

ПОЛИТИКА
применения регистрационных свидетельств
Удостоверяющего центра

Владелец:	Департамент цифрового развития	
Совладелец:		
Разработчик:	Департамент цифрового развития	
Субъекты регулирования:	Департамент технологических решений Департамент сопровождения ИС Департамент архитектурных решений Департамент системного обеспечения и телекоммуникаций Департамент защиты информационных систем	
Утвержден:	Советом директоров (протокол № 02/06/23-01)	от «02» июня 2023г.
ВД, признаваемые утратившими силу:	Политика применения регистрационных свидетельств Удостоверяющего центра	Утверждена Советом директоров АО «Jusan Bank» (протокол № 27/04/23-01 от 27.04.2023г.)

Содержание

Глава 1. Общие положения.....	3
Глава 2. Глоссарий	3
Глава 3. Назначение регистрационных свидетельств.....	5
Глава 4. Хранилище Удостоверяющего центра и публикация в нем данных	5
§1. Хранилище и публикация.....	5
§2. Периодичность актуализации данных в хранилище.....	5
§3. Контроль доступа к хранилищу	5
Глава 5. Идентификация и аутентификация	6
§1. Требования к именам	6
§2. Первоначальная проверка идентичности.....	6
Глава 6. Общие требования к жизненному циклу регистрационных	6
свидетельств.....	6
§1. Заявление на выпуск (выдачу) регистрационного свидетельства	6
§2. Обработка заявления на выпуск (выдачу) регистрационного свидетельства	6
§3. Выпуск регистрационных свидетельств	6
§4. Использование регистрационных свидетельств и ключевых пар	6
§5. Смена ключей и обновление сроков действия в регистрационных свидетельствах	7
§6. Изменение данных в регистрационных свидетельствах	7
§7. Отзыв регистрационных свидетельств.....	7
Глава 7. Виды контроля Удостоверяющего центра	7
§1. Физический контроль	7
§2. Операционный контроль	7
§3. Управляющий контроль	7
§4. Процедуры контрольного протоколирования	7
§5. Смена ключей Удостоверяющего центра	8
§6. Восстановление функционирования в случае чрезвычайных происшествий или	8
компрометации	8
§7. Ведение архива.....	8
Глава 8. Технический контроль безопасности ключей.....	8
§1. Генерация и установка.....	8
§2. Защита закрытых ключей и инженерные контроли.....	8
криптографических модулей.....	8
§3. Иные аспекты управления ключами.....	8
§4. Контроль безопасности вычислительных ресурсов.....	9
§5. Контроль управления развитием и безопасностью.....	9
Глава 9. Профили регистрационных свидетельств, COPC и OCSP	9
§1. Профили регистрационных свидетельств.....	9
§2. Профили списка отозванных регистрационных свидетельств	9
§3. Профиль сервиса OCSP	9
Глава 10. Проверка деятельности	9
Глава 11. Прочие вопросы	9
§1. Тарифы.....	9
§2. Защита персональных данных участников.....	9
§3. Права интеллектуальной собственности.....	9
§4. Гарантии и заверения.....	10
§5. Уведомления и связь с участниками	10
§6. Разрешение споров.....	10
Глава 12. Ответственность	10
Глава 13. Конфиденциальность	10
Глава 14. Заключительные положения.....	10

Глава 1. Общие положения

1. Настоящая Политика применения регистрационных свидетельств удостоверяющего центра (далее – Политика) определяет общее положение и направление Удостоверяющего центра (далее – УЦ), связанных с жизненным циклом выпущенных регистрационных свидетельств УЦ.

2. Политика разработана в соответствии с законодательством Республики Казахстан¹ (далее – РК) в целях обеспечения функционирования УЦ.

3. Политика 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).

4. Целью Политики является определение общих требований к процедурам и условиям предоставления услуг владельцам УЦ, связанных с жизненным циклом регистрационных свидетельств УЦ.

5. Основными задачами Политики являются, определение основных принципов и требований к применению регистрационных свидетельств в информационных системах Банка.

6. Требования Политики обязательны для исполнения всеми участникам инфраструктуры открытых ключей Банка, использующими регистрационные свидетельства УЦ.

Глава 2. Глоссарий

7. В Политике используются следующие понятия:

1) аутентификация – способ проверки подлинности пользователя при помощи комбинации различных параметров, в том числе генерации и ввода паролей или аутентификационных признаков (цифровых сертификатов, токенов, смарт-карт, генераторов одноразовых паролей и средств биометрической идентификации);

2) Банк – АО «Jusan Bank»;

3) ВД – внутренние документы Банка;

4) владелец регистрационного свидетельства – физическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;

5) данные активации – любые данные, за исключением ключей, которые необходимы для выполнения криптографических операций и требуют защиты: персональные идентификационные номера (PIN), парольные фразы, компоненты разделенного ключа, биометрические параметры и другие;

6) доверяющая сторона – пользователь регистрационного свидетельства, использующий полученные сведения о регистрационном свидетельстве, выпущенном УЦ, для проверки принадлежности ЭЦП владельцу посредством корневого УЦ РК, портала Банка, государственных информационных систем, использующие регистрационные свидетельства УЦ;

7) дерево международных объектных идентификаторов – стандартизированный ITU-T и ISO/IEC механизм (X.660) именованная любых реальных или абстрактных объектов однотипными недвусмысленными всеобъемлющими именами, предназначенный для регистрации имен с помощью трех иерархических деревьев особой формы (от 3 разных

¹ Законодательство РК, в том числе Закон РК об электронном документе и электронной цифровой подписи; Закон РК о персональных данных и их защите; Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре, утвержденные Приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НК; Правила проверки подлинности электронной цифровой подписи, утвержденные Приказом Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187

корней), в которых каждый последующий узел наделен целочисленным номером и ответственен за дальнейшее выделение и регистрацию ветвей, исходящих от него самого;

8) жизненный цикл – выдача, хранение и прекращение срока действия (отзыв), публикация выпущенных регистрационных свидетельств УЦ;

9) закрытый ключ электронной цифровой подписи (закрытый ключ ЭЦП) – последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;

10) идентификация – в контексте Политики, процесс (или результат процесса), который устанавливает идентичность физического лица (показывающий, что данное лицо является однозначно определенным реально существующим лицом);

11) информационная система (ИС) – центр регистрации, организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

12) инфраструктура открытых ключей (ИОК) – набор средств (технических, материальных, людских и прочих), 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;

13) объектный идентификатор – уникальный набор цифр, который связан с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов;

14) открытый ключ электронной цифровой подписи (открытый ключ ЭЦП) – последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

15) Правила деятельности удостоверяющего центра (Правила) – ВД, который определяет порядок организации основной деятельности УЦ, осуществляемой в соответствии с Политикой;

16) регистрационное свидетельство – электронный документ, выдаваемый УЦ для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом РК «Об электронном документе и электронной цифровой подписи»;

17) список отозванных регистрационных свидетельств (СОРС) – часть регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва;

18) средства криптографической защиты информации (СКЗИ) – средства, реализующие алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами;

19) средства электронной цифровой подписи (средства ЭЦП) – совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи (средства электронной цифровой подписи являются одной из разновидностей средств криптографической защиты информации);

20) участники инфраструктуры открытых ключей (участник ИОК) – работники УЦ, отвечающие за обслуживание клиентов, а также владельцы регистрационных свидетельств;

21) Удостоверяющий центр (УЦ) - Банк, удостоверяющий соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающий достоверность регистрационного свидетельства;

22) центр сертификации – программно-аппаратный комплекс УЦ для выдачи, обслуживания и отзыва регистрационного свидетельства, своевременный импорт СОРС, действующий в соответствии с законодательством РК;

23) центр регистрации - фронтальная система Банка (мобильное приложение Jusan),

принимаящая заявления от владельца на выпуск и отзыв регистрационного свидетельства, а также осуществляющая проверку, идентификацию и аутентификацию заявителей;

24) электронная цифровая подпись (ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

25) электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством ЭЦП.

Иные термины и сокращения, используемые по тексту Политики, применяются в соответствии со значением, закрепленным в законодательстве РК, общепанковском глоссарии, а при их отсутствии в законодательстве РК и общепанковском глоссарии – в соответствии со значением, закрепленном в международной банковской практике.

Все ссылки на части, разделы, главы, параграфы, пункты, приложения в тексте Политики без указания названия документа относятся к настоящей Политике.

Глава 3. Назначение регистрационных свидетельств

8. УЦ выдает, регистрирует, отзывает, хранит регистрационные свидетельства, ведет регистр регистрационных свидетельств, выданных в установленном порядке, а также публикует регистрационные свидетельства УЦ и необходимые нормативные документы, другие данные о своих сервисах.

9. Не допускается использование владельцами регистрационных свидетельств, выпущенных им регистрационных свидетельств в центре сертификации, связанных с управлением источниками повышенной опасности (ядерным, системами контроля вооружений и другие), а также в любых случаях, которые могут повлечь за собой ранение/смерть персонала, или ущерб окружающей среде.

10. Не допускается использование регистрационных свидетельств, выпущенных УЦ, способами, противоречащими законодательству РК, Политике, Правилам.

11. Регистрационные свидетельства владельцев УЦ используются для работы с программным обеспечением доверяющих сторон.

Глава 4. Хранилище Удостоверяющего центра и публикация в нем данных

§1. Хранилище и публикация

12. Составной частью центра сертификации УЦ является хранилище, которое УЦ использует в качестве справочника информации при предоставлении своих основных сервисов.

13. УЦ ведет раздел на официальном информационном ресурсе Банка в сети Интернет (корпоративный интернет ресурс), в котором публикует регистрационные свидетельства УЦ и необходимые нормативные документы и другие данные о своих сервисах (далее – Сведения).

§2. Периодичность актуализации данных в хранилище

14. УЦ публикует каждое вновь выпущенное регистрационное свидетельство в хранилище.

15. В случае отзыва регистрационного свидетельства УЦ удаляет его в порядке, определенном в Правилах.

16. Действие регистрационного свидетельства прекращается, по истечении срока на который выдано регистрационное свидетельство.

§3. Контроль доступа к хранилищу

17. УЦ создает ключи ЭЦП по обращению заявителей/владельцев с принятием мер для защиты закрытых ключей ЭЦП от неправомерного доступа в соответствии с Правилами и ВД, регламентирующим процедуру обеспечения ИБ ИС.

18. УЦ принимает меры для предотвращения утери, модификации, подделки находящихся на хранении открытых ключей и/или закрытых ключей ЭЦП.

19. Сведения, публикуемые на сайте УЦ, предоставляются в режиме свободного доступа с правами «только для чтения».

Глава 5. Идентификация и аутентификация

§1. Требования к именам

20. УЦ использует правила именования субъектов, призванные обеспечить идентификацию владельцев во всех выпускаемых регистрационных свидетельствах.

§2. Первоначальная проверка идентичности

21. Первоначальная проверка идентичности и любая последующая процедура, требующая идентификации владельца регистрационного свидетельства проводится в соответствии с Правилами.

Глава 6. Общие требования к жизненному циклу регистрационных свидетельств

§1. Заявление на выпуск (выдачу) регистрационного свидетельства

22. Заявление на выпуск (выдачу) регистрационного свидетельства имеют право подавать физические лица.

23. Принципы оформления заявлений на выпуск регистрационного свидетельства владельца УЦ определены Правилами.

§2. Обработка заявления на выпуск (выдачу) регистрационного свидетельства

24. Центр регистрации обрабатывает заявление на выпуск регистрационного свидетельства в соответствии с законодательством РК по вопросам электронного документа и электронной цифровой подписи.

25. Срок рассмотрения и обработки заявлений на выпуск регистрационных свидетельств определяется Правилами.

26. Зарегистрированное заявление отклоняется УЦ в случаях, установленных законодательством РК по вопросам электронного документа и электронной цифровой подписи и Правилами.

§3. Выпуск регистрационных свидетельств

27. Каждое регистрационное свидетельство создается УЦ по факту регистрации и успешной обработки отдельного заявления на выпуск регистрационного свидетельства в центре регистрации.

28. Принципы и основные этапы выпуска регистрационного свидетельства владельцу УЦ определены в Правилах.

§4. Использование регистрационных свидетельств и ключевых пар

29. Необходимые условия использования регистрационных свидетельств и пар ключей определены Правилами.

30. УЦ не отвечает перед использующими регистрационные свидетельства лицами, которые не обязались выполнять требования Политики и Правил в части, касающейся обязанностей пользователя регистрационных свидетельств (доверяющей стороны), в форме письменного обязательства, электронного документа либо иной формы согласия, зафиксированной в ИС Банка.

§5. Смена ключей и обновление сроков действия в регистрационных свидетельствах

31. УЦ не предоставляет услуги по обновлению сроков действия ключей в регистрационных свидетельствах. Смена ключей в регистрационных свидетельствах осуществляется в соответствии с Правилами.

§6. Изменение данных в регистрационных свидетельствах

32. УЦ не предоставляет услуги по изменению данных в регистрационных свидетельствах.

§7. Отзыв регистрационных свидетельств

33. Регистрационные свидетельства, выпущенные УЦ, могут быть отозваны УЦ по основаниям установленным законодательством РК по вопросам электронного документа и электронной цифровой подписи и в Правилах.

Глава 7. Виды контроля Удостоверяющего центра

§1. Физический контроль

34. Условия размещения оборудования центра сертификации в основном и резервном центрах обработки данных соответствуют требованиям, действующим в РК к системам бесперебойного функционирования технических средств и информационной безопасности, а также регламентированным Правилами.

35. Операции с ключами УЦ проводятся только на физически защищенных объектах, в условиях, где затруднены и фиксируются любые попытки несанкционированного доступа, использования или раскрытия конфиденциальной информации. Допускается дистанционное осуществление деятельности УЦ при условии соблюдения требований Правил, ВД о процедуре обеспечения ИБ ИС и иных ВД Банка по вопросам информационной безопасности, а также законодательством РК.

§2. Операционный контроль

36. Физический и логический доступ к оборудованию центра сертификации разделены процедурно.

37. 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 Банка в соответствии с Правилами.

38. Процедуры обработки логических запросов к центру сертификации автоматизированы на уровне прикладного программного обеспечения, с контролем полномочий инициаторов запроса.

§3. Управляющий контроль

39. Все функции для работы УЦ выполняются работниками УЦ в соответствии с полномочиями, регламентированными в Правилах.

40. Допускается привлечение контрагентов в рамках договоров поставки и технической поддержки аппаратного и программного обеспечения центра сертификации УЦ.

41. Привлечение лиц на основании договоров гражданско-правового характера к выполнению функций и работ УЦ не допускается.

§4. Процедуры контрольного протоколирования

42. Обработка запросов (на выдачу и отзыв регистрационных свидетельств, проверку состояния регистрационных свидетельств и другие) УЦ осуществляется с обязательным контрольным протоколированием, включающим регистрацию инициатора запроса.

43. Типы событий, подлежащих протоколированию, определены Правилами.

§5. Смена ключей Удостоверяющего центра

44. Смена ключей осуществляется в соответствии с эксплуатационно-технической документацией аппаратных криптографических модулей (HSM) УЦ в соответствии с Правилами.

§6. Восстановление функционирования в случае чрезвычайных происшествий или компрометации

45. На случай чрезвычайных и иных происшествий, влекущих прерывание функционирования сервисов УЦ, УЦ действует в соответствии с Инструкцией по действиям работников Удостоверяющего центра во внештатных, кризисных ситуациях, Инструкцией по резервному копированию, архивированию и восстановлению данных информационных ресурсов Удостоверяющего центра, а также ВД, регламентирующим правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации.

46. Приоритетом восстановления функционирования является возобновление основных сервисов УЦ по публикации сведений о статусе регистрационных свидетельств, выпуска и отзыва регистрационных свидетельств.

§7. Ведение архива

47. УЦ ведет архив, в котором хранит письменные и электронные документы, определенные Правилами.

48. Архив УЦ ведется на постоянной основе в соответствии с регламентированными сроками и требованиями законодательства РК.

Глава 8. Технический контроль безопасности ключей

§1. Генерация и установка

49. Генерация ключей центром сертификации проводится только с помощью средств криптографической защиты информации, криптографическая стойкость которых подтверждена сертификатом соответствия действующему в РК стандарту, который определяет общие технические требования к средствам криптографической защиты информации (далее – Стандарт).

50. Генерация ключей центром сертификации проводится только несколькими выделенными для этой цели и предварительно обученными работниками УЦ в соответствии с Правилами.

§2. Защита закрытых ключей и инженерные контроли криптографических модулей

51. Меры защиты закрытых ключей УЦ от разглашения, искажения, подмены и несанкционированного использования определены в Правилах

52. Для генерации и хранения закрытых ключей центром сертификации используются аппаратные криптографические модули (HSM), сертифицированные на соответствие Стандарту. При этом закрытые ключи центра сертификации создаются в модулях безопасности HSM, сертифицированных на соответствие Стандарту по уровню не ниже второго; закрытые ключи облачных регистрационных свидетельств создаются в модулях безопасности HSM, сертифицированных на соответствие Стандарту по уровню не ниже третьего. Более подробная информация изложена в Правилах.

§3. Иные аспекты управления ключами

53. Все открытые ключи, заверенные регистрационным свидетельством, которое когда-либо выпустил УЦ, подлежат архивированию в составе этих регистрационных свидетельств.

54. Порядок управления ключами определяется Правилами.

§4. Контроль безопасности вычислительных ресурсов

55. Вычислительные ресурсы, программное обеспечение и данные центра сертификации защищаются от несанкционированного доступа в соответствии с ВД о процедуре обеспечения ИБ ИС и Правилами.

§5. Контроль управления развитием и безопасностью

56. Работоспособность и целостность технических и программных средств УЦ 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.

Глава 9. Профили регистрационных свидетельств, COPC и OSCP

§1. Профили регистрационных свидетельств

57. УЦ выпускает регистрационные свидетельства в соответствии со стандартом ITU-T X.509.

58. Основные поля, содержащиеся в регистрационных свидетельствах, вместе с требованиями к их содержанию определяются в соответствии с Правилами.

§2. Профили списка отозванных регистрационных свидетельств

59. УЦ выпускает списки отозванных регистрационных свидетельств в соответствии со стандартом ITU-T X.509.

60. Основные поля и расширения, содержащиеся в списках отозванных регистрационных свидетельств, вместе с требованиями к их содержанию определяются в соответствии с Правилами.

§3. Профиль сервиса OSCP

61. Сервис OSCP для получения информации о статусе регистрационных свидетельств, выпущенных УЦ, предоставляется в соответствии с Правилами.

Глава 10. Проверка деятельности

62. Уполномоченный государственный орган вправе осуществлять проверки деятельности УЦ.

Глава 11. Прочие вопросы

§1. Тарифы

63. Услуги УЦ не тарифицируются и не оплачиваются.

§2. Защита персональных данных участников

64. УЦ обеспечивает защиту персональных данных участников ИОК в соответствии с законодательством РК по вопросам персональных данных и их защиты.

§3. Права интеллектуальной собственности

65. В своей деятельности УЦ использует программное обеспечение в соответствии с Правилами. Порядок использования программного обеспечения определяется условиями лицензий, приобретенных Банком.

§4. Гарантии и заверения

66. УЦ и центр сертификации в своей деятельности выполняет условия гарантий и заверений владельца и пользователя регистрационных свидетельств (владельца и доверяющей стороны), изложенные в Правилах.

§5. Уведомления и связь с участниками

67. Участники ИОК для связи друг с другом используют каналы, в соответствии с Правилами.

§6. Разрешение споров

68. Споры между участниками ИОК: между владельцами и пользователями регистрационных свидетельств (владельцами и доверяющими сторонами), а также между владельцем или доверяющей стороной с одной стороны, и Удостоверяющим центром, с другой стороны, - разрешаются в соответствии с положениями договоров, действующих между сторонами, и/или законодательством РК.

69. В случае если часть положений Политики будет признана неприменимой судом или уполномоченным государственным органом, остальная их часть сохраняет силу.

Глава 12. Ответственность

70. Ответственность УЦ, владельцев и пользователей регистрационных свидетельств (владельцев и доверяющих сторон) ограничена законодательством РК.

71. Ответственность за неисполнение и/или ненадлежащее исполнение Политики возлагается на работников и руководителей структурных подразделений Головного Банка и обособленных подразделений Банка, участвующих в процессе обслуживания центра регистрации, центра сертификации, УЦ.

72. Общий контроль за организацией и поддержание УЦ, центра регистрации, центра сертификации осуществляется подразделениями, участвующими в процессе обслуживания центра регистрации, центра сертификации, УЦ, как участниками первой линии защиты системы внутреннего контроля Банка, регламентированной Политикой внутреннего контроля Банка. Общий контроль функционирования центра регистрации, центра сертификации, УЦ осуществляется на постоянной основе.

73. Руководитель подразделения цифрового развития несет ответственность за организацию и поддержание эффективного внутреннего контроля в соответствии с положениями ВД Банка, регламентирующих политику внутреннего контроля и процедуру осуществления внутреннего контроля в Банке.

Глава 13. Конфиденциальность

74. УЦ обеспечивает защиту сведений о владельцах регистрационных свидетельств и раскрывает их в случаях, предусмотренных законодательством РК.

75. Сведения о владельцах регистрационных свидетельств, являющиеся конфиденциальными в соответствии с соглашением сторон, не включаются в общедоступный регистр регистрационных свидетельств.

76. Регистрационные свидетельства, выпускаемые УЦ, и информация об их отзыве или ином статусе, не являются и не рассматриваются в качестве конфиденциальной информации.

Глава 14. Заключительные положения

77. Политика публикуется по истечении 5 (пяти) рабочих дней со дня утверждения Советом Директоров Банка, если решением Совета Директоров не установлен иной срок публикации.

78. Решение о признании утраты силы Политики вступают в силу в день ввода в действие новой редакции Политики или замещающего его внутреннего документа.

79. Политика и все изменения и дополнения к ней вступают в силу со дня ее опубликования на корпоративном интернет-ресурсе АО «Jusan Bank».

80. Положения, не урегулированные Политикой, регулируются законодательством РК.

81. В случае изменения законодательства РК и возникновения противоречий отдельных положений Политики законодательству РК, такие положения Политики утрачивают силу, и работники Банка руководствуются в своей деятельности законодательством РК до соответствующей актуализации Политики.

82. В случае внесения изменений и дополнений в Политику, Политика утверждается Советом Директоров Банка в новой редакции.

83. Все изменения и дополнения в Политику утверждаются и публикуются в новой редакции Политики и размещаются на корпоративном интернет ресурсе Банка.

84. Публикация новой утвержденной редакции Политики является официальным уведомлением о вступлении ее в силу для пользователей всех регистрационных свидетельств, выпущенных УЦ, включая их владельцев.

85. С даты публикации новой редакции Политики, если иное не предусмотрено переходными положениями утверждающего решения, изменения и дополнения становятся обязательными для применения пользователями всех регистрационных свидетельств, выпущенных УЦ, включая их владельцев.

86. Политика с учетом публикуемых изменений и дополнений к ней, сохраняет силу до момента опубликования новой редакции Политики на корпоративном интернет ресурсе Банка.

87. Незначительные изменения в Политику (изменение адресов и ссылок, контактной информации, исправление опечаток и прочее) вносятся без предварительного уведомления участников ИОК. Решения об уровне значимости изменений и дополнений (существенные или несущественные) принимаются участниками процесса по обслуживанию УЦ самостоятельно.

88. Существенные изменения и дополнения в Политику УЦ предварительно публикует, в форме проекта, на корпоративном интернет ресурсе Банка, как правило за 14 (четырнадцать) календарных дней до вступления в силу, если иное не предусмотрено опубликованными изменениями в законодательстве РК.

89. В случае внесения изменений и дополнений в Политику участниками процесса по обслуживанию УЦ отвечает за определение необходимости внесения изменений и дополнений в перечень объектных идентификаторов политики регистрационных свидетельств и приведение его в соответствие с новой редакцией Политики.

90. Если в связи с изменениями и дополнениями в Политике необходимо изменение перечня объектных идентификаторов политики регистрационных свидетельств, то соответствующие изменения в него, а также в Правилах публикуются и вносятся одновременно.