|  |
| --- |
| УТВЕРЖДЕНО  Протокол заседания Правления ОАО «Белорусская универсальная товарная биржа»  от 31.10.2019 № 219 |

**Политика применения атрибутных сертификатов**

Удостоверяющего центра

ОАО «Белорусская универсальная товарная биржа»

г. Минск

СОДЕРЖАНИЕ

[ССЫЛКИ НА НОРМАТИВНЫЕ ДОКУМЕНТЫ 3](#_Toc23265954)

[ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 4](#_Toc23265955)

[ВВЕДЕНИЕ 7](#_Toc23265956)

[1. ТРЕБОВАНИЯ К УЧАСТНИКАМ ИНФРАСТРУКТУРЫ АС 8](#_Toc23265957)

[1.1 Требования к УЦ СЭА 8](#_Toc23265958)

[1.2 Пользователи ППАС 8](#_Toc23265959)

[2 ТРЕБОВАНИЯ К УЦ СЭА 9](#_Toc23265960)

[2.1 Требования по управлению ключами ЦАС 9](#_Toc23265961)

[2.1.1 Выработка личного ключа ЦАС 9](#_Toc23265962)

[2.1.2 Хранение, резервное копирование и восстановление личного ключа ЦАС 9](#_Toc23265963)

[2.1.3 Распространение открытого ключа ЦАС 9](#_Toc23265964)

[2.1.4 Депонирование личного ключа УЦ СЭА 10](#_Toc23265965)

[2.1.5 Использование личного ключа ЦАС УЦ СЭА 10](#_Toc23265966)

[2.1.6 Окончание срока действия личного ключа ЦАС 10](#_Toc23265967)

[2.1.7 Управление средством ЭЦП, используемым для издания АС 10](#_Toc23265968)

[2.2 Требования по управлению АС 10](#_Toc23265969)

[2.2.1 Регистрация абонента 10](#_Toc23265970)

[2.2.2 Издание АС 10](#_Toc23265971)

[2.2.3 Распространение АС 11](#_Toc23265972)

[2.2.4 Отзыв и приостановка действия АС 11](#_Toc23265973)

[2.2.5 Возобновление действия АС и обновление данных 12](#_Toc23265974)

[2.2.6 Предоставление информации о статусе АС 12](#_Toc23265975)

# ССЫЛКИ НА НОРМАТИВНЫЕ ДОКУМЕНТЫ

1. Закон Республики Беларусь №455-З от 10.11.2008 «Об информации, информатизации и защите информации».
2. Закон Республики Беларусь №113-3 от 28.12.2009 «Об электронном документе и электронной цифровой подписи».
3. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь №62 от 30.08.2013 «О некоторых вопросах технической и криптографической защиты информации».
4. ГОСТ 21.101-93 Основные требования к рабочей документации.
5. СТБ ISO/IЕС 27001-2011 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
6. СТБ 34.101.1-2014 (ISO/IЕС 15408-1:2009) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. (ISO/IЕС I5408-1:2009, MOD).
7. СТБ 34.101.2-2014 (ISO/IЕС 15408-2:2008) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. (ISO/IЕС 15408-2:2008, MOD).
8. СТБ 34.101.3-2014 (ISO/IЕС 15408-3:2008) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности. (ISO/IЕС 15408-3:2008, MOD).
9. СТБ 34.101.17-2012 Информационные технологии. Синтаксис запроса на получение сертификата.
10. СТБ 34.101.19-2012 Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей.
11. СТБ 34.101.48-2012 Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров.

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

**НКИ** Носитель ключевой информации

**ППАС** Политика применения атрибутных сертификатов

**СИБ** Система информационной безопасности

**СОК** Сертификат открытого ключа

**СОС** Список отозванных сертификатов

**СОАС** Список отозванных атрибутных сертификатов

**ТНПА** Технические нормативные правовые акты

**УЦ Биржи** Удостоверяющий центрОАО «Белорусская универсальная товарная биржа»

**УЦ СЭА** Удостоверяющий центр по выпуску атрибутных сертификатов для участия в закупках, проводимых в электронном формате

**ЦАС** Центр атрибутных сертификатов

**ЭЦП** Электронная цифровая подпись

**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

**Абонент** - юридическое или физическое лицо, в том числе индивидуальный предприниматель, принимающее условие Публичного договора;

**Атрибутный сертификат (далее – АС)** - структура данных с электронной цифровой подписью центра атрибутных сертификатов, связывающая определенные значения атрибутов с идентификационной информацией о держателе;

**Генерация личного и открытого ключей** - процедура, реализующая алгоритм выработки личного ключа и соответствующего ему открытого ключа.

**Доверяющая сторона** - юридическое или физическое лицо, полагающееся на достоверность сведений, содержащихся в сертификате открытого ключа, и (или) электронную цифровую подпись, проверенную с использованием данного сертификата.

**Компрометация личного ключа** - утрата доверия к личному ключу.

**Носитель ключевой информации** - специальное отчуждаемое программно-аппаратное устройство хранения информации, подключаемое к USB-порту ПЭВМ и обеспечивающее хранение личных ключей в зашифрованном виде.

**Отзыв сертификата открытого ключа** - процедура, заключающаяся в досрочном прекращении действия сертификата открытого ключа.

**Политика применения сертификата** - установленный набор правил, характеризующих возможность применения сертификатов определенным сообществом субъектов и/или классом приложений с определенными требованиями безопасности.

**Приостановление действия сертификата** - процедура изменения состояния сертификата открытого ключа с целью исключения использования его на время приостановления.

**Регламент УЦ СЭА** - документ «Регламент работы ОАО «Белорусская универсальная товарная биржа» по распространению сертификатов открытых ключей проверки электронной цифровой подписи и выпуску атрибутных сертификатов для участия в закупках, проводимых в электронном формате.

**Сертификат открытого ключа** - электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенным организации или физическому лицу, и иную информацию, предусмотренную Законом Республики Беларусь №113-3 от 28.12.2009 «Об электронном документе и электронной цифровой подписи» и иными актами законодательства Республики Беларусь.

**Система информационной безопасности (СИБ)** - комплекс организационных и технических мер, направленных на обеспечение безопасности информационных активов, включая разработку и внедрение соответствующих политик и процедур, создание технологической инфраструктуры, внедрение программных и технических средств защиты.

**Список отозванных сертификатов** - электронный документ, созданный УЦ Биржи и содержащий информацию о сертификатах открытого ключа, действие которых прекращено или приостановлено до истечения срока действия открытых ключей, указанных в сертификатах открытого ключа.

**Список отозванных атрибутных сертификатов (далее - СОАС)** - список отозванных атрибутных сертификатов, которые были выпущены в центре атрибутных сертификатов.

**Срок действия сертификата** - промежуток времени, в течение которого Предприятие гарантирует подлинность СОК и актуальность его состояния.

**Субъект** - владелец личного ключа, связанного с открытым ключом, указанным в сертификате.

**Удостоверяющий центр (УЦ)** - поставщик услуг издания, распространения, хранения сертификатов открытых ключей и списков отозванных сертификатов открытых ключей.

**Уполномоченный представитель** - физическое лицо, наделенное полномочиями на представление интересов юридического или физического лица, в том числе индивидуального предпринимателя, во взаимоотношениях с УЦ Биржи.

**Центр атрибутных сертификатов (далее - ЦАС)** - центр (сервис), удостоверяющий полномочия или свойство стороны путем выпуска атрибутных сертификатов.

# ВВЕДЕНИЕ

Политика применения атрибутных сертификатов (далее - ППАС) является документом, содержащим описание услуг, которые оказывает удостоверяющий центр ОАО «Белорусская универсальная товарная биржа» (далее - УЦ Биржи) по изданию, распространению, хранению атрибутных сертификатов (далее - АС), а также по управлению отзывом АС и предоставлению информации о статусе АС.

Настоящий документ разработан в соответствии с законодательством Республики Беларусь, регулирующим деятельность в области защиты информации, информатизации и электронного документооборота (Законом Республики Беларусь «Об информации, информатизации и защите информации» от 10.11.2008 №455-3), в том числе с учетом требований СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения СОК удостоверяющих центров» и СТБ ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов».

УЦ Биржи должен ознакомить абонентов с настоящей ППАС путем размещения на сайте Биржи.

УЦ Биржи должен уведомлять абонентов и иных заинтересованных лиц о внесении изменений и дополнений в настоящую ППАС.

Требования ППАС должны реализоваться в соответствии с Регламентом УЦ СЭА.

# ТРЕБОВАНИЯ К УЧАСТНИКАМ ИНФРАСТРУКТУРЫ АС

## 1.1. Требования к УЦ СЭА

УЦ СЭА должен выполнять все требования, установленные в данной ППАС.

УЦ СЭА несет ответственность в соответствии с законодательством за соответствие процедурам, установленным ППАС.

Данная ППАС не противоречит Регламенту УЦ СЭА.

## 1.2. Пользователи ППАС

На основании СОК Субъекта в УЦ может издаваться АС, в котором определяются права владельца СОК в информационных системах.

АС изданные в УЦ устанавливают права (привилегии) владельцев СОК в информационных системах, владельцы которых заключили соответствующее соглашение с УЦ Биржи.

АС являются элементом инфраструктуры управления правами (приви­легиями) владельцев СОК. АС применяется в информационных системах совместно с СОК Субъекта, при этом СОК используется для идентификации и аутентификации, а АС для определения его прав.

Сервисы по изданию и управлению АС в УЦ предоставляются ЦАС, являющейся частью инфраструктуры открытых ключей УЦ.

**1.3. Типы АС**

ЦАС издает АС для Субъектов способом, обеспечивающим сохранение их подлинности и целостности.

АС издается только к существующему СОК Субъекта.

Формат АС, издаваемых УЦ соответствуют требованиям СТБ 34.101.67-­2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов».

УЦ Биржи гарантирует уникальность идентификационного номера АС Субъекта.

УЦ Биржи обеспечивает конфиденциальность и целостность регистрационных данных предоставляемых уполномоченным представителем.

УЦ Биржи оказывает услуги по изданию и управлению АС, устанавливающих (подтверждающих) связь ФЛ с юридическим лицом (далее - ЮЛ) с указанием идентификационных данных ЮЛ и должностью ФЛ (далее - АС ЮЛ). Образцы атрибутных сертификатов приведены в Приложении 1 к настоящей ППАС.

# 2. ТРЕБОВАНИЯ К УЦ СЭА

## 2.1. Требования по управлению ключами ЦАС

### 2.1.1. Выработка личного ключа ЦАС

Выработка личного ключа ЦАС должна осуществляться под контролем как минимум двух сотрудников УЦ Биржи в конструктивно защищенной среде.

Выработка личного ключа и открытого ключа ЦАС должна осуществляться с использованием сертифицированного программно-аппаратного средства.

ЦАС является частью инфраструктуры открытых ключей УЦ.

Срок действия СОК ЦАС - 10 лет.

УЦ Биржи за один год до истечения срока действия СОК ЦАС вырабатывает новую пару ключей и принимает все необходимые меры для того, чтобы избежать нарушения деятельности любого участника, использующего АС.

Новые ключи УЦ СЭА также должны создаваться и распространяться в соответствии с настоящей ППС.

### 2.1.2 . Хранение, резервное копирование и восстановление личного ключа ЦАС

Личный ключ ЦАС должен храниться в защищенном виде на носителях ключевой информации (далее - НКИ).

УЦ СЭА должен осуществлять резервное копирование своих личных ключей.

Резервные копии личных ключей должны храниться в защищенном виде на НКИ.

Личные ключи УЦ СЭА должны копироваться и восстанавливаться в присутствии минимум двух сотрудников УЦ Биржи.

Средства контроля доступа к НКИ, на которых хранятся резервные копии личных ключей УЦ, должны гарантировать отсутствие несанкционированного доступа к ним.

### 2.1.3. Распространение открытого ключа ЦАС

УЦ СЭА должен распространять свой открытый ключ ЦАС в виде СОК.

Доверяющая сторона должна провести проверку подлинности и целостности открытого ключа ЦАС УЦ СЭА при его получении.

### 2.1.4. Депонирование личного ключа УЦ СЭА

УЦ СЭА не должен осуществлять депонирование своих личных ключей.

### 2.1.5. Использование личного ключа ЦАС УЦ СЭА

УЦ СЭА использует свой личный ключ ЦАС только для целей издания АС, СОАС ЦАС и предоставления информации о статусе АС.

### 2.1.6. Окончание срока действия личного ключа ЦАС

Личные ключи ЦАС УЦ СЭА, по окончании срока их действия, должны не использоваться и уничтожаться без возможности восстановления.

### 2.1.7. Управление средством ЭЦП, используемым для издания АС

УЦ СЭА должен обеспечивать безопасность средства ЭЦП в течение всего срока его применения для издания АС.

УЦ СЭА должен гарантировать, что:

- средство ЭЦП, используемое для издания АС и СОАС, не было повреждено во время поставки;

- средство ЭЦП, используемое для издания АС и СОАС, не было скомпрометировано во время хранения;

- установка, активация, резервное копирование и восстановление ключей ЦАС УЦ СЭА в средстве ЭЦП проводятся под контролем не менее двух доверенных сотрудников УЦ Биржи;

- средство ЭЦП, используемое для издания АС или СОАС, функционирует правильно;

- личный ключ ЦАС, хранимый в программно-аппаратном средстве ЭЦП, уничтожается при изъятии данного средства из обращения.

## 2.2. Требования по управлению АС

### 2.2.1. Регистрация абонента

Услуги по регистрации абонентов с выпуском АС осуществляются в соответствии с Регламентом УЦ СЭА (в зависимости от услуги).

### 2.2.2. Издание АС

АС, издаваемые УЦ СЭА, должен соответствовать профилю формата атрибутного сертификата (Приложение 1).

После издания АС Субъекту предоставляются путем размещения на сайте УЦ Биржи или иным доступным способом (в том числе через Личный кабинет (Персональный раздел) Абонента):

АС, изданный ЦАС;

СОАС, изданный ЦАС;

СОК ЦАС;

СОК и список отозванных сертификатов (далее - СОС) КУЦ.

### 2.2.3. Распространение АС

УЦ СЭА должен вести реестр изданных АС в электронном виде или на бумажном носителе в течение установленного срока хранения.

УЦ СЭА может выполнять отзыв действующего АС и выпуск нового АС в соответствии с п. 2.2.4 и п. 2.2.2.

Информация о назначении АС должна быть доступна доверяющим сторонам.

Данная информация должна быть доступна 24 часа в сутки 365 дней в году. В случае отказа системы, сервисов или при наличии других факторов, не зависящих от УЦ СЭА, УЦ СЭА должен принять все необходимые меры, чтобы гарантировать, что данная информационная услуга будет недоступна только в течение максимально короткого интервала времени.

### 2.2.4. Отзыв и приостановка действия АС

УЦ СЭА должен отзывать АС на основании заявления и в сроки, установленные в Регламенте УЦ СЭА.

Заявления, связанные с отзывом СОК, должны обрабатываться УЦ СЭА по мере их поступления.

Заявления, связанные с отзывом, должны идентифицироваться и проверяться УЦ СЭА на предмет их получения из достоверных источников.

Абонент отозванного или приостановленного АС должен информироваться УЦ СЭА об изменении статуса его СОК.

Если АС отозван, он не должен использоваться в дальнейшем никогда.

Информация о статусе АС должна распространяться УЦ СЭА посредством издания СОАС, который должен быть издан и опубликован в течение 30 минут с момента отзыва АС.

Услуги УЦ СЭА по управлению отзывом и получению статуса АС должны быть доступны 24 часа в сутки 365 дней в году. В случае отказа системы, сервисов или при наличии других факторов, не зависящих от УЦ СЭА, УЦ СЭА должен гарантировать, что данная информационная услуга будет недоступна только в течение максимально короткого интервала времени.

### 2.2.5. Возобновление действия АС и обновление данных

Возобновление действия АС должно осуществляться УЦ СЭА на основании заявления абонента.

Возобновление действия АС должно осуществляться без изменения любой регистрационной информации, содержащейся в данном АС.

Перед тем как восстановить АС УЦ СЭА должен удостовериться, что информация, использованная для подтверждения личности и полномочий абонента, на момент обращения является действительной.

### 2.2.6. Предоставление информации о статусе АС

ЦАС распространяет информацию о статусе АС посредством издания, соответствующего СОАС.

Периодичность издания СОАС - ежемесячно. СОАС издается с соблюдением следующих правил:

каждый СОАС содержит информацию о времени издания следующего СОАС;

СОАС подписан личным ключом ЦАС.

Новый СОАС может быть издан перед установленным временем издания следующего СОАС. Например, внеочередной СОАС издается ЦАС сразу же после обработки запроса на управление статусом АС (отзыв, приостановление действия, возобновление действия).