У т в е р ж д е н а
решением Совета директоров АО ДБ "Альфа-Банк"
(протокол заседания
от 3 июля 2021 года № 19)
Введена в действие
с 7 июля 2021 года

П О Л И Т И К А
применения регистрационных свидетельств удостоверяющего центра АО ДБ «Альфа-Банк» (редакция 1.0.0)

г. Алматы

2021г.

С О Д Е Р Ж А Н И Е:

Глава 1. ВВЕДЕНИЕ

Параграф 1.1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика применения регистрационных свидетельств удостоверяющего центра АО ДБ «Альфа-Банк» (далее – Политика сертификатов) разработана в соответствии с требованиями нормативных правовых актов Республики Казахстан по вопросам электронного документа и электронной цифровой подписи в целях обеспечения функционирования удостоверяющего центра АО ДБ «Альфа-Банк» (далее – Удостоверяющий центр/Банк).
2. Политика сертификатов разработана с учетом международных отраслевых рекомендаций RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” (Структура документов политики и практики сертификатов в интернет инфраструктуре открытых ключей формата X.509).
3. Политика сертификатов определяет виды сертификатов, выпускаемых Удостоверяющим центром, определяет основные принципы и общие требования их применимости в заинтересованных информационных системах Удостоверяющего центра, объединенных типовыми требованиями информационной безопасности Банка, что гарантирует определенный уровень доверия в информационных системах Банка, использующих эти сертификаты.
4. Политика сертификатов не определяет детальный порядок и процедуры функционирования Удостоверяющего центра, обеспечения безопасности инфраструктуры открытых ключей, которые согласно требованиям нормативных правовых актов Республики Казахстан и международных отраслевых рекомендаций RFC 3647 вынесены в отдельные правила деятельности Удостоверяющего центра.
5. С момента подписания участником информационной системы Банка, использующей сервисы Удостоверяющего центра, заявления на выпуск сертификата, для участника становятся обязательными к выполнению применимые к нему требования Политики сертификатов и тех правил деятельности удостоверяющего центра, ссылка на которые содержится в подписанном заявлении.
6. Исчерпывающий перечень видов сертификатов, выпускаемых Удостоверяющим центром, с указанием идентифицирующих их признаков (профилей) определяется параграфом 1.1 правил деятельности Удостоверяющего центра.

Параграф 1.2. НАИМЕНОВАНИЕ И АТРИБУТЫ ДОКУМЕНТА

7. Документ именуется “Политика применения регистрационных свидетельств удостоверяющего центра АО ДБ «Альфа-Банк»”, как этого требует правовой акт по вопросам аккредитации удостоверяющих центров, изданный уполномоченным органом в сфере обеспечения информационной безопасности[1].
8. Редакция документа 1.0.0.
9. Политика сертификатов в настоящей редакции введена в действие протокольным решением Совета директоров Банка от 3 июля 2021 года № 19.
10. Действующая редакция Политики сертификатов публикуется на официальном информационном ресурсе Банка в сети Интернет по адресу https://alfabank.kz/pki.
11. Политика сертификатов зарегистрирована в дереве международных объектных идентификаторов с присвоением объектного идентификатора.

[1] На дату утверждения Политики сертификатов действует приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 1 июня 2020 года № 224/НҚ “Об утверждении Правил проведения аккредитации удостоверяющих центров”.

Параграф 1.3. УЧАСТНИКИ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ БАНКА

12. Удостоверяющий центр – структурное подразделение Банка, удостоверяющее соответствие открытого криптографического ключа закрытому криптографическому ключу, а также подтверждающее достоверность регистрационного свидетельства[2].
13. Центры регистрации Удостоверяющего центра – отделения и/или уполномоченные выделенные работники Банка, ответственные за прием документов на выпуск или отзыв сертификатов, идентификацию заявителей и предоставление заявителям доступа к готовым сертификатам.
14. Подписчики Удостоверяющего центра – субъекты (физические лица или юридические лица, действующие в лице своих уполномоченных представителей), для которых Удостоверяющий центр выпустил сертификат.
15. Доверяющие стороны (или пользователи сертификатов) – подписчики Удостоверяющего центра или любые другие субъекты, действующие, полагаясь на сертификаты, выпущенные Удостоверяющим центром, и/или электронные документы с электронными цифровыми подписями, подлинность которых проверяется с помощью этих сертификатов.

Параграф 1.4. НАЗНАЧЕНИЕ СЕРТИФИКАТОВ

16. Удостоверяющий центр выпускает сертификаты для обеспечения потребностей информационных систем, принадлежащих Банку, и не выпускает – для информационных систем, принадлежащих другим лицам.
17. Удостоверяющий центр выпускает сертификаты различного назначения.
18. Назначение сертификата определяется целью использования пары криптографических ключей, открытый ключ которой удостоверен сертификатом.
19. Закрепленная цель использования пары криптографических ключей фиксируется в каждом сертификате, выпускаемом Удостоверяющим центром для участника, в расширении “keyUsage”.
20. Кроме этого, область допустимого применения выпускаемых Удостоверяющим центром сертификатов может дополнительно подразделяться с помощью объектных идентификаторов политики, которые фиксируются в расширении сертификата “cerificatePolicies”.
21. Наличие объектных идентификаторов политики дает информационным системам, использующим сертификаты, возможность дополнительной защиты в форме контроля системой наборов необходимых и запрещенных политик с ограничением применения неподходящих сертификатов.
22. Не допускается использование сертификатов, выпущенных Удостоверяющим центром, способами, противоречащими законодательству Республики Казахстан, Политике сертификатов, правилам деятельности Удостоверяющего центра и внутренним документам Банка.
23. Сертификаты подписчиков Удостоверяющего центра используются для работы с программным обеспечением доверяющих сторон и не используются как технологические сертификаты информационной системы Удостоверяющего центра. В свою очередь технологические сертификаты информационной системы Удостоверяющего центра не используются ни для каких иных целей кроме их прямого функционального назначения.

[2] На дату утверждения Политики сертификатов указанную задачу решает управление удостоверяющего центра Департамента информационной безопасности Блока председателя Правления Банка.

Параграф 1.5. УПРАВЛЕНИЕ ДОКУМЕНТОМ

24. Политика сертификатов актуализируется Удостоверяющим центром, расположенным по адресу: A15G5M8, г. Алматы, ул. Айманова, д. 140, блок Б2.
25. Контактное лицо по вопросам актуализации документа – главный аналитик Удостоверяющего центра, A15G5M8, г. Алматы, ул. Айманова, д. 140, блок Б2, +7 (727) 259-05-01 (вн. 4758), amakhnin@alfabank.kz.
26. Изменения и дополнения в Политику сертификатов готовятся Удостоверяющим центром либо в форме новой редакции, либо в форме перечня изменений и дополнений к текущей редакции Политики сертификатов.
27. Перед утверждением изменения и дополнения в Политику сертификатов проходят согласование с заинтересованными подразделениями и должностными лицами Банка согласно внутренним процедурам[3].
28. Изменения и дополнения в Политику сертификатов утверждаются протокольным решением Совета директоров Банка.
29. Все изменения и дополнения в Политику сертификатов публикуются на официальном информационном ресурсе Банка в сети Интернет.
30. Публикация новой редакции Политики сертификатов является официальным уведомлением всех подписчиков и доверяющих сторон Удостоверяющего центра о ее вступлении в силу.
31. С даты публикации новой редакции Политики сертификатов, если иное не предусмотрено входящими в нее переходными положениями, новая редакция становится обязательной для применения всеми юридическими и физическими лицами, связанными с Банком обязательствами по договорам, ссылающимся на Политику сертификатов, вне зависимости от даты заключения договора.

Параграф 1.6. ТЕРМИНЫ ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

32. В дополнение к терминам, определениям и сокращениям законодательства Республики Казахстан по вопросам электронного документа и электронной цифровой подписи (ЭЦП), в Политике сертификатов используются следующие понятия:
    1) аутентификация – процесс или сервис безопасности, реализующий этот процесс, который предназначен для проверки того, что лицо (предмет) является тем, кем себя именует (чем он поименован);
    2) Банк – АО ДБ «Альфа-Банк»;
    3) данные активации – любые данные, за исключением криптографических ключей, которые необходимы для выполнения криптографических операций и требуют защиты: персональные идентификационные номера (PIN), парольные фразы, компоненты разделенного криптографического ключа и т.п;
    4) дерево международных объектных идентификаторов – стандартизированный ITU-T и ISO/IEC механизм (X.660) именования любых реальных или абстрактных объектов однотипными недвусмысленными всеобъемлющими именами, предназначенный для регистрации имен с помощью трех иерархических деревьев особой формы (от 3 разных корней), в которых каждый последующий узел наделен целочисленным номером и ответственен за дальнейшее выделение и регистрацию ветвей, исходящих от него самого;
    5) закрытый криптографический ключ – в криптосистемах с открытым ключом, тот ключ из ключевой пары, который известен только подписчику;

[3] На дату утверждения Политики сертификатов действует “Инструкция по взаимодействию подразделений при разработке, изменении и/или дополнении и прекращении действия внутренних нормативных документов”, утвержденная протокольным решением Правления Банка от 25 сентября 2019 года № 65.

6) идентификация – в контексте Политики сертификатов, процесс (или результат такого процесса), который предназначен для проверки идентичности физического или юридического лица, показывает, что данное лицо является конкретным, вполне определенным лицом, и состоит из двух этапов:

   установление соответствия предъявленного лицом имени реально существующей идентичности лица и

   установление того, что лицо, обращающееся за доступом к чему-либо от определенного имени, на самом деле является тем лицом, которым себя именует (аутентификация);
7) инфраструктура открытых ключей – набор средств (технических, материальных, людских и т.д.), распределённых служб и компонентов, в совокупности используемых для решения криптографических задач (аутентификации, шифрования, контроля целостности и доказательности) на основе криптосистем с открытым ключом, способный самостоятельно обеспечить управление открытыми ключами, посредством которых решаются указанные задачи;
8) компрометация криптографических ключей – утрата владельцем криптографических ключей уверенности в том, что конкретные криптографические ключи обеспечивают безопасность защищаемой с их помощью информации;
9) носитель ключевой информации – электронное устройство (специализированный аппаратный токен, карта памяти, жесткий диск и т.п.), способное хранить криптографические ключи в электронной форме;
10) объектный идентификатор – идентификатор, который однозначно именует узел дерева международных объектных идентификаторов в форме списка целочисленных значений, упорядоченного от корня дерева к данному узлу;
11) открытый криптографический ключ – в криптосистемах с открытым ключом, тот ключ из ключевой пары, который известен публике;
12) политика применения регистрационных свидетельств (также именуется Политикой сертификатов) – озаглавленный набор правил, которые определяют применимость сертификата в определенной общности (классе) приложений с общими требованиями информационной безопасности;
13) правила деятельности удостоверяющего центра – нормативный документ, определяющий порядок организации основной деятельности, включая течение основных бизнес-процессов удостоверяющего центра, которые осуществляются в соответствии с Политикой сертификатов;
14) сертификат – открытый криптографический ключ подписчика вместе с дополнительной информацией, подлинность и взаимосвязь которых удостоверена электронной цифровой подписью, сформированной закрытым криптографическим ключом Удостоверяющего центра[4];
15) список отозванных сертификатов (СОС) – список, отображающий набор сертификатов, которые Удостоверяющий центр объявил недействительными до истечения срока их действия;
16) токен – в контексте Политики сертификатов, физическое устройство, выдаваемое авторизованному пользователю вычислительных ресурсов в целях упрощения процедур его аутентификации;
17) участники инфраструктуры открытых ключей – физические лица или юридические лица, действующие в лице своих уполномоченных представителей,

[4] Одной из разновидностей сертификатов являются регистрационные свидетельства, выпускаемые Удостоверяющим центром в соответствии с Законом Республики Казахстан “Об электронном документе и электронной цифровой подписи”.

которые выполняют роли подписчиков, доверяющих сторон, центров регистрации или удостоверяющего центра в одной и той же инфраструктуре открытых ключей;

18) цепочка сертификатов – упорядоченная последовательность сертификатов, начинающаяся с сертификата, ЭЦП в котором может быть проверена с помощью доверенного корневого сертификата, успешная обработка которой с помощью стандартизированного алгоритма позволяет подтвердить принадлежность открытого ключа лицу, указанному в заключительном сертификате последовательности, в поле “subject”.

Глава 2. ОТВЕТСТВЕННОСТЬ ЗА ХРАНИЛИЩЕ И ПУБЛИКАЦИЮ ДАННЫХ В НЕМ

Параграф 2.1. ХРАНИЛИЩЕ

33. Деятельность Удостоверяющего центра требует непрерывного размещения в оперативном доступе актуальных данных реестра сертификатов, выпущенных Удостоверяющим центром, и информации об их статусе.
34. В связи с этим, составной частью информационной системы Удостоверяющего центра является хранилище, которое в качестве справочника необходимой информации обслуживаемые информационные системы Банка используют напрямую, а подписчики и доверяющие стороны – опосредованно, через используемые информационные системы Банка.
35. Кроме этого, Удостоверяющий центр ведет раздел на официальном информационном ресурсе Банка в сети Интернет, в котором также публикует свои корневые сертификаты и списки отозванных сертификатов, а также необходимый минимум нормативных документов и других данных о своих сервисах (включая Политику сертификатов и правила деятельности Удостоверяющего центра).

Параграф 2.2. ПУБЛИКАЦИЯ В ХРАНИЛИЩЕ ИНФОРМАЦИИ О СЕРТИФИКАТАХ

36. Основным протоколом информационного взаимодействия с хранилищем Удостоверяющего центра является облегченный протокол доступа к службам каталогов в версии, определенной рекомендациями RFC 2251 (Lightweight Directory Access Protocol v.3, версия 3).
37. По данному протоколу подписчики и доверяющие стороны через информационные системы Банка, обслуживаемые Удостоверяющим центром, обращаются в режиме онлайн с запросами о наличии валидных сертификатов, их содержании и статусе.
38. Любые исключения из этих требований, в случае их возникновения, должны быть включены в Правила деятельности Удостоверяющего центра и опубликованы в свободном доступе подписчиков и доверяющих сторон.

Параграф 2.3. ПЕРИОДИЧНОСТЬ АКТУАЛИЗАЦИИ ДАННЫХ В ХРАНИЛИЩЕ

39. Удостоверяющий центр публикует каждый вновь выпущенный сертификат в хранилище.
40. В случае отзыва сертификата Удостоверяющий центр не удаляет его из хранилища немедленно. Сертификат удаляется из хранилища по мере истечения срока действия, указанного в соответствующем поле сертификата.
41. В случае отзыва любого сертификата Удостоверяющий центр формирует и публикует в хранилище обновленный список отозванных сертификатов.

42. Отозванные сертификаты удаляются из списков отозванных сертификатов по факту истечения срока действия сертификата.
43. В условиях отсутствия событий отзыва или истечения срока действия отозванных сертификатов новые списки отозванных сертификатов формируются и выпускаются на регулярной основе.

Параграф 2.4. КОНТРОЛЬ ДОСТУПА К ХРАНИЛИЩУ

44. Доступ для чтения данных из хранилища Удостоверяющего центра разрешается любому пользователю, опосредованно, через обслуживаемые информационные системы Банка, без ограничений постоянного характера.
45. Доступ для добавления данных в хранилище, изменения данных в хранилище или исключения (удаления) данных из хранилища запрещен Удостоверяющим центром для неуполномоченных на то лиц.
46. В случаях кибератак, иных угроз перебоя в предоставлении сервисов или обоснованных подозрений в них Удостоверяющий центр оставляет за собой право применять вре́менные ограничения доступа для чтения данных из хранилища в качестве активных мер противодействия.
47. Ограничения и контроли доступа в хранилище применяются в соответствии с Политикой информационной безопасности Банка[5].

Глава 3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Параграф 3.1. ТРЕБОВАНИЯ К ИМЕНАМ

48. Удостоверяющий центр использует правила именования субъектов, призванные обеспечить однозначную идентификацию подписчиков во всех выпускаемых сертификатах.
49. Однозначность идентификации достигается за счет максимально возможного использования идентификационных номеров из единого республиканского реестра (ИИН и БИН).
50. В случае отсутствия у физического лица ИИН, вместо него используются номер и другие реквизиты паспорта, при отсутствии паспорта – документа, заменяющего паспорт.
51. В случае отсутствия у юридического лица БИН, вместо него используется номер и реквизиты документа о регистрации плательщика НДС (VAT).
52. Для наглядности в состав имен помимо идентификационных номеров допускается включение фамилии, имени, отчества, торговой марки, названия информационной системы, аббревиатуры организационно-правовой формы, названия организации и других общепринятых и понятных для человеческого восприятия имен и названий.
53. Анонимность подписчиков не допускается.
54. Использование подписчиками псевдонимов вместо общеизвестных имен не допускается.
55. Заявители на выпуск сертификатов не должны использовать в своих заявлениях имена, нарушающие права их законных правообладателей. Удостоверяющий центр не несет ответственности за проверку на предмет правообладания заявителя именем, указанным в заявлении, и не вступает в споры и разбирательства, связанные с собственностью на доменные, торговые и тому подобные имена и марки.

[5] Текст Политики информационной безопасности постоянно доступен на официальном ресурсе Банка в сети Интернет по адресу https://alfabank.kz/uploads/up_docs/about_docs/10/ru/gNP54exu53BtRVTkYZ4KnajfYg3EMqSg.pdf.

56. Удостоверяющий центр оставляет за собой право отклонить любое заявление на выпуск сертификата или приостановить его рассмотрение, если ему становится известно о факте подобного спора или разбирательства.
57. Содержание поля “Issuer” всех сертификатов, выпускаемых Удостоверяющим центром, определяется в соответствии с параграфом 3.1 правил деятельности Удостоверяющего центра.
58. В корневых сертификатах Удостоверяющего центра в поле “Subject” содержатся в точности те же данные, что и в поле “Issuer”.
59. Структура содержания поля “Subject” сертификатов всех подписчиков Удостоверяющего центра определяется в соответствии с параграфом 3.1 правил деятельности Удостоверяющего центра.
60. Вследствие правового требования однозначной идентификации, имена всех подписчиков являются уникальными. Вместе с тем, выпуск и использование двух и более сертификатов с одним и тем же именем в поле “Subject” разрешается при условии, что соответствующими закрытыми криптографическими ключами владеет и пользуется одно и то же физическое лицо.

Параграф 3.2. ПЕРВОНАЧАЛЬНАЯ ПРОВЕРКА ИДЕНТИЧНОСТИ

61. Первоначальная проверка идентичности – это наиболее полная форма процедур идентификации и аутентификации, которая согласно международным отраслевым рекомендациям проводится в отношении подписчика при выпуске первого сертификата.
62. Вместе с тем, любую другую процедуру, требующую идентификации подписчика (выпуск или отзыв любого сертификата), Удостоверяющий центр проводит по полной форме первоначальной проверки идентичности.

Глава 4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТОВ

Параграф 4.1. ЗАЯВЛЕНИЯ НА ВЫПУСК СЕРТИФИКАТОВ

63. Заявления на выпуск сертификата подают:
    1) уполномоченные представители юридических лиц;
    2) физические лица, действующие самостоятельно.
64. Заявления на выпуск сертификата подаются в центр регистрации.
65. Заявление на выпуск сертификата содержит ссылку на Политику сертификатов и Правила деятельности Удостоверяющего центра.
66. Заявление на выпуск сертификата является письменным (электронным) документом, означающим принятие подписчиком обязательств подписчика и доверяющей стороны соблюдать принципы и выполнять требования Политики сертификатов и Правил деятельности Удостоверяющего центра.
67. Необходимые Удостоверяющему центру обязательства подписчика и доверяющей стороны изложены в параграфе 9.6 (заявления и гарантии подписчика и доверяющей стороны).

Параграф 4.2. ОБРАБОТКА ЗАЯВЛЕНИЙ НА ВЫПУСК СЕРТИФИКАТОВ

68. Заявление на выпуск сертификата регистрируется только в случае наличия заключенного договора о предоставлении банковских услуг между заявителем и Банком.
69. Зарегистрированное заявление отклоняется центром регистрации, если:

1) заявитель указал в нем не всю информацию, необходимую в соответствии с правилами деятельности Удостоверяющего центра;
2) заявитель не обладает и не имеет возможности использовать средство электронной цифровой подписи, совместимое с сервисами Удостоверяющего центра;
3) в иных случаях, установленных законами Республики Казахстан.

70. После регистрации заявления проводится идентификация и аутентификация заявителя.
71. Срок рассмотрения и обработки заявлений на выпуск сертификатов определяется параграфом 4.2 правил деятельности Удостоверяющего центра.
72. Если заявитель в установленный срок не прошел успешно процедуру идентификации и аутентификации, т.е. не предоставил документальных доказательств достоверности информации, указанной в заявлении на выпуск сертификата, такое заявление на выпуск сертификата отклоняется.

Параграф 4.3. ВЫПУСК СЕРТИФИКАТОВ

73. Каждый сертификат создается Удостоверяющим центром по факту регистрации отдельного заявления на выпуск сертификата в центре регистрации.
74. Заявление на выпуск сертификата удовлетворяется центром регистрации только после успешного прохождения заявителем процедуры идентификации и аутентификации в соответствии с параграфом 4.2.
75. Выпуск любого сертификата подписчику Удостоверяющего центра состоит из следующих этапов:
    1) идентификация личности подписчика, а также, если требуется, проверка его полномочий представлять юридическое лицо, в соответствии с параграфом 4.2;
    2) защищенная генерация ключевой пары подписчика в центре регистрации;
    3) защищенная доставка открытого криптографического ключа подписчика из центра регистрации в Удостоверяющий центр;
    4) проверка Удостоверяющим центром факта владения подписчиком закрытым криптографическим ключом, соответствующим открытому криптографическому ключу, который подлежит регистрации Удостоверяющим центром.
76. При выпуске сертификата Удостоверяющий центр основывается на информации из заявления, которую успешно проверил центр регистрации в ходе процедур идентификации и аутентификации.
77. Любой сертификат, выпущенный Удостоверяющим центром, автоматически публикуется в хранилище для чтения всеми заинтересованными доверяющими сторонами.
78. О факте создания сертификата и способах его получения заявитель уведомляется через центр регистрации, принявший заявление на выпуск сертификата. Центр регистрации одновременно предоставляет заявителю сведения, необходимые для доступа подписчика к выпущенному сертификату.
79. Способами получения сертификата заявителем являются получение на руки в центре регистрации или загрузка через ту информационную систему Банка, для работы с которой заявитель запросил выпуск этого сертификата.

Параграф 4.4. ПРИНЯТИЕ СЕРТИФИКАТОВ

80. После получения сертификата всем подписчикам предоставляется право в течение 14 календарных дней с даты выпуска сертификата заявить Удостоверяющему центру об отказе от намерения иметь этот сертификат или о несогласии с его содержанием, при

условии, что соответствующий закрытый криптографический ключ с момента выпуска сертификата до заявления об отказе не использовался подписчиком.

81. Если подписчик не использует указанное право, то сертификат автоматически считается принятым подписчиком.
82. Если подписчик, не заявляя о своем отказе от намерения иметь сертификат или о несогласии с содержанием сертификата, до истечения предоставляемого Удостоверяющим центром 14-дневного срока начинает использовать соответствующий закрытый криптографический ключ, то сертификат автоматически считается принятым подписчиком с момента первого использования закрытого ключа.

Параграф 4.5. ИСПОЛЬЗОВАНИЕ КЛЮЧЕВЫХ ПАР И СЕРТИФИКАТОВ

83. Закрытый криптографический ключ используется подписчиком только после того, как подписчик дал письменное обязательство выполнять обязанности подписчика по договору с Банком, Удостоверяющий центр выпустил сертификат соответствующего открытого ключа, и подписчик принял этот сертификат.
84. Закрытый криптографический ключ используется подписчиком только в соответствии с законодательством, договорными обязательствами, Политикой сертификатов и Правилами деятельности Удостоверяющего центра.
85. Использование закрытого криптографического ключа должно соответствовать содержанию расширения “keyUsage” в соответствующем сертификате.
86. Подписчики защищают свои закрытые криптографические ключи от несанкционированного доступа и прекращают их использование после истечения срока действия или отзыва соответствующего сертификата.
87. Удостоверяющий центр не отвечает перед использующими сертификаты лицами, которые не обязались выполнять требования Политики сертификатов и Правил деятельности Удостоверяющего центра в части, касающейся обязанностей доверяющей стороны, в форме письменного обязательства, электронного документа либо согласия, зафиксированного в информационной системе Банка.
88. Прежде чем, предпринять любой акт, основываясь на доверии к сертификату, выпущенному Удостоверяющим центром, доверяющая сторона самостоятельно проверяет каждый соответствующий электронный документ, в частности, каждую имеющуюся в нем ЭЦП, а также связанные с ней сертификаты, метки времени, квитанции (ответы службы) OCSP или списки отозванных сертификатов.
89. Для проведения проверки ЭЦП доверяющая сторона:
    1) определяет и проверяет цепочку сертификатов, которая позволяет установить субъекта, сформировавшего ЭЦП. В ходе проверки цепочки сертификатов используется алгоритм, изложенный в рекомендациях RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (Профиль сертификата и списка отозванных сертификатов интернет инфраструктуры открытых ключей формата X.509);
    2) в ходе проверки каждого сертификата цепочки дополнительно контролирует содержание расширений “keyUsage” и “extendedKeyUsage” на соответствие цели использования;
    3) самостоятельно проверяет наличие у подписавшего лица полномочий, достаточных для подписания электронного документа. Информационная система Удостоверяющего центра сервисов контроля полномочий подписчика не предоставляет.
90. Если любой шаг проверки дает отрицательный результат или его невозможно выполнить, то ЭЦП полагается недействительной, и электронный документ отвергается.

91. Если в электронном документе имеется отметка времени, сформированная Удостоверяющим центром, то для выполнения действия, требующего доверия к отметке времени, необходимо также проверить эту отметку времени в порядке, аналогичном проверке ЭЦП в электронном документе.
92. Если любой из сертификатов цепочки на момент проверки ЭЦП имеет статус “отозван”, только доверяющая сторона исключительно на свой риск решает, оправдано или нет полагаться на электронный документ, сформированный подписчиком до отзыва одного из сертификатов цепочки. Удостоверяющий центр в случаях такого рода не несет ответственности перед доверяющими сторонами, так как подача заявления на отзыв сертификата является обязанностью конкретного подписчика.
93. Если обстоятельства указывают на необходимости дополнительных гарантий со стороны авторов электронного документа, то доверяющая сторона получает такие дополнительные гарантии от подписчиков самостоятельно, до выполнения действий, требующих доверия к сертификату, и без обращения в Удостоверяющий центр.

Параграф 4.6. ОБНОВЛЕНИЕ СРОКОВ ДЕЙСТВИЯ В СЕРТИФИКАТАХ

94. Услуг по обновлению сроков действия в сертификатах Удостоверяющий центр не предоставляет.
95. При необходимости дальнейшего использования сервисов информационной системы Банка, требующих наличия криптографических ключей, подписчик обращается в центр регистрации и оформляет заявление на выпуск (новых) сертификатов, в порядке, определенном параграфами 4.1, 4.2 и 4.3

Параграф 4.7. СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ В СЕРТИФИКАТАХ

96. Услуг по смене ключей в сертификатах Удостоверяющий центр не предоставляет.
97. Для смены криптографических ключей подписчик обращается в центр регистрации и оформляет заявление на выпуск (новых) сертификатов, в порядке, определенном параграфами 4.1, 4.2 и 4.3.

Параграф 4.8. ИЗМЕНЕНИЕ ДАННЫХ В СЕРТИФИКАТАХ

98. Услуг по изменению данных в сертификатах Удостоверяющий центр не предоставляет.
99. Для изменения данных в сертификате подписчик обращается в центр регистрации и оформляет заявление на выпуск (новых) сертификатов, в порядке, определенном параграфами 4.1, 4.2 и 4.3.

Параграф 4.9. ОТЗЫВ СЕРТИФИКАТОВ

100. Сертификаты, выпущенные Удостоверяющим центром, отзываются Удостоверяющим центром.
101. Основанием для отзыва сертификата является письменное заявление, оформленное подписчиком или центром регистрации и содержащее причину отзыва.
102. Возможные причины отзыва определяются законодательством Республики Казахстан и перечислены в разделе 4.9 Правил деятельности Удостоверяющего центра. В случае изменения применяются требования законодательства. Правила деятельности Удостоверяющего центра подлежат приведению в соответствие с законодательством в установленном порядке.
103. Заявления на отзыв сертификата подаются незамедлительно с момента обнаружения вышеуказанных оснований.

104. Перед отзывом сертификата центр регистрации и/или Удостоверяющий центр проверяет полномочия инициатора запрашивать отзыв, включая идентификацию заявителя. При этом применяется механизм идентификации, указанный в параграфе 3.2.
105. Доверяющие стороны обязуются проверять статус всех сертификатов, на которые они полагаются в своих действиях.
106. Если доверяющая сторона не использует для проверки статуса сертификатов онлайн обращение к службе протокола OCSP, то она должна использовать для этого актуальный список отозванных сертификатов, опубликованный в хранилище Удостоверяющего центра.
107. Списки отозванных сертификатов являются едиными в том смысле, что они содержат отзываемые сертификаты всех участников инфраструктуры открытых ключей: Удостоверяющего центра, центров регистрации и подписчиков.
108. Список отозванных сертификатов и служба протокола OCSP Удостоверяющего центра доступны в сети Интернет круглосуточно и непрерывно, за исключением времени плановых профилактических работ в соответствии с условиями Соглашения об уровне обслуживания Удостоверяющего центра.
109. Исключение истекших сертификатов из списка отозванных сертификатов осуществляется ежесуточно по расписанию, определенному соответствующей настройкой информационной системы Удостоверяющего центра.
110. Новый список отозванных сертификатов формируется и публикуется либо по факту исключения из списка истекшего сертификата, либо по факту отзыва сертификата любого участника инфраструктуры открытых ключей, либо спустя неделю по расписанию, определенному соответствующей настройкой информационной системы Удостоверяющего центра, если в течение недели ни одно из вышеуказанных событий не произошло.
111. Вновь созданный список отозванных сертификатов автоматически публикуется в хранилище Удостоверяющего центра незамедлительно по факту формирования, в режиме онлайн.
112. Юридические лица в случае увольнения работника, имеющего доступ к закрытым криптографическим ключам, или его перевода на другой участок работы, оформляют заявление на отзыв сертификатов, соответствующих закрытым ключам перемещаемого работника, не позднее даты перемещения. При необходимости подаются заявления на выпуск сертификатов для другого ответственного лица.
113. Услуг по временному приостановлению или возобновлению действия сертификатов Удостоверяющий центр не предоставляет.
114. Подписчик удостоверяющего центра имеет возможность прекратить обслуживание в Удостоверяющем центре:
    1) расторгнув действующий договор, предусматривающий обслуживание;
    2) отзывая все действующие сертификаты до окончания срока их действия.
115. В случае истечения срока действия всех сертификатов подписчика обслуживание подписчика в Удостоверяющем центре прекращается автоматически.
116. Услуг по депонированию закрытого ключа подписчика Удостоверяющий центр не предоставляет.
117. В случае компрометации закрытых криптографических ключей Удостоверяющего центра, Удостоверяющий центр оповещает об этом владельцев всех информационных систем Банка, использующих сервисы Удостоверяющего центра.

Глава 5. ФИЗИЧЕСКИЙ, ОПЕРАЦИОННЫЙ И УПРАВЛЯЮЩИЕ КОНТРОЛИ

Параграф 5.1. ФИЗИЧЕСКИЙ КОНТРОЛЬ

118. Деятельность Удостоверяющего центра и центров регистрации ведется на физически защищенных объектах, в условиях, где затруднены и фиксируются любые попытки несанкционированного доступа, использования или раскрытия конфиденциальной информации.
119. Детальные меры физического контроля Удостоверяющего центра определены и утверждены внутренними документами Банка и в Политике сертификатов не раскрываются. В настоящей главе приведен общий обзор этих мер.
120. Информационная система удостоверяющего центра обеспечена двумя дата-центрами (основной и резервный), расположенными на разных объектах в целях резервирования и восстановления функционирования в случае чрезвычайной ситуации.
121. Условия размещения оборудования Удостоверяющего центра в основном и резервном дата-центрах выбраны с учетом действующим в Республике Казахстан требований к системам бесперебойного функционирования технических средств и информационной безопасности[6].
122. Подразделения, реализующие меры пропускного и внутриобъектового режима в Банке, подконтрольны службе внутреннего аудита в соответствии с разделом 8.

Параграф 5.2. ОПЕРАЦИОННЫЙ КОНТРОЛЬ

123. Требования к уровню услуг УЦ со стороны заинтересованных информационных систем Банка составляют:
    1) доступность сервисов – 99,5% в режиме 24/7/365, т.е. не более 1 суток 19 часов и 50 минут простоя в год, без учета плановых работ;
    2) скорость обработки запросов каждого типа – не ниже 8 запросов в минуту;
    3) обслуживание не менее 4 млн. сертификатов в операционном доступе.
124. Физический и логический доступ к оборудованию Удостоверяющего центра разделены процедурно.
125. Для физического доступа к процедурам настройки и обслуживания аппаратных криптографических модулей (Hardware Security Module, HSM) и их ключевого материала требуется участие минимум двоих уполномоченных работников Удостоверяющего центра.
126. Процедуры обработки логических запросов к информационной системе Удостоверяющего центра автоматизированы на уровне прикладного программного обеспечения, с контролем полномочий инициаторов запроса.

Параграф 5.3. КОНТРОЛЬ ПЕРСОНАЛА

127. К назначению на должности работников Удостоверяющего центра и центров регистрации применяются квалификационные требования.
128. Специалисты и руководители Удостоверяющего центра повышают свою квалификацию путем прохождения обучения или сертификации в определенном наборе тем[7].

[6] На дату утверждения Политики сертификатов действуют Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

[7] На дату утверждения Политики сертификатов действуют Требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности, утвержденные постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 89.

129. Ограничений на частоту и последовательность перемещений работников Удостоверяющего центра по службе не накладывается, за исключением квалификационных требований к должностям в Удостоверяющем центре.
130. Привлечение внештатных сотрудников к выполнению функций и работ Удостоверяющего центра не предусмотрено.
131. Каждому работнику Удостоверяющего центра и центров регистрации для компетентного исполнения должностных обязанностей обеспечивается доступ к текстам правовых актов законодательства и внутренних документов Банка.

Параграф 5.4. ПРОЦЕДУРЫ КОНТРОЛЬНОГО ПРОТОКОЛИРОВАНИЯ

132. Обработка запросов Удостоверяющим центром осуществляется с обязательным контрольным протоколированием, включающим регистрацию инициатора запроса.
133. В Удостоверяющем центре обязательному протоколированию подлежат следующие типы событий:
    1) жизненный цикл криптографических ключей Удостоверяющего Центра (генерация и удаление ключей, создание, хранение, восстановление и уничтожение резервных копий);
    2) жизненный цикл сертификатов (получение запросов на выпуск и изменение статуса сертификатов, генерация и изменение статуса сертификатов, генерация и выпуск списков отозванных сертификатов);
    3) жизненный цикл аппаратных криптографических модулей HSM (получение, ввод в эксплуатацию, штатные процедуры, определенные эксплуатационно-технической документацией, сервисное обслуживание, ремонт, вывод из эксплуатации, уничтожение);
    4) жизненный цикл заявлений на выпуск и отзыв сертификатов (тип и реквизиты документа, удостоверяющего личность заявителя, данные должностного лица, проводившего идентификацию и аутентификацию, дата и время обработки);
    5) иные события, подлежащие протоколированию согласно Политике информационной безопасности Банка (сеансы администрирования компонентов информационной системы Удостоверяющего Центра, инциденты информационной безопасности и пр.).
134. Криптографические ключи и данные их активации не подлежат записи в контрольные протоколы.

Параграф 5.5. ВЕДЕНИЕ АРХИВА

135. Удостоверяющий центр ведет архив:
    1) всех выпущенных сертификатов, включая отозванные сертификаты и сертификаты с истекшим сроком действия;
    2) информации о жизненном цикле сертификатов, включая заявления об их отзыве и списки отозванных сертификатов;
    3) контрольных протоколов информационной системы (в соответствии с параграфом 5.4).
136. Архив Удостоверяющего центра ведется на постоянной основе в соответствии с регламентированными сроками и требованиями законодательства Республики Казахстан[8].

[8] Закон Республики Казахстан “Об электронном документе и электронной цифровой подписи” (статья 16) и другие правовые акты.

137. В случае принятия решения о прекращении деятельности Удостоверяющего центра данные архива подлежат хранению в течение срока, установленного законодательством Республики Казахстан[9].
138. Доступ к архиву предоставляется только работникам Удостоверяющего центра.
139. Внешнее резервирование архива Удостоверяющего центра не предусматривается.

Параграф 5.6. СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

140. Новые криптографические ключи Удостоверяющего центра генерируются либо на замену истекающим, либо в дополнение к действующим в целях обеспечения ввода в эксплуатацию новых сервисов.
141. Смена криптографических ключей Удостоверяющего центра осуществляется заблаговременно до истечения срока их действия.
142. Плавность перехода доверяющих сторон к использованию новых криптографических ключей Удостоверяющего центра обеспечивается за счет выпуска сертификатов новых ключей Удостоверяющего центра и прекращения подписания новых сертификатов подписчиков теми ключами Удостоверяющего центра, которые подлежат плановой смене. При этом Удостоверяющий центр продолжает подписывать списки отозванных сертификатов ключом, срок действия которого завершается, вплоть до того момента, когда истечет срок действия последнего сертификата, подписанного с его помощью.

Параграф 5.7. ВОССТАНОВЛЕНИЕ ФУНКЦИОНИРОВАНИЯ В СЛУЧАЕ ЧРЕЗВЫЧАЙНЫХ ПРОИСШЕСТВИЙ ИЛИ КОМПРОМЕТАЦИИ

143. На случай чрезвычайных и иных происшествий, влекущих прерывание функционирования сервисов Удостоверяющего центра, составлен План восстановления функционирования.
144. В Плане восстановления функционирования Удостоверяющего центра предусмотрены:
    1) выбор площадки для восстановления на базе основного или резервного дата-центров;
    2) восстановление рабочих записей из резервной или архивной копии.
145. Приоритетом восстановления функционирования является возобновление основных сервисов удостоверяющего центра по публикации сведений о статусе сертификатов, выпуска и отзыва сертификатов.
146. Оборудование Удостоверяющего центра в дата-центрах обеспечивается резервированным подключением к сети с использованием нескольких каналов.
147. Все изменения в базах данных Удостоверяющего центра постоянно реплицируются между дата-центрами.
148. Обоснованные подозрения в компрометации закрытых криптографических ключей Удостоверяющего центра обрабатываются как инцидент информационной безопасности критического уровня, влекущий за собой введение в действие Плана восстановления функционирования.
149. Проверка готовности резервного оборудования, резервных и архивных копий данных Удостоверяющего центра проверяется переключением работы информационной системы Удостоверяющего центра между основным и резервным дата-центрами не

[9] Закон Республики Казахстан “Об электронном документе и электронной цифровой подписи” (статья 22) и другие правовые акты.

реже одного раза в год с использованием рабочих инструкций, изложенных в Плане восстановления функционирования.

Параграф 5.8. ПРЕКРАЩЕНИЕ РАБОТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

150. В случае принятия решения о прекращение работы Удостоверяющего центра уведомление контрагентов Банка (включая подписчиков Удостоверяющего центра и доверяющих сторон), передача и архивное хранение записей Удостоверяющего центра организовываются в соответствии с Законом Республики Казахстан “Об электронном документе и электронной цифровой подписи” (статья 22).

Глава 6. ТЕХНИЧЕСКИЙ КОНТРОЛЬ БЕЗОПАСНОСТИ

Параграф 6.1. ГЕНЕРАЦИЯ И УСТАНОВКА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

151. Генерация криптографических ключей проводится только с помощью средств криптографической защиты информации, криптографическая стойкость которых подтверждена сертификатом соответствия действующему в Республике Казахстан стандарту, который определяет общие технические требования к средствам криптографической защиты информации[10] (далее – Стандарт).
152. Генерация криптографических ключей Удостоверяющего центра проводится только несколькими выделенными для этой цели и предварительно обученными работниками. При этом используются только аппаратные криптографические модули (HSM), которые соответствуют не ниже чем второму уровню безопасности согласно Стандарту.
153. Закрытые криптографические ключи подписчиков генерируются непосредственно на защищенном носителе ключевой информации, исключающем возможность его разглашения, изменения или несанкционированного использования.
154. Перечень криптографических алгоритмов, для которых предназначены ключи, регистрируемые Удостоверяющим центром, приведен в параграфе 6.1 Правил деятельности Удостоверяющего центра.

Параграф 6.2. ЗАЩИТА ЗАКРЫТЫХ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И ИНЖЕНЕРНЫЕ КОНТРОЛИ КРИПТОГРАФИЧЕСКИХ МОДУЛЕЙ

155. Детальные меры защиты закрытых криптографических ключей Удостоверяющего центра от разглашения, искажения, подмены и несанкционированного использования определены и утверждены внутренними документами Банка и в Политике сертификатов не раскрываются. В настоящем параграфе приведен общий обзор этих мер.
156. Для генерации и хранения закрытых криптографических ключей Удостоверяющего центра используются аппаратные криптографические модули (HSM), сертифицированные на соответствие Стандарту не ниже, чем по второму уровню безопасности.
157. Закрытые криптографические ключи Удостоверяющего центра после создания не подлежат депонированию. Вместе с тем, в целях обеспечения возможности восстановления функционирования информационной систем после чрезвычайного происшествия или иного сбоя в работе непосредственно после генерации каждого нового закрытого криптографического ключа Удостоверяющий центр создается и

[10] На дату утверждения Политики сертификатов действует государственный стандарт Республики Казахстан СТ РК 1073-2007 “Средства криптографической защиты информации. Общие технические требования”.

хранится резервная копия всех используемых в текущий момент закрытых криптографических ключей.

158. На этапе хранения резервная копия закрытых ключей Удостоверяющего центра защищена от разглашения, искажения и подмены криптографическими и организационными мерами.
159. Шифрование резервной копии закрытых криптографических ключей Удостоверяющего центра при их (за-)выгрузке (в) из аппаратного(-ый) криптографического(-ий) модуля(-ь) (HSM) осуществляется с созданием (использованием) данных активации в форме секрета, разделенного на части, каждая из которых закрепляется за отдельным ответственным лицом (хранителем части секрета), записывается на защищенный носитель информации и защищается персональным паролем.
160. Для выполнения операций с криптографическими ключами Удостоверяющего центра, активированными внутри HSM, требуется участие не менее двоих уполномоченных работников Удостоверяющего центра.
161. Вышеуказанные HSM, их комплектующие и детали не подлежат выбытию из Банка или повторному использованию в любом ином качестве.
162. Меры защиты своих закрытых криптографических ключей и данных их активации от разглашения, искажения, подмены и несанкционированного использования на всем протяжении их жизненного цикла, от генерации до уничтожения, подписчики Удостоверяющего центра принимают самостоятельно, в соответствии с требованиями законодательства и Политики сертификатов.

Параграф 6.3. ПРОЧИЕ АСПЕКТЫ УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ

163. Все открытые ключи, заверенные сертификатом, который когда-либо выпустил Удостоверяющий центр, подлежат архивированию в составе этих сертификатов, в соответствии с параграфом 5.5.
164. Срок действия сертификата Удостоверяющего центра составляет 20 лет и исчисляется с даты и времени его выпуска.
165. Сроки действия сертификатов подписчиков в различных информационных системах, обслуживаемых Удостоверяющим центром, составляют 1, 2 или 3 года и устанавливаются нормативно-технической документацией заинтересованной информационной системы Банка.
166. Для непрерывной работы в информационных системах, которые требуют наличия сертификатов, выпущенных Удостоверяющим центром, подписчики в соответствии с Политикой сертификатов наделены правом запрашивать выпуск новых сертификатов на замену сертификатов с истекающим сроком действия.

Параграф 6.4. ДАННЫЕ АКТИВАЦИИ

167. Закрытые криптографические ключи подписчиков Удостоверяющего центра используются непосредственно на защищенном носителе ключевой информации, исключающем возможность их разглашения, изменения или несанкционированного использования.
168. Для использования закрытого криптографического ключа подписчику Удостоверяющего центра необходимо создать и применять данные активации в форме пароля.

Параграф 6.5. КОНТРОЛЬ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ

169. Вычислительные ресурсы, программное обеспечение и данные информационной системы Удостоверяющего центра защищаются от несанкционированного доступа в соответствии с Политикой информационной безопасности Банка и в Политике сертификатов не раскрываются. В настоящем параграфе приведен общий обзор этих мер.
170. Серверы для подписи сертификатов, списков отозванных сертификатов, ответов (квитанций) службы OCSP изолированы от несанкционированного доступа.
171. Операционные системы серверов поддерживаются на высоком уровне защиты путем применения рекомендованных пакетов защиты и обновлений, в том числе антивирусных.
172. Количество запущенных на серверах служб операционных систем сведено до необходимого минимума.
173. Доступ к основным серверам разрешен только назначенным администраторам, пользователи программных приложений Удостоверяющего центра не имеют доступа к системным или технологическим учетным записям.
174. Сегменты сети, используемые для обслуживания участников инфраструктуры открытых ключей, логически отделены от остальной сети Банка. Это выделение исключает любой сетевой доступ пользователей к данным Удостоверяющего центра кроме доступа через определенные прикладные программные процессы. Прямой доступ к базам данных Удостоверяющего центра ограничен минимально необходимой группой администраторов информационной системы.
175. Для защиты сегментов сети Удостоверяющего центра от внешнего или внутреннего вмешательства, ограничения содержания и источников сетевой активности используются межсетевые экраны.
176. В деятельности Удостоверяющего центра используются средства криптографической защиты информации (СКЗИ: HSM и программные СКЗИ), сертифицированные на соответствие требованиям Стандарта.
177. Специальных требований по сертификации информационной безопасности иных (некриптографических) компонентов и программного обеспечения не выдвигается.

Параграф 6.6. КОНТРОЛЬ УПРАВЛЕНИЯ РАЗВИТИЕМ И БЕЗОПАСНОСТЬЮ

178. Работоспособность и целостность технических и программных средств Удостоверяющего центра обеспечивается системой организационных и технических мер, основанных на разделении прав и ответственности за использование этих средств, прав доступа к ним и техническим средствам ИТ-архитектуры, обеспечивающей доступ.
179. В целях апробации любых изменений в информационной системе Удостоверяющий центр имеет и поддерживает ее тестовый контур, обеспеченный необходимым минимумом вычислительной техники, средств криптографической защиты информации и лицензий на использование программного обеспечения.

Параграф 6.7. КОНТРОЛЬ БЕЗОПАСНОСТИ СЕТИ

180. Функции Удостоверяющего центра выполняются в корпоративной сети Банка, защищенной (в регламентированном порядке) от несанкционированного доступа и вмешательства.

Параграф 6.8. МЕТКИ ВРЕМЕНИ

181. Сертификаты, списки отозванных сертификатов, ответы квитанции (ответы службы) OCSP, контрольные протоколы информационной системы Удостоверяющего центра, содержащие информацию о выпуске и изменении статуса сертификатов, содержат информацию о дате и времени событий.

Глава 7. ПРОФИЛИ СЕРТИФИКАТОВ, СОС и OCSP

Параграф 7.1. ПРОФИЛИ СЕРТИФИКАТА

182. Удостоверяющий центр выпускает сертификаты в соответствии со стандартом ITU-T X.509.
183. Основные поля, содержащиеся в сертификатах, вместе с требованиями к их содержанию определяются в соответствии с параграфом 7.1 правил деятельности Удостоверяющего центра.

Параграф 7.2. ПРОФИЛИ СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ

184. Удостоверяющий центр выпускает списки отозванных сертификатов в соответствии со стандартом ITU-T X.509.
185. Основные поля и расширения, содержащиеся в списках отозванных сертификатов, вместе с требованиями к их содержанию определяются в соответствии с параграфом 7.2 правил деятельности Удостоверяющего центра.

Параграф 7.3. ПРОФИЛЬ СЕРВИСА OCSP

186. Сервис OCSP для получения информации о статусе сертификатов, выпущенных Удостоверяющим центром, предоставляется в соответствии с рекомендациями RFC 2560 “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP” (Онлайн протокол статуса сертификатов интернет инфраструктуры открытых ключей X.509).

Глава 8. ПРОВЕРКА ДЕЯТЕЛЬНОСТИ

187. Деятельность Удостоверяющего центра подлежит регулярным проверкам уполномоченного государственного органа в сфере обеспечения информационной безопасности в процессе аккредитации.

Глава 9. ПРОЧИЕ ВОПРОСЫ

Параграф 9.1. ТАРИФЫ

188. Расходы на предоставление услуг Удостоверяющего центра не тарифицируются и не оплачиваются.

Параграф 9.2. ОТВЕТСТВЕННОСТЬ

189. Ответственность участников инфраструктуры открытых ключей, обслуживаемой Удостоверяющим центром, установлена законодательством Республики Казахстан[11].

[11] Кодекс Республики Казахстан “Об административных правонарушениях”, статья 640.

Параграф 9.3. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

190. Сертификаты, выпускаемые Удостоверяющим центром, и информация об их отзыве или ином статусе, публично доступные в хранилище Удостоверяющего центра, не являются и рассматриваются в качестве конфиденциальной информации.

Параграф 9.4. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ УЧАСТНИКОВ

191. Любой подписчик или доверяющая сторона признают, что, подавая заявление на выпуск сертификата в Удостоверяющий центр, они дают согласие на размещение содержащейся в нем информации о себе в публичном доступе. Заявление на выпуск сертификата является письменным документом, означающим согласие субъекта на сбор и обработку его персональных данных в соответствии с законодательством Республики Казахстан по вопросам персональных данных и их защиты[12].

Параграф 9.5. ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

192. В своей деятельности Удостоверяющий центр использует программное обеспечение, авторские и исключительные имущественные права на которое не принадлежат Банку. Порядок использования программного обеспечения определяется условиями лицензий, приобретенных Банком.
193. Подписчики сохраняют все свои права на имена и торговые марки, содержащиеся в сертификатах.

Параграф 9.6. ГАРАНТИИ И ЗАВЕРЕНИЯ

194. Каждый подписчик Удостоверяющего центра обеспечивает:
    1) использование только того своего закрытого криптографического ключа, для которого имеется соответствующий ему сертификат, выпущенный Удостоверяющим центром, принятый подписчиком и действительный на момент использования (не просрочен и не отозван);
    2) защиту своих закрытых криптографических ключей от доступа любых других лиц;
    3) достоверность сведений о себе, предоставляемых для выпуска сертификатов в центр регистрации;
    4) проверку достоверности сведений о себе, содержащихся в сертификате, перед принятием сертификата;
    5) не использование своего закрытого ключа в целях подписания каких-либо сертификатов, списков отозванных сертификатов, любого другого формата удостоверений открытого ключа или информации о его статусе.
195. Каждый подписчик и каждая доверяющая сторона обеспечивает при использовании сертификатов, выпущенных Удостоверяющим центром, принятие только обоснованных решений, опирающихся на достаточный объем объективной информации о подписчике и его сертификате.

Параграф 9.7. ОТКАЗ ОТ ГАРАНТИЙ

196. Удостоверяющий центр не несет перед подписчиками и доверяющими сторонами дополнительной ответственности, вытекающей из договоров оказания банковских услуг, включая ответственность за товарную пригодность и соответствие, кроме той ответственности, которая установлена законодательством Республики Казахстан по

[12] Закон Республики Казахстан “О персональных данных и их защите”, статья 8.

вопросам электронного документа и электронной цифровой подписи и задекларирована Политикой сертификатов.

Параграф 9.8 ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

197. Ответственность Удостоверяющего центра, центров регистрации, подписчиков и доверяющих сторон ограничена законодательством Республики Казахстан[13].

Параграф 9.9. КОМПЕНСАЦИИ

198. В части, не противоречащей действующему законодательству Республики Казахстан, на счет подписчиков относятся расходы, связанные с компенсацией:
    1) предоставления ошибочной, вводящей в заблуждение или заведомо ложной информации в заявлениях на выпуск или отзыв сертификата;
    2) непреднамеренного или умышленного сокрытия существенных фактов, подлежащих отражению в заявлении на выпуск или отзыв сертификата;
    3) непринятия мер защиты собственного закрытого криптографического ключа, приведшее к его компрометации, разглашению, изменению или несанкционированному использованию;
    4) использования в составе своего выделенного имени названий, нарушающих права интеллектуальной собственности третьих лиц.
199. В части, не противоречащей действующему законодательству Республики Казахстан, на счет доверяющих сторон относятся расходы, связанные с компенсацией:
    1) необоснованного доверия к сертификату, допущенному из-за нарушения обязательств доверяющей стороны;
    2) непринятием мер по проверке сертификата с целью определения его сроков действия и статуса (отозван/не отозван).

Параграф 9.10. ВСТУПЛЕНИЕ В СИЛУ И ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ

200. Политика сертификатов и все изменения и дополнения к ней вступают в силу со дня опубликования на официальном ресурсе Банка в сети Интернет.
201. Политика сертификатов, с учетом публикуемых изменений и дополнений к ней, сохраняет силу до момента опубликования новой редакции Политики сертификатов на официальном ресурсе Банка в сети Интернет.

Параграф 9.11. ИНДИВИДУАЛЬНЫЕ УВЕДОМЛЕНИЯ И СВЯЗЬ С УЧАСТНИКАМИ

202. Участники инфраструктуры открытых ключей: Удостоверяющий центр, центры регистрации, подписчики и доверяющие стороны, - для связи друг с другом используют любые целесообразные каналы, соответствующие предмету взаимодействия, степени важности и срочности коммуникации, если иное не определено соглашением между сторонами.

Параграф 9.12. ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ

203. Незначительные изменения в Политику сертификатов (изменение адресов и ссылок, контактной информации, исправление опечаток и т.п.) вносятся без предварительного уведомления участников инфраструктуры открытых ключей. Решения об уровне значимости изменений и дополнений (существенные или несущественные) принимаются Удостоверяющим центром самостоятельно.

[13] Кодекс Республики Казахстан “Об административных правонарушениях”, статья 640.

204. Существенные изменения и дополнения в Политику сертификатов Удостоверяющий центр предварительно публикует, в форме проекта, на официальном информационном ресурсе Банка в сети Интернет, как правило за 21 календарный день до вступления в силу, если иное не предусмотрено опубликованными изменениями в законодательстве Республики Казахстан.
205. В случае внесения изменений и дополнений в Политику сертификатов Удостоверяющий центр отвечает за определение необходимости внесения изменений и дополнений в перечень объектных идентификаторов Политики сертификатов и приведение его в соответствие с новой редакцией Политики сертификатов.
206. Если в связи с изменениями и дополнениями в Политике сертификатов необходимо изменение перечня объектных идентификаторов Политики сертификатов, то соответствующие изменения в него, а также в правила деятельности Удостоверяющего центра публикуются и вносятся одновременно.

Параграф 9.13. РАЗРЕШЕНИЕ СПОРОВ

207. Споры между участниками инфраструктуры открытых ключей: между подписчиками и доверяющими сторонами, а также между подписчиком или доверяющей стороной с одной стороны, и Удостоверяющим центром или центром регистрации, с другой стороны, - разрешаются в соответствии с положениями договоров, действующих между сторонами.
208. Если спор не решен в досудебном порядке, то он подлежит разрешению в судебном порядке.

Параграф 9.14. ЮРИСДИКЦИЯ

209. Для разрешения споров, предметом которых являются разногласия по существу Политики сертификатов, применяется законодательство Республики Казахстан.

Параграф 9.15. СООТВЕТСТВИЕ ПРИМЕНИМОМУ ЗАКОНОДАТЕЛЬСТВУ

210. К участникам инфраструктуры открытых ключей: Удостоверяющему центру, центрам регистрации, подписчикам и доверяющим сторонам, - применимы требования законодательства Республики Казахстан по вопросам:
    1) электронного документа и электронной цифровой подписи;
    2) разрешений и уведомлений (в части, касающейся реализации средств криптографической защиты информации);
    3) платежей и платежных систем;
    4) персональных данных и их защиты.

Параграф 9.16. ПРОЧИЕ ПОЛОЖЕНИЯ

211. В случае если часть положений Политики сертификатов будет признана неприменимой судом или уполномоченным государственным органом, остальная их часть сохраняет силу.
212. В случае наступления обстоятельств непреодолимой силы (форс-мажор) участники инфраструктуры открытых ключей: Удостоверяющий центр, центры регистрации, подписчики и доверяющие стороны, - руководствуются соответствующими положениями действующих между ними договоров.