котором сохраняются имя атрибута и значение атрибута.

Тип объекта – определяет назначение объекта и процедуры, которые могут быть выполнены над объектом;

Процедура – действие, изменяющее значения атрибутов объекта, создающее объект в реестре, либо удаляющее объект из реестра.

Управление объектом –выполнение разрешенных процедур над объектом.

Состояние объекта – возможность выполнения определённых процедур с объектом.

Статус – значение атрибута объекта в виде определённой последовательности символов, определяющее состояние объекта.

Периоды жизни – периоды хранения информации об объекте в реестре фиксированной продолжительности, в течение которых объект имеет определённые статусы и, в течение которых над объектом могут выполняться определённые процедуры.

Субординатный (сервер или домен) – сервер или домен, имеющий интернет-адрес вида qq.domainame.tld, где qq – имя сервера или домена, domainname.tld – имя домена верхнего уровня. Сервер или домен qq.domainame.tld является субординатным по отношению к домену domainname.tld. Домен domainname.tld в свою очередь является субординатным по отношению к домену верхнего уровня .tld.

Техническая политика реестра – набор параметров, которые могут отличаться у разных доменов верхнего уровня, согласно Правилам регистрации доменов в этих реестрах. Набор параметров также варьируется в зависимости от технической возможности предоставления доступа к различным реестрам и от порядка оказания услуг доступа к различным реестрам.

ДВУ – домен верхнего уровня «.РФ» (XN--P1AI), «.RU», «.SU», «.ДЕТИ», «.TATAR».;

DNSSEC - расширение DNS, предназначено для обеспечения мер безопасности при делегировании доменов;

KSK (англ. Key Signing Key) – ключ для подписи ресурсной записи DNSKEY;

ZSK (англ. Zone Signing Key) – ключ для подписи ресурсных записей;

KSR (англ. Key Signing Request) – запрос на подпись ключей DNSSEC;

SKR (англ. Signed Key Response) – подписанный набор ключей DNSSEC.

ВВЕДЕНИЕ

1.1. Обзор

Данный документ описывает основные процедуры и меры, принятые для внедрения DNSSEC в домене верхнего уровня (далее – ДВУ).

1.2. Название документа

Политика управления DNSSEC.

1.3. Сообщество и применимость

1.3.1. Регистратура

Регистратура ДВУ обладает полномочиями по выработке правил регистрации доменных имен в ДВУ, в том числе выработку политики DNSSEC по рекомендациям ICANN, а также отвечает за аккредитацию регистраторов. Регистратура использует ООО “Технический Центр Интернет” (далее - ТЦИ) как внешнего субподрядчика для технической эксплуатации Реестра. ТЦИ отвечает за: функционирование Реестра и систему регистрации в ДВУ; проверку и обработку данных DNSSEC, полученных от аккредитованного регистратора; формирование и подписание ресурсных записей в файле ДВУ; управление ZSK и распространение ДВУ по надлежащим серверам DNS.

1.3.2. Регистратор

Регистратор - юридическое лицо, аккредитованное регистратурой ДВУ. Регистрация новых доменных имен и размещение DS записей для них в ДВУ осуществляется аккредитованными регистраторами. Аккредитованные регистраторы несут ответственность за проверку принадлежности ключа KSK администратору доменного имени.

1.3.3. Администратор домена

Администратор домена - лицо, заключившее договор о регистрации доменного имени с регистратором и осуществляющее администрирование данного домена.

Администраторы доменных имен, размещенных в ДВУ, вносят необходимые изменения с помощью аккредитованных регистраторов и несут ответственность за правильность подписи своей доменной зоны, а также за актуальность размещенных в реестре открытых ключей в виде DS-записей в соответствии со своими потребностями.

1.3.4. Заинтересованные стороны

Заинтересованные стороны – участники сети Интернет, которые полагаются на работу DNSSEC, например, валидирующие DNS-серверы. Заинтересованные стороны несут ответственность за настройку и обновление надлежащих доверенных открытых ключей на своем оборудовании.

1.3.5. **Применимость**

Применение DNSSEC в субординатных доменах выходит за рамки данного документа и описывается администраторами этих доменов.

1.4. **Управление документом**

Данный документ будет пересматриваться и обновляться в случае необходимости.

1.4.1. **Организация**

Организация, ответственная за внесение изменений в данный документ, - ООО “Технический Центр Интернет”

1.4.2. **Контактная информация**

127083, г. Москва, улица 8 Марта, дом 1, строение 12, офис Э. 7, ПМ. XL К. 23-32;

Телефон: +7 (495) 730-29-69.

1.4.3. **Процедуры изменения документа**

Любое изменение в данном документе должно быть согласованно начальником отдела информационной безопасности ТЦИ.

ПУБЛИКАЦИЯ ОТКРЫТЫХ КЛЮЧЕЙ И РЕПОЗИТАРИИ

1.5. **Репозитарии**

ТЦИ публикует информацию, относящуюся к функционированию DNSSEC в ДВУ, на официальном сайте компании в соответствующем разделе, доступном по адресу:

https://www.tcinet.ru/documents

Электронная версия этого документа, находящаяся по приведенной выше ссылке, является официальной версией этого документа.

1.6. **Контроль доступа к репозитариям**

Информация, опубликованная на официальном сайте ТЦИ, защищена от несанкционированного удаления или модификации. При доступе к официальному сайту ТЦИ рекомендовано проверять сертификат SSL.

1.7. **Публикация ключа для подписи ключей**

ТЦИ составляет цепочку доверия DNSSEC, публикуя открытый KSK в форме DS-записи непосредственно в корневой зоне DNS.

ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ

1.8. **Активация DNSSEC для субординатного домена**

Для активации DNSSEC в субординатном домене необходимо разместить DNSKEY запись и соответствующую ей DS запись в реестре ДВУ. ТЦИ проверяет данные на корректность, выполняя следующие тесты: Проверка поддержки реестром алгоритма, по которому сформирована DS-запись; Проверка подписи; Проверка тега ключа.

Если домен делегирован и проверка DS-записи прошла успешно, то DS-запись для данного домена будет опубликована в DNS. Опубликованная DS-запись устанавливает цепочку доверия к субординатному домену.

1.9. **Идентификация и аутентификация администратора домена**

Надежная идентификация и аутентификация администратора субординатного домена входит в обязанности регистратора, с помощью подходящих для этого способов.

1.10. **Регистрация DS-записей**

ТЦИ принимает DNSKEY-записи и соответствующие им DS-записи от регистраторов, используя EPP-интерфейс. DS и DNSKEY записи должны быть корректными и отправлены в формате, описанном в RFC 4310. Реестр ТЦИ поддерживает размещение DS-записей, сформированных в соответствии с RFC 4034 и RFC 5933

1.11. **Способ определения владельца закрытого ключа**

ТЦИ не выполняет дополнительных проверок с целью достоверного определения, что администратор субординатного домена владеет закрытым ключом. Выполнение надлежащих проверок возлагается на регистраторов.

1.12. **Удаление DS-записей**

ТЦИ удаляет из реестра DNSKEY-запись и соответствующую ей DS-запись при получении от регистратора соответствующего запроса через EPP-интерфейс. Удаление всех DNSKEY-записей и соответствующих им DS-записей для субординатного домена деактивирует DNSSEC для этого домена. Только администратор субординатного домена или сторона, официально уполномоченная представлять интересы администратора субординатного домена, могут при помощи регистратора отправить запрос на удаление DS-записи для этого домена.

СРЕДСТВА УПРАВЛЕНИЯ И ЭКСПЛУАТАЦИОННЫЙ КОНТРОЛЬ

1.13. Физические средства управления

1.13.1. Площадка проведения процедур и её конфигурация

ТЦИ располагает несколькими объектами на территории России. Эти объекты включают в себя: защищенные от несанкционированного доступа серверные стойки в центрах обработки данных, подготовленное основное помещение для проведения процедур в офисе ТЦИ и резервное помещение в одном из центров обработки данных.

1.13.2. Физический доступ

К объектам ТЦИ организован ограниченный доступ, который предоставляется только уполномоченному персоналу.

1.13.3. Электропитание и кондиционирование воздуха

Объекты ТЦИ оснащены источниками бесперебойного питания и системами кондиционирования воздуха. Оборудование ТЦИ, расположенное в центрах обработки данных, имеет резервные источники питания, на случай выхода из строя одного из них.

1.13.4. Подверженность затоплению

ТЦИ предприняты меры предосторожности для минимизации влияния водного воздействия на оборудование.

1.13.5. Пожарная безопасность

Объекты ТЦИ оснащены пожарными датчиками и централизованной системой пожаротушения.

1.13.6. Хранение информации

Критичные носители информации размещаются в сейфах, доступ к которым предоставляется только уполномоченному персоналу.

1.13.7. Уничтожение информации

Критичные документы уничтожаются способом измельчения. Электронные носители информации перед утилизацией подвергаются специальному форматированию для исключения возможности восстановления информации, ранее записанной на эти носители.

1.13.8. Резервная копия

ТЦИ создает резервные копии критических системных данных. Резервные носители критичной информации располагаются на резервных площадках. Эти носители информации защищены от несанкционированного доступа.

1.14. **Процедурные средства управления**

Для работы с закрытым KSK созданы две доверенные роли: **крипто-офицер** и **крипто-оператор,** каждая из которых состоит минимум из двух допущенных лиц. Каждое из допущенных лиц имеет персональный идентификатор и пароль к нему. Генерацию, выдачу, замену, уничтожение персональных идентификаторов **крипто-офицеров** и паролей (ПИН-кодов) к ним осуществляет ТЦИ, с отражением всех действий в журналах учета. Для работы с закрытым KSK необходимо наличие минимум двух крипто-офицеров и одного крипто-оператора. Сотрудник, привлеченный к работе с закрытым KSK, не может одновременно совмещать роли **крипто-офицера** и **крипто-оператора.**

Для работы с ZSK создана доверенная роль: **администратор доменной зоны,** которая состоит минимум из двух допущенных лиц. Для контроля и управления ключами ZSK в полуавтоматическом режиме необходимо хотя бы одно допущенное лицо.

Для контроля над ходом выполнения ключевых процедур может быть создана роль: **Наблюдатель -** внешний эксперт, который, после прохождения согласовательного процесса в регистратуре, допускается к присутствию при выполнении работ по подписи доменных зон.

1.15. **Средства управления персоналом**

1.15.1. **Квалификация и опыт**

Выше описанный персонал является сотрудниками ТЦИ, АО «ЦВКС «МСК-IX», принимающими участие в процессе обеспечения функционирования сервисов DNS, либо лицами, специально утвержденными регистратурой АНО «Координационный центр национального домена сети Интернет» на роль **крипто-офицера**. Для исполнения обязанностей **крипто-офицера** назначаются российские интернет-эксперты с опытом работы в телекоммуникационных и интернет компаниях не менее 5 лет. Обязанности крипто-офицера исполняются на добровольной основе. Оплата за исполнение этих обязанностей не предусмотрена

1.15.2. **Требования к подготовке**

Новые сотрудники, перед вступлением в вышеописанные роли, должны изучить внутреннюю документацию, описывающую реализацию DNSSEC в ТЦИ. Они также должны принять участие в ключевых процедурах в качестве наблюдателей перед началом исполнения своих обязанностей.

1.15.3. **Переподготовка**

ТЦИ периодически проверяет готовность персонала к проведению процедур и осуществляет переподготовку по мере необходимости.

1.15.4. **Документация**

Документация, описывающая порядок выполнения процедур, доступна для всех вовлеченных сотрудников.

1.16. **Учет доступа**

Каждый факт доступа в специально отведенную зону работы с критичной информацией DNSSEC сохраняется в автоматизированной системе учета. В тех зонах, где автоматизация невозможна факты доступа протоколируется в специальных журналах. Журналы и сохраненные протоколы автоматизированной системы учета доступа регулярно просматриваются и анализируются. Периодичность анализа определяется политикой информационной безопасности ТЦИ. При анализе журналов доступа строго выполняется разделение ролей между лицом (лицами), проводящим (и) анализ, и теми, чьи действия подвергаются мониторингу.

1.17. **Компрометация и восстановление после сбоя**

Если некоторое событие привело или может привести к нарушениям безопасности, то проводится внутреннее расследование с целью выявления причин произошедшего и их устранения. Если данное событие компрометирует критичную информацию DNSSEC, то происходит аварийная замена ключей. Инициирует процедуру аварийной замены ключей крипто-оператор. В случае компрометации ключа ТЦИ продолжит эксплуатацию этого ключа до завершения процедуры аварийной замены ключей.

Технические средства безопасности

1.18. Генерация ключей и их внедрение

1.18.1.1. Генерация ключей

Создаваемые ключи KSK генерируются и хранятся в специализированном устройстве, называемом HSM (Hardware Secure Module – Аппаратный модуль защиты), у которого отсутствует подключение к сетевой инфраструктуре. Все операции с использованием криптографических преобразований, требующие участия закрытого KSK, выполняются на этом устройстве или на идентичном ему, которое используется в качестве резервного. Для обеспечения безопасности закрытый KSK может покидать устройство только в зашифрованном виде.

Создаваемые ключи ZSK генерируются и хранятся на сервере подписания, который подключен к внутренней сети реестра доменов верхнего уровня. Все операции с использованием криптографических преобразований, требующие участия закрытого ZSK, выполняются на этом устройстве или на идентичном ему, которое используется в качестве резервного. Для обеспечения безопасности закрытый ZSK может покидать устройство только в зашифрованном виде.

1.18.1.2. Распространение открытого ключа

Открытый KSK распространяется среди сообщества средствами протокола DNS.

1.18.1.3. Параметры генерации открытого ключа и проверка качества

Задание параметров и проверка качества ключевой информации осуществляется ТЦИ.

1.18.1.4. Применение ключа

ТЦИ использует ключевую информацию исключительно для подписи зоны домена верхнего уровня.

1.19. Средства защиты закрытого ключа

1.19.1.1. Контроль несколькими людьми за использованием закрытого ключа

Операции, требующие закрытой части KSK, выполняются крипто-офицерами и крипто-операторами в порядке, определённом в секции «Процедурные средства управления». Персональный идентификатор крипто-офицера содержит часть парольной фразы, необходимой для получения доступа к защищённому диску на HSM. Для восстановления пароля достаточно участия крипто-офицеров в количестве m<n, где n – общее количество частей парольной фразы (крипто-офицеров).

1.19.1.2. **Резервное копирование закрытого ключа**

Периодически выполняется резервное копирование закрытого ключа. Закрытый ключ покидает устройство исключительно в зашифрованном виде. Резервная копия закрытого KSK содержится в зашифрованном виде отдельно от HSM в хранилище, доступ к которому контролируется крипто-оператором, и может быть расшифрована крипто-офицерами.

Резервная копия закрытого ZSK хранится на резервном сервере подписания с горячим подключением, расположенном на резервной площадке, и включается в каждую резервную копию базы данных реестра.

1.19.1.3. **Архивация закрытого ключа**

Выведенные из использования закрытые ключи хранятся исключительно в виде резервных копий.

1.19.1.4. **Перемещение закрытого ключа**

Закрытые ключи могут быть извлечены из устройств подписания в зашифрованном виде и восстановлены на резервных системах уполномоченным персоналом в порядке, определённом в секции «Процедурные средства управления».

1.19.1.5. **Способ активации закрытого ключа**

Доступ к закрытому KSK открывается после открытия доступа к HSM и после дешифрования защищённого диска. Крипто-оператор обеспечивает доступ крипто-офицеров к консоли HSM. Крипто-офицеры используют персональные идентификаторы для дешифрования защищённого диска.

Доступ к закрытому ZSK обеспечивается Администратором доменной зоны из интерфейса управления DNSSEC.

1.19.1.6. **Способ деактивации закрытого ключа**

Доступ к закрытому KSK прекращается автоматически немедленно после проведения операции подписания.

Закрытый ключ ZSK хранится в онлайновой части системы и находится активном состоянии пока у этого ключа статус "Active". Изменение статуса ZSK может быть выполнено из интерфейса управления DNSSEC администратором зоны.

1.19.1.7. **Способ уничтожения закрытого ключа**

Не предполагается уничтожение закрытых ключей. Они могут быть удалены из системы с целью недопущения их использования в будущем.

1.20. Примечания к управлению ключевыми парами

1.20.1.1. Резервное копирование открытых ключей

Открытые ключи подвергаются резервному копированию при проведении плановых процедур резервного копирования на устройствах.

1.20.1.2. Сроки использования ключей

Срок действия KSK устанавливается в один год, ZSK – три месяца. Оператор реестра при необходимости может изменить данные сроки. Устаревшие ключи не используются повторно.

1.21. Данные для активации

1.21.1.1. Генерация данных для активации и их внедрение

Данные для доступа к KSK представляют собой набор паролей к персональным идентификаторам крипто-офицеров и паролей к персональным идентификаторам крипто-операторов (PIN-коды).

1.21.1.2. Защита данных для активации

Крипто-офицеры и крипто-операторы обеспечивают сохранность данных для доступа в соответствии с рекомендациями по безопасности.

1.21.1.3. Примечания по работе с данными для активации

В качестве экстренной меры крипто-офицеры и крипто-операторы хранят копии парольных данных в индивидуальных опечатанных пеналах, хранящихся в безопасном месте.

1.21.2. Средства управления компьютерной безопасностью

Все критичные для деятельности ТЦИ компоненты располагаются на защищённых от несанкционированного доступа площадок. Разграничение доступа проводится среди уполномоченного персонала в соответствии с их должностными обязанностями; осуществляется учёт фактов получения доступа.

1.21.3. Средства управления сетевой безопасностью

Онлайновая часть системы подписания присоединяется к внутренней сети ТЦИ, которая логически отделена от внешней сети. Подключение к данной онлайновой части возможно исключительно через межсетевой экран, при этом межсетевой экран предоставляет минимально необходимые для осуществления управления возможности.

Содержащая KSK часть системы подписания не имеет сетевого подключения. Передача запроса на подписание ключевого набора (KSR) осуществляется через съёмный носитель.

1.21.4. **Метки времени**

Онлайновая часть системы подписания осуществляет синхронизацию времени с доверенным источником во внешней сети. Установка времени в офлайновой части системы осуществляется вручную при каждом включении HSM.

1.21.5. **Средства управления жизненным циклом**

1.21.5.1. **Системные средства управления разработкой**

Разрабатываемые ТЦИ приложения используют системы контроля версий. Перед внедрением в рабочий реестр предоставляемые третьей стороной разработки проходят лабораторное тестирование на совместимость с разработками ТЦИ.

1.21.5.2. **Средства управления безопасностью**

ТЦИ проводит периодический аудит безопасности.

1.21.5.3. **Средства управления безопасностью жизненного цикла**

Системы подписания разработаны с учётом минимизации обслуживания. Критичные с точки зрения безопасности и функциональности обновления применяются после прохождения лабораторного тестирования.

1.22. **Подпись доменной зоны**

1.22.1. **Длины и алгоритмы ключей**

В системе подписания применяются необходимые с точки зрения безопасности на протяжении периода использования длины ключей и их алгоритмы. Текущим алгоритмом для KSK и ZSK является RSA-SHA256 с длиной ключа 2048 и 1024 бит соответственно.

1.22.2. **Авторитетное подтверждение отсутствия домена**

Для авторитетного подтверждения отсутствия домена используется механизм NSEC3 OPT-OUT, [RFC 5155].

1.22.3. **Формат подписи**

Подпись формируется по алгоритму RSA и хешированием по SHA256, [RFC 5702].

1.22.4. **Ротация ZSK**

Для ротации ZSK применяется схема с предварительной публикацией, [RFC 4641].

1.22.5. **Ротация KSK**

Для ротации KSK применяется схема с двойной подписью, [RFC 4641].

1.22.6. **Время действия подписей и частота обновления подписи**

Время жизни подписи для ключевого набора устанавливается в 20 дней. Для записей других типов время жизни подписей устанавливается в 45 дней. Обновление подписи зоны осуществляется каждые 2 часа.

Данные параметры могут быть изменены при необходимости.

1.22.7. **Проверка набора ключей**

При создании состоящего из открытых ключей KSK и ZSK ключевого набора (KSR) происходит подписание последнего при помощи содержащегося в онлайновой части системы ключа PGP реестра. Офлайновая часть системы автоматически проверяет подпись KSR при помощи предварительно импортированного открытого ключа PGP реестра перед принятием KSR на подпись.

1.22.8. **Проверка ресурсных записей**

ТЦИ проверяет ресурсные записи на соответствие стандартам.

1.22.9. **Время актуальности ресурсных записей на кэширующем сервере**

Время жизни записей типа DNSKEY, DS и соотносящихся с ними RRSIG установлено в 345600 секунд (4 дня).

Время жизни записей типа NSEC3 установлено в 3600 секунд (1 час), что соответствует времени отрицательного кэша для зоны.

Данные параметры могут быть изменены при необходимости.

1.23. **Аудит соответствия**

В соответствии с внутренней политикой безопасности проводится регулярный аудит, результатом которого является устранение замечаний и недостатков работы системы и введение улучшений.

1.24. **Правовые вопросы**

ТЦИ не несёт юридической ответственности за вопросы, описанные в данном документе.

В своей деятельности ТЦИ опирается на законодательство Российской Федерации и распорядительные документы АНО «Координационный центр национального домена сети Интернет».

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Версия	Дата	Номер раздела, рисунка или таблицы	Тип изменений[1]	Автор	Примечание

[1] Д – добавлено, И – изменено, У - удалено