



**Акционерное общество «Национальная платежная корпорация
Национального Банка Республики Казахстан»**

Уровень доступа: Общий

Утверждена
решением Правления АО «НПК»
от «05» 03 2025 года
(приложение № 2
к протоколу № 7)

Дата вступления в силу с
«05» 03 2025 г.

**Регламент деятельности
удостоверяющего центра акционерного общества «Национальная платежная
корпорация Национального Банка Республики Казахстан»
(CERTIFICATE PRACTICE STATEMENT)**

Рег. № 14

г. Алматы

Содержание

1. Введение	5
1.1. Общие положения.....	5
1.2. Наименование и идентификация документа	6
1.3. Участники инфраструктуры открытых ключей	6
1.4. Использование регистрационных свидетельств.....	7
1.5. Управление документом	7
1.6. Термины, определения и сокращения	7
2. Ответственность за публикацию и хранилище	10
2.1. Хранилище	10
2.2. Публикация информации о регистрационных свидетельствах	10
2.3. Периодичность публикации	11
2.4. Контроль доступа к хранилищу	12
3. Идентификация и аутентификация.....	12
3.1. Требование к именам	12
3.2. Первоначальная проверка идентичности.....	13
4. Операционные требования к жизненному циклу регистрационных свидетельств	15
4.1. Заявления на выпуск регистрационных свидетельств.....	15
4.2. Обработка заявлений на выпуск регистрационных свидетельств	16
4.3. Выпуск регистрационных свидетельств	17
4.4. Принятие регистрационных свидетельств	18
4.5. Использование регистрационных свидетельств и ключевых пар	18
4.6. Обновление регистрационных свидетельств.....	20
4.7. Смена ключей регистрационных свидетельств.....	20
4.8. Изменение данных в регистрационных свидетельствах	20
4.9. Отзыв и приостановление действия регистрационных свидетельств....	21
5. Контроль объектов, управления и функционирования	23
5.1. Физический контроль.....	23
5.2. Процедурный контроль.....	25
5.3. Контроль персонала	27
5.4. Процедуры контрольного протоколирования	28
5.5. Ведение архива	29
5.6. Смена ключей УЦ.....	29
5.7. Восстановление после компрометации и происшествий	30
5.8. Прекращение работы удостоверяющего центра	32
6. Контроль технической безопасности	33
6.1. Генерация и установка ключевых пар.....	33
6.2. Защита закрытого ключа и инженерный контроль криптографического	



модуля	34
6.3. Другие особенности управления ключевыми парами	36
6.4. Данные активации	37
6.5. Контроль компьютерной безопасности.....	38
6.6. Технический контроль жизненного цикла.....	39
6.7. Средства управления сетевой безопасностью	39
6.8. Метки времени.....	39
7. Профили регистрационных свидетельств, COPC И OCSP	40
7.1. Профиль регистрационного свидетельства	40
7.2. Профиль COPC	40
7.3. Профиль OCSP	40
8. Проверка деятельности	41
9. Прочие коммерческие и юридические вопросы.....	42
9.1. Тарифы.....	42
9.2. Финансовая ответственность.....	42
9.3. Конфиденциальность коммерческой информации	43
9.4. Конфиденциальность персональных данных	43
9.5. Права интеллектуальной собственности.....	44
9.6. Гарантии и заверения	44
9.7. Отказ от гарантий	45
9.8. Ограничение ответственности	45
9.9. Компенсации	46
9.10. Вступление в силу и прекращение действия	46
9.11. Индивидуальные уведомления и связь с участниками.....	47
9.12. Изменения и дополнения	47
9.13. Положения о разрешении споров.....	48
9.14. Юрисдикция	48
9.15. Соответствие действующему законодательству.....	48
9.16. Прочие положения.....	48



1. Введение

1.1. Общие положения

1. Настоящий Регламент деятельности удостоверяющего центра акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан» (далее – Регламент) определяет деятельность Удостоверяющего центра и детализирует для участников, обслуживаемых акционерным обществом «Национальная платежная корпорация Национального Банка Республики Казахстан» (далее – Общество) информационных систем, Политику применения регистрационных свидетельств Удостоверяющего центра Общества (далее – Политика).

2. Регламент устанавливает нормы, реализуемые Удостоверяющим центром Общества (далее – УЦ) при обеспечении сервисов, которые определены Политикой и включают в себя, но не ограничиваются выпуском, управлением и отзывом регистрационных свидетельств.

3. Политика разработана в соответствии с законодательством Республики Казахстан:

- Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи»;
- Закон Республики Казахстан «О персональных данных и их защите»;
- Кодекс Республики Казахстан «Об административных правонарушениях»;

– Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 1 июня 2020 года № 224/НК «Правила выдачи и отзыва свидетельства об аккредитации удостоверяющих центров»;

– Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года №405/НК «Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре» (далее – Правила облачной ЭЦП);

– Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи»;

– Приказ Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 года № 1231 «Правила выдачи, хранения, отзыва регистрационных свидетельств, и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключением корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан» (далее – Правила выдачи и хранения);

– СТ Республики Казахстан 1073-2007 «Средства криптографической защиты информации. Общие технические требования».

4. Настоящий документ разработан в соответствии с рекомендациями (IETF) 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) для структуры Политики и Регламента.

5. Регламент раскрывает деятельность УЦ, обеспечивает реализацию Политики и детализирует порядок, в соответствии с которым УЦ:

- обеспечивает безопасность и управление ядром инфраструктуры обслуживаемых информационных систем;
- выпускает, управляет и отзывает для нее регистрационные свидетельства.

6. Регламент не является юридическим соглашением между Обществом и участниками обслуживаемых им информационных систем. Статус такого юридического соглашения приобретает в момент подписания участником заявления на выпуск регистрационного свидетельства (в любой форме: на бумажном, в электронном виде или в форме электронной заявки, сохраняемой в информационной системе Общества) или договора, содержащих ссылку на Политику и Регламент.

1.2. Наименование и идентификация документа

7. Наименование документа: «Регламент деятельности удостоверяющего центра акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан» (Certification Practice Statement)» согласно правовому акту по вопросам аккредитации удостоверяющих центров.

8. Редакция документа: 2.0

9. Объектный идентификатор - 1.2.398.3.5.1.2.

1.3. Участники инфраструктуры открытых ключей

10. Удостоверяющий центр – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства, выполняющее все свои функции в соответствии с Регламентом.

11. Центр регистрации (ЦР) – структурное подразделение удостоверяющего центра или действующее на основании договора с удостоверяющим центром юридическое лицо, ответственные за идентификацию заявителя, прием документов на выпуск или отзыв регистрационных свидетельств и предоставление заявителю готовых регистрационных свидетельств.

12. Доверяющая сторона (пользователи регистрационных свидетельств) – владельцы, или любые другие субъекты, которые действуют, полагаясь на регистрационные свидетельства, выпущенные УЦ, и/или электронные документы с электронными цифровыми подписями, подлинность которых проверяется с помощью этих регистрационных свидетельств.

13. Владелец регистрационного свидетельства (далее владелец) – физические или юридические лица, в лице уполномоченного представителя, на имя которого в УЦ выдано регистрационное свидетельство, правомерно



владеющий закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве. Вместе с тем, в роли владельца могут выступать технические средства, например, платежные терминалы, серверы и т.п., при этом в некоторых случаях под владельцем подразумевается юридическое или физическое лицо, которое правомерно владеет и пользуется данным техническим средством.

1.4. Использование регистрационных свидетельств

14. УЦ выпускает регистрационные свидетельства, различные по целям использования. Разрешенное использование, согласно профилю, отражается в расширениях «keyUsage» и/или «extendedKeyUsage» каждого регистрационного свидетельства.

15. По назначению открытых ключей, которые ими удостоверяются, все регистрационные свидетельства, выпускаемые УЦ, делятся на профили, полный перечень которых опубликован на информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz>.

16. По области допустимого применения регистрационные свидетельства могут быть разделены объектными идентификаторами, которые отражаются в расширении «certificatePolicies».

17. Наличие объектных идентификаторов дает информационным системам, использующим регистрационные свидетельства, возможность дополнительной защиты в форме контроля системой наборов обязательных и запрещенных политик с ограничением применения неподходящих регистрационных свидетельств.

18. Полный перечень объектных идентификаторов регистрационных свидетельств, назначенных УЦ, опубликован на официальном информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz>.

1.5. Управление документом

19. Ответственная организация – акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстан», расположенное по адресу: г. Алматы, микрорайон «Коктем-3», д. 21.

20. Контактное лицо – Начальник Управления удостоверяющего центра Общества. г.Алматы, микрорайон «Коктем-3», д. 21. Тел. +7 (727) 297-91-00, UUC@kisc.kz.

21. Публикация актуальной редакции Регламента или утвержденных уведомлений об изменениях и дополнениях к нему осуществляется на официальном информационном ресурсе Общества в сети Интернет по адресу: <https://npck.kz>. Их публикация по указанному адресу является официальным уведомлением заинтересованных участников.

1.6. Термины, определения и сокращения

22. В качестве основных определений использованы понятия, введенные международными стандартами и рекомендациями, в частности сериями Сектора стандартизации Международного союза электросвязи (International



Telecommunication Union Telecommunication Standardization Sector, ITU-T) и Специальной комиссии интернет-разработок (Internet Engineering Task Force, IETF).

23. В случаях, когда один или несколько схожих терминов имеют на практике несколько схожих определений, они приводятся в скобках со ссылкой на дополнительный источник.

24. В Регламенте используются следующие понятия и сокращения:

1) аутентификация – процесс проверки того, что лицо или предмет является тем, кем (чем) себя объявляет;

2) данные активации – любые данные, за исключением криптографических ключей, которые необходимы для функционирования криптографических модулей и требуют защиты (например, персональные идентификационные номера (PIN), парольные фразы или физически хранимые части ключа);

3) 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.

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

5) заявитель – физическое или юридическое лицо, подавшее документы на выпуск или отзыв регистрационного свидетельства;

6) идентификация – процесс проверки идентичности физического или юридического лица, показывающий, что данное лицо является конкретным вполне определенным лицом;

7) инфраструктура открытых ключей (ИОК) – набор средств (технических, материальных, людских и пр.), 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) ключевая пара и регистрационное свидетельство первичной инициализации – ключевая пара и регистрационное свидетельство с ограниченно коротким периодом действия, которые используются новым владельцем, успешно прошедшим процедуру первоначальной проверки идентичности, для самостоятельного формирования постоянной ключевой пары;

9) компрометация ключей – утрата владельцем ключей уверенности в том, что используемые криптографические ключи обеспечивают безопасность информации;



- 10) МСПД - межбанковская система перевода денег;
- 11) носитель ключевой информации – электронное устройство, которое может хранить электронные данные и содержит ключевую информацию (например: токен, дискета, CD-ROM, DVD-ROM, Смарт карты, Флэш карты, JaCarta, e-Token, USB Flash drive и другие);
- 12) Объектный идентификатор – упорядоченный список целочисленных значений от корня к узлу дерева международных объектных идентификаторов, который однозначно идентифицирует этот узел;
- 13) 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;
- 14) подписывающее лицо – физическое или юридическое лицо, правомерно владеющее закрытым ключом электронной цифровой подписи и обладающее правом на ее использование на электронном документе;
- 15) Политика применения регистрационных свидетельств – озаглавленный набор правил, которые определяют применимость регистрационного свидетельства в определенной общности и/или классе приложений с общими требованиями безопасности;
- 16) понятие «регистрационное свидетельство», определенный Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи», в контексте данного документа несет это же смысловое значение;
- 17) понятие «сертификат» используется международным стандартом ITU-T X.509 «Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks» (Информационная технология – Взаимодействие открытых систем – Справочник: структуры сертификатов открытых (криптографических) ключей и атрибутов);
- 18) регистрационное свидетельство - электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи»;
- 19) Регламент деятельности удостоверяющего центра – нормативный документ, определяющий порядок организации основной деятельности удостоверяющего центра, осуществляемой в соответствии с Политикой применения регистрационных свидетельств, включая течение основных процессов УЦ;
- 20) список отозванных регистрационных свидетельств (COPC) – часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва;
- 21) средства криптографической защиты информации (СКЗИ) – средства, реализующие алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами;



22) средства электронной цифровой подписи (средства ЭЦП) – совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи;

23) токен – физическое устройство, выдаваемое уполномоченному лицу в целях упрощения процедур аутентификации, а также организации защищенного хранения резервной копии закрытых ключей и настроек аппаратных криптографических модулей (Hardware Security Module, HSM) удостоверяющего центра;

24) ФАСТИ – финансовая автоматизированная система транспорта информации;

25) цепочка регистрационных свидетельств – упорядоченная последовательность регистрационных свидетельств, которая может быть обработана для получения открытого ключа последнего объекта цепочки от открытого ключа первого объекта цепочки;

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

27) электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи;

28) HSM (Hardware Security Module) - программно-аппаратный модуль, предназначенный для генерации, хранения, защиты секретных ключей УЦ и выполнения криптографической обработки данных УЦ;

29) HSM ES – специализированный программно-аппаратный модуль для криптографической обработки данных, работы с ключами пользователей и их надежного хранения.

2. Ответственность за публикацию и хранилище

2.1. Хранилище

25. Составной частью информационной системы УЦ является хранилище, которое используют напрямую обслуживаемые информационные системы в качестве справочника необходимой информации, а владельцы и пользователи регистрационных свидетельств (доверяющие стороны) – опосредованно, через используемые информационные системы.

2.2. Публикация информации о регистрационных свидетельствах

26. УЦ предоставляет владельцам и доверяющим сторонам информацию по адресам, где находятся соответствующее хранилище и служба онлайн протокола статуса сертификатов (OCSP).

27. На официальном информационном ресурсе Общества в сети Интернет размещаются актуальные версии Политики и Регламента.

28. Владельцам и доверяющим сторонам в хранилище доступны действующие (неотозванные) регистрационные свидетельства, а также действующие СОРС.



29. Регистрационные свидетельства публикуются в соответствии со следующей таблицей:

Тип регистрационного свидетельства	Требования по доступу
Регистрационные свидетельства УЦ	Доступны на официальном информационном ресурсе УЦ в сети Интернет по адресу https://npck.kz ; Доступны в хранилище УЦ по протоколу LDAP ¹ ; Доступны как часть цепочки регистрационных свидетельств, которая может быть получена вместе с регистрационным свидетельством владельца.
Регистрационные свидетельства сервиса OCSP	Доступны в хранилище УЦ по протоколу LDAP; Доступны как часть любой квитанции (ответа) сервиса OCSP.
Регистрационные свидетельства владельцев	Доступны в хранилище УЦ по протоколу LDAP.
Регистрационные свидетельства сервиса метки времени	Доступны в хранилище УЦ по протоколу LDAP. Доступны как часть любой квитанции (ответа) сервиса TSP.

2.3. Периодичность публикации

30. При выпуске нового регистрационного свидетельства, оно незамедлительно публикуется в хранилище.

31. Согласно расписанию планировщика информационной системы УЦ, не реже одного раза в сутки, производится проверка срока действия всех регистрационных свидетельств, опубликованных в хранилище. Регистрационные свидетельства с истекшим сроком действия удаляются из действующего хранилища.

32. В случае отзыва регистрационного свидетельства УЦ автоматически удаляет данное регистрационное свидетельство из действующего хранилища.

33. По окончании каждой операции по отзыву регистрационного свидетельства обновляется СОПС и незамедлительно публикуется в хранилище.

34. В случае отсутствия операций отзыва, СОПС обновляется на регулярной основе, не реже одного раза в неделю.

35. По истечению срока действия регистрационного свидетельства, оно исключается из СОПС.

¹ Адрес для обращения в хранилище УЦ по протоколу LDAP доводится владельцам и доверяющим сторонам по запросу после прохождения процедур первичной регистрации.



2.4. Контроль доступа к хранилищу

36. УЦ размещает в хранилище информацию, предназначенную для публичного доступа, только для чтения. При этом УЦ реализует меры безопасности, предотвращающие добавление, исключение или изменение данных в хранилище неавторизованными на то лицами.

37. УЦ не использует на постоянной основе средства ограничения чтения данных из хранилища. Ссылки на COPS, информация о том, по каким адресам необходимо обращаться в хранилище и к службе онлайн протокола статуса сертификатов (OCSP), доступны всем желающим на официальном информационном ресурсе Общества в сети Интернет.

38. В случаях кибератак, иных угроз перебоя в предоставлении сервисов или обоснованных подозрений в них УЦ оставляет за собой право применять временные ограничения доступа для чтения данных из хранилища в качестве активных мер противодействия.

3. Идентификация и аутентификация

3.1. Требование к именам

39. Имена, присутствующие в регистрационных свидетельствах УЦ, обеспечивают однозначную идентификацию владельцев во всех выпускаемых регистрационных свидетельствах.

40. Регистрационные свидетельства УЦ в полях «Issuer» и «Subject» содержат отличительное имя (DN-имя), соответствующее международным рекомендациям ITU-T X.520.

41. Содержание и атрибуты поля «Issuer» у всех регистрационных свидетельств, выпускаемых УЦ, одинаковы, их значения приведены на официальном информационном ресурсе Общества в сети Интернет по адресу: <https://npck.kz>.

42. Набор атрибутов поля «Subject» в регистрационных свидетельствах и правила их заполнения приведены на официальном информационном ресурсе НПК в сети Интернет по адресу: <https://npck.kz/>.

43. Поле «Subject» в регистрационных свидетельствах, выпускаемых УЦ, должно отражать данные, однозначно идентифицирующие владельца.

44. Однозначность идентификации достигается за счет использования идентификационных номеров из национальных реестров идентификационных номеров (индивидуальный идентификационный номер (ИИН) и бизнес-идентификационный номер (БИН)).

45. В случае отсутствия у физического лица ИИН, используется номер паспорта с указанием страны, при отсутствии паспорта – номер документа, заменяющего паспорт.

46. В случае отсутствия у юридического лица БИН, используется номер и реквизиты документа о регистрации плательщика НДС (VAT).

47. Если владельцем является техническое средство, например, сервер, поле «Subject» может отражать его полное доменное имя, если служба – название службы и т.п.



48. В рамках, установленных Регламентом, в состав имен помимо идентификационных номеров допускается включение фамилии, имени, отчества (при наличии), торговой марки, названия информационной системы, аббревиатуры организационно-правовой формы, названия организации и других общепринятых и понятных для человеческого восприятия имен и названий.

49. Анонимность владельцев не допускается.

50. Назначение псевдонима допускается только при условии документального закрепления исключительной принадлежности этого псевдонима владельцу. Например, псевдоним может быть назначен в рамках заключенного договора владельцем, центром регистрации или УЦ. При этом в любом случае псевдоним должен однозначно идентифицировать владельца.

51. Вследствие правового требования идентификации, имена всех владельцев являются уникальными. Выпуск и использование двух и более регистрационных свидетельств с одним и тем же DN-именем в поле «Subject» разрешается при условии, что соответствующими закрытыми ключами владеет и пользуется одно и то же физическое лицо или представитель юридического лица.

52. Заявители на выпуск регистрационного свидетельства не должны использовать в своих заявлениях имена, нарушающие права их законных правообладателей. УЦ не несет ответственности за проверку на предмет правообладания заявителем именем, указанным в заявлении. УЦ не обязан вступать в споры, связанные с собственностью на доменные, торговые и тому подобные имена и марки.

53. УЦ оставляет за собой право отклонить любое заявление на изготовление ключей и регистрационного свидетельства и/или регистрацию пользователя (далее – заявление на выпуск регистрационного свидетельства) или приостановить его рассмотрение, если подобное разбирательство является общеизвестным фактом.

3.2. Первоначальная проверка идентичности

54. Первоначальная проверка идентичности – это наиболее полная форма процедуры идентификации и аутентификации при выпуске регистрационного свидетельства, которая состоит из следующих этапов:

- проверка достоверности информации о заявителе, выполняемая центром регистрации или удостоверяющим центром;
- генерация ключевой пары владельца;
- доставка открытого ключа владельца в УЦ;
- доказательство удостоверяющему центру факта владения закрытым ключом, который соответствует открытому ключу, подлежащему удостоверению регистрационным свидетельством.

55. Первоначальная проверка идентичности проводится одним из двух способов:

- 1) при личной явке заявителя в центр регистрации или удостоверяющий центр;
- 2) дистанционно, средствами информационной системы.



56. Если достоверность информации о заявителе проверяется впервые или не может быть проверена и подтверждена на основе действующих регистрационных свидетельств, процедуры идентификации и аутентификации проводятся в форме первоначальной проверки идентичности.

57. В ходе первоначальной проверки идентичности заявитель демонстрирует УЦ, центру регистрации факт правомерного владения закрытым ключом, соответствующим открытому ключу, который будет указан в регистрационном свидетельстве.

58. Способом доказательства владения закрытым ключом может являться электронный документ в формате PKCS#10 или PKCS#7. Формат PKCS#10 используется только в случае, когда заявителем выступает потенциальный владелец, процедура первоначальной проверки идентичности проводится без участия центра регистрации, и регистрационное свидетельство выпускается без использования ключевой пары и регистрационного свидетельства первичной инициализации.


59. В остальных случаях используется формат PKCS#7 с ЭЦП, сформированной закрытым ключом, соответствующим действующему регистрационному свидетельству, например, закрытым ключом заявителя, центра регистрации или закрытым ключом первичной инициализации потенциального владельца. При этом в качестве подписываемых данных выступает запрос на изготовление регистрационного свидетельства в формате PKCS#10 с ЭЦП потенциального владельца.

60. Допускается, чтобы генерация ключевой пары владельца осуществлялась в УЦ при условиях, что такой способ выбирается при согласии заявителя, генерация осуществляется с обязательным использованием защищенного носителя ключевой информации, исключающего возможность доступа к закрытому ключу. В данном случае иных доказательств правомерного владения закрытым ключом не требуется.

61. Если заявителем на выпуск регистрационного свидетельства выступает юридическое лицо, его уполномоченным представителем в центр регистрации или удостоверяющий центр представляется заявление по соответствующей форме, размещенной на информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz>.

62. При наличии у заявителя, действующего регистрационного свидетельства заявление на выпуск нового регистрационного свидетельства, может быть подано в форме электронного документа. Сведения, содержащиеся в заявлении, подтверждаются ЭЦП заявителя, сформированной с использованием закрытого ключа, соответствующего действующему регистрационному свидетельству. При этом ответственность за полноту и достоверность сведений, указанных в заявлении, несет заявитель.

63. Дистанционно первоначальная проверка идентичности проводится в соответствии с Правилами облачной ЭЦП. В частности, проводится двухфакторная аутентификация заявителя, одним из факторов которой является биометрическая аутентификация.



64. Заявителем на выпуск регистрационного свидетельства – физическим лицом в УЦ, в центр регистрации представляется заявление по соответствующей форме, размещенной на информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz>.

65. Заявитель обязуется ознакомиться с Политикой и Регламентом. Подпись под заявлением на выпуск регистрационного свидетельства подтверждает согласие владельца нести обязательства и выполнять требования, предусмотренные Политикой и Регламентом.

66. В процессе рассмотрения заявлений на выпуск регистрационного свидетельства физическому лицу, уполномоченному представлять юридическое лицо, УЦ и центр регистрации действуют в соответствии с данным параграфом. Дополнительные проверки полномочий не проводится, они подтверждаются соответствующим заявлением и прилагаемыми к нему документами.

67. УЦ в порядке, установленном законодательством Республики Казахстан, проверяет сведения, указанные в заявлениях на выпуск регистрационного свидетельства. Для непрерывного использования регистрационных свидетельств перед истечением срока действия текущего регистрационного свидетельства владельцу необходимо выпустить новое регистрационное свидетельство. При этом владелец генерирует новую ключевую пару для замены истекающей.

68. Заявление на отзыв регистрационного свидетельства подаются по формам, размещенным на информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz>, для юридического или физического лица соответственно.

69. Заявление может быть подано в форме электронного документа, в этом случае оно должно быть удостоверено электронной цифровой подписью заявителя.

4. Операционные требования к жизненному циклу регистрационных свидетельств

4.1. Заявления на выпуск регистрационных свидетельств

70. Заявления на выпуск регистрационного свидетельства подаются в УЦ и центр регистрации.

71. Заявление на выпуск регистрационного свидетельства имеют право подавать:

- физические лица;
- уполномоченные представители юридических лиц.

72. Подача заявлений на выпуск регистрационного свидетельства, оформленных в форме документа на бумажном носителе, осуществляется только при личной явке заявителя.

73. В случае дистанционного обращения заявителя за выпуском регистрационного свидетельства вместо документа на бумажном носителе в информационной системе Общества, для которой запрашивается выпуск регистрационного свидетельства, сохраняется электронная заявка заявителя,



содержащая полный набор данных и обязательств заявителя, установленный Правилами выдачи и хранения.

74. В обоих случаях заявление или электронная заявка на выпуск регистрационного свидетельства является обязательством заявителя соблюдать принципы и выполнять требования Политики и Регламента в части, касающейся владельца и пользователя регистрационных свидетельств (доверяющей стороны).

75. В случаях дистанционного обращения заявителя за выпуском регистрационного свидетельства и создания закрытых ключей в облачной ЭЦП в порядке, определенном параграфом 4.2, регистрационные свидетельства выпускаются УЦ без оформления и предоставления заявлений на выпуск и сопутствующих документов, определенных Правилами выдачи и хранения.

4.2. Обработка заявлений на выпуск регистрационных свидетельств

76. Заявления и электронные заявки на выпуск регистрационного свидетельства обрабатываются в соответствии с Правилам выдачи и хранения с учетом требований Правил облачной ЭЦП, в применимых случаях.

77. Перед регистрацией заявления (сохранением электронной заявки) на выпуск регистрационного свидетельства проводится идентификация и аутентификация заявителя.

78. В случае, если заявитель при подаче заявления в установленный срок (электронной заявки – в режиме онлайн) не прошел успешно процедуру идентификации и аутентификации, т.е. не предоставил документальных доказательств достоверности информации, указанной в заявлении (электронной заявке) на выпуск регистрационного свидетельства, такое заявление (электронная заявка) не регистрируется.

79. УЦ или центр регистрации отклоняет заявление на выпуск регистрационного свидетельства, если:

- 1) заявитель не представил всю необходимую информацию в соответствии с Правилам выдачи и хранения;
- 2) заявитель представил недостоверную информацию;
- 3) заявитель не прошел процедуру идентификации и аутентификации;
- 4) УЦ или центру регистрации известно о решении суда, запрещающем выдачу регистрационного свидетельства на имя потенциального владельца;
- 5) потенциальный владелец не достиг возраста шестнадцати лет;
- 6) средство электронной цифровой подписи, предлагаемое к использованию заявителем, не поддерживается УЦ;
- 7) в иных случаях, установленных законодательством Республики Казахстан по вопросам электронного документа и электронной цифровой подписи.

80. УЦ оставляет за собой право отказать в выпуске регистрационного свидетельства без детального разъяснения причин, в случае выявления каких-либо факторов, которые могут нанести вред его деловой репутации.

81. В случае изменения, определенного законодательством Республики Казахстан перечня оснований для отказа в выдаче регистрационного



свидетельства, применяются требования законодательства Республики Казахстан. Регламент подлежит приведению в соответствие с законодательством в установленном порядке

82. Заявления на выпуск регистрационного свидетельства рассматриваются УЦ и центрами регистрации в срок не более 5 (пяти) рабочих дней с момента их поступления.

4.3. Выпуск регистрационных свидетельств

83. Каждое регистрационное свидетельство создается и выпускается по факту успешного завершения следующих шагов:

1) идентификация личности заявителя, а также, если требуется, проверка его полномочий представлять юридическое лицо, в соответствии с Правилам выдачи и хранения;

2) защищенная генерация ключевой пары владельца в центре регистрации или, в случае дистанционного обращения владельца, непосредственно у владельца или в УЦ;

3) защищенная доставка открытого ключа владельца из центра регистрации в УЦ, в случае личной явки заявителя в центр регистрации;

4) проверка УЦ факта владения закрытым ключом, соответствующим открытому ключу, который подлежит регистрации УЦ, в случае личной явки заявителя в центр регистрации.

84. Каждое регистрационное свидетельство создается УЦ либо по факту регистрации отдельного заявления на выпуск регистрационного свидетельства в центре регистрации, либо по факту сохранения электронной заявки на выпуск регистрационного свидетельства.

85. Защита ключевой пары при ее генерации на стороне владельца и центра регистрации достигается за счет использования защищенного носителя ключевой информации, а на стороне УЦ - аппаратных криптографических модулей (HSM).

86. Если закрытые ключи владельца генерируются в центре регистрации, то эта процедура как правило выполняется непосредственно на защищенном носителе ключевой информации, который исключает возможность их копирования. По окончании процедуры выпуска регистрационного свидетельства защищенный ключевой носитель, содержащий закрытые ключи и регистрационные свидетельства УЦ, работник центра регистрации вручает заявителю лично.

87. В исключительных случаях, когда отсутствует техническая возможность использовать технологический закрытый ключ информационной системы УЦ непосредственно с защищенного носителя ключевой информации, такой закрытый технологический закрытый ключ допускается после генерации сохранять на произвольный носитель ключевой информации с обязательным использованием данных активации.

88. Если закрытые ключи владельца генерируются в УЦ, то эта процедура выполняется в HSM УЦ в соответствии с Правилами облачной ЭЦП.



89. Способы получения своих регистрационных свидетельств являются сообщения электронной почты, содержащие соответствующие регистрационные свидетельства, либо загрузка регистрационных свидетельств из хранилища УЦ через сеть Интернет.

90. По усмотрению владельца регистрационное свидетельство может быть передано из рук в руки лично ему или уполномоченному им представителю при личной явке в Общество.

4.4. Принятие регистрационных свидетельств

91. После выпуска регистрационного свидетельства всем владельцам предоставляется право в течение 5 (пяти) календарных дней с даты выпуска, заявить УЦ об отказе от намерения иметь это регистрационное свидетельство или о несогласии с его содержанием.

92. Для реализации указанного права заявителю необходимо обратиться в центр регистрации заявлением об отзыве регистрационного свидетельства на бумажном носителе или в форме электронного документа.

93. Если владелец не использует указанное право, то регистрационное свидетельство автоматически считается принятым владельцем.

94. Если владелец, не заявляя о своем отказе от намерения иметь регистрационное свидетельство или о несогласии с его содержанием, до истечения предоставляемого УЦ пятидневного срока, то регистрационное свидетельство автоматически считается принятым владельцем.

4.5. Использование регистрационных свидетельств и ключевых пар

95. Использование закрытого ключа разрешается только при соблюдении следующих условий:

1) владелец дал обязательство выполнять требования Политики и Регламента;

2) УЦ в порядке, установленном законодательством Республики Казахстан, выпустил регистрационное свидетельство соответствующего открытого ключа;

3) владелец принял это регистрационное свидетельство.

96. Регистрационное свидетельство должно использоваться только в соответствии с законодательством, Политикой и Регламентом. Использование регистрационного свидетельства должно соответствовать содержанию расширений «keyUsage» и «extendedKeyUsage».

97. Владельцы обязаны защищать свой закрытый ключ от несанкционированного доступа, в ином случае рекомендуется прекращать его использование после истечения срока действия или отзыва соответствующего регистрационного свидетельства.

98. Необходимым условием доверия к регистрационным свидетельствам, выпущенным УЦ, для доверяющих сторон является принятие обязательств о выполнении требований Политики и Регламента.

99. Прежде, чем предпринять любой акт, основываясь на доверии к регистрационному свидетельству, выпущенному УЦ, доверяющие стороны



должны самостоятельно проверить каждый соответствующий электронный документ, в частности, каждую имеющуюся на нем ЭЦП, а также связанные с этим регистрационные свидетельства, метки времени, квитанции (ответы) службы OCSP или COPS. Для проведения данной проверки доверяющей стороне следует:

1) определить и проверить цепочку регистрационных свидетельств, которая позволяет установить субъекта, сформировавшего ЭЦП. В ходе проверки цепочки регистрационных свидетельств используется алгоритм, изложенный в рекомендациях RFC 3280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile» (Профиль регистрационного свидетельства и COPS интернет-инфраструктуры открытых ключей формата X.509);

2) в ходе проверки каждого регистрационного свидетельства цепочки дополнительно контролировать содержание расширений «keyUsage» и «extendedKeyUsage» на соответствие цели использования;

3) самостоятельно проверять наличие у подписавшего лица полномочий, достаточных для подписания электронного документа. Информационная система УЦ сервисов контроля полномочий владельца не предоставляет.

100. Если любой шаг проверки дает отрицательный результат или его невозможно выполнить, то ЭЦП полагается недействительной, и электронный документ отвергается.

101. Если в электронном документе имеется отметка времени, сформированная УЦ, то для выполнения действия, требующего доверия к отметке времени, необходимо также проверить эту отметку времени в порядке, аналогичном проверке ЭЦП в электронном документе.

102. Если любое из регистрационных свидетельств цепочки на момент проверки ЭЦП имеет статус «отозвано», только доверяющая сторона исключительно на свой риск решает, оправдано или нет полагаться на электронный документ, сформированный владельцем до отзыва одного из регистрационных свидетельств цепочки. УЦ в случаях такого рода не несет ответственности перед пользователями регистрационных свидетельств (доверяющими сторонами), так как подача заявления на отзыв регистрационного свидетельства является обязанностью конкретного владельца.

103. Если обстоятельства указывают на необходимости дополнительных гарантий со стороны авторов электронного документа, то пользователь регистрационного свидетельства (доверяющая сторона) получает такие дополнительные гарантии от владельцев самостоятельно, до выполнения действий, требующих доверия к регистрационному свидетельству, и без обращения в УЦ.

104. Если пользователь регистрационного свидетельства (доверяющая сторона), предпринимая любой акт, основанный на доверии к регистрационному свидетельству, выпущенному УЦ, не выполнил вышеперечисленные условия параграфа 4.5 Регламента, то УЦ не несет перед доверяющей стороной ответственности за последствия такого акта.



105. Закрытый ключ используется владельцем только после того, как он дал обязательство выполнять обязанности владельца и доверяющей стороны в соответствии с параграфом 4.1 Регламента, УЦ выпустил регистрационное свидетельство соответствующего открытого ключа, и владелец принял это регистрационное свидетельство.

106. Закрытый ключ используется владельцем только в соответствии с законодательством Республики Казахстан, договорными обязательствами, Политикой и Регламентом.

107. Использование закрытого ключа должно соответствовать содержанию расширений «keyUsage» и «extendedKeyUsage». Например, если в содержании указанных расширений отсутствует значение «Цифровая подпись», то регистрационное свидетельство не должно использоваться в целях проверки ЭЦП.

4.6. Обновление регистрационных свидетельств

108. УЦ не предоставляет услуг по обновлению регистрационных свидетельств.

109. При необходимости использования регистрационных свидетельств УЦ, владелец повторно проходит процедуру выпуска регистрационных свидетельств, в порядке, определенном параграфами 4.1, 4.2 и 4.3 Регламента.

4.7. Смена ключей регистрационных свидетельств

110. УЦ не предоставляет услуг по смене криптографических ключей регистрационных свидетельств.

111. При необходимости смены ключей центры регистрации и владельцы имеют возможность инициировать выпуск нового регистрационного свидетельства в соответствии с параграфами 4.1, 4.2 и 4.3 Регламента.

112. Если эта необходимость вызвана компрометацией закрытого ключа, то центр регистрации и владелец обязан в первую очередь инициировать отзыв регистрационного свидетельства, соответствующего скомпрометированному закрытому ключу.

4.8. Изменение данных в регистрационных свидетельствах

113. УЦ не предоставляет услуг по изменению данных в регистрационных свидетельствах.

114. Для изменения данных в регистрационных свидетельствах УЦ, владелец повторно проходит процедуру выпуска новых регистрационных свидетельств, в порядке, определенном параграфами 4.1, 4.2 и 4.3 Регламента.

115. При этом, центр регистрации и владелец обязаны в первую очередь инициировать отзыв регистрационного свидетельства, а затем подать заявление на выпуск нового.



4.9. Отзыв и приостановление действия регистрационных свидетельств

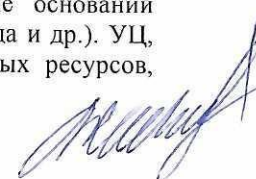
116. Регистрационное свидетельство владельца отзывается уполномоченными сотрудниками УЦ и публикуется в СОРС в следующих случаях:

- 1) поступило содержащее причину отзыва заявление центра регистрации или владельца, который больше не использует (или не желает использовать) регистрационное свидетельство;
- 2) в случае смерти владельца;
- 3) смены наименования, реорганизации, ликвидации юридического лица – владельца, смены руководителя юридического лица;
- 4) изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца;
- 5) по вступившему в законную силу решению суда;
- 6) при установлении факта представления недостоверных сведений либо неполного пакета документов при получении регистрационного свидетельства;
- 7) иные причины, предусмотренные Политикой и Регламентом²:
 - наличие доказательства того, что регистрационное свидетельство было выпущено с нарушением процедур Правил выдачи и хранения, Политики и Регламента, выпуска регистрационного свидетельства неидентифицированному или лицу, идентифицированному ошибочно;
 - наличие доказательств ошибочности сведений из заявления на выпуск регистрационного свидетельства;
 - владелец или центр регистрации не произвел должную оплату;
 - УЦ, центр регистрации или владелец располагает доказательствами компрометации закрытого ключа или обоснованных подозрений такой компрометации. (согласно Политики и Регламенту, УЦ рекомендует владельцу незамедлительного информирования об обнаружении или обоснованном подозрении в компрометации закрытого ключа)
 - УЦ или центр регистрации располагают доказательствами существенного нарушения владельцем обязательства, заверения или гарантии действующего договора;
 - продолжение использования регистрационного свидетельства опасно для информационных систем.

117. УЦ, владелец или центр регистрации при определении опасности использования регистрационного свидетельства для информационных систем среди прочего рассматривают:

- количество и характер полученных жалоб;
- идентичность лиц, подавших жалобы;

² Согласно пункту 28 Правил выдачи и хранения Удостоверяющий центр вправе производить отзыв регистрационного свидетельства без заявления от заявителя при наступлении одного из случаев, за исключением подпункта 1). Однако, в случаях, перечисленных в подпунктах 2)-5) пункта 28, основанием для отзыва служит письменное заявление на отзыв регистрационного свидетельства (на бумажном носителе) с предъявлением оригинала официального документа уполномоченной инстанции, подтверждающего наличие оснований (например, свидетельство о смерти, справка о перерегистрации юридического лица, решение суда и др.). УЦ, центры регистрации и уполномоченные посредники не проводят мониторинг информационных ресурсов, содержащих сведения соответствующего рода.



– иные возможные меры по исключению опасности со стороны владельца.

118. Регистрационные свидетельства могут отзываться по иным основаниям, установленным законодательством Республики Казахстан.

119. Отзыв осуществляется по заявлению владельца или центра регистрации, оформленному в виде документа на бумажном носителе или электронного документа.

120. Подавать заявления на отзыв регистрационных свидетельств имеют право владельцы или центры регистрации, а также их должным образом уполномоченные представители. Запрашивать отзыв регистрационных свидетельств также могут уполномоченные работники УЦ.

121. Инициатор отзыва регистрационного свидетельства представляет в УЦ, в центр регистрации, владельцу заявление по соответствующей форме, размещенной на информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz> (для физических или юридических лиц соответственно). Заявление об отзыве может подаваться в форме электронного документа.

122. Перед отзывом регистрационного свидетельства владельца УЦ, центр регистрации или владелец проверяют, что инициатор запрашивает отзыв правомочно. При этом могут применяться все механизмы идентификации и аутентификации, которые приведены в параграфе 3.2 Регламента.

123. Процедура отзыва регистрационного свидетельства осуществляется в соответствии с Правилами выдачи и хранения. В случае обоснованности заявления, регистрационное свидетельство отзывается не позднее рабочего дня, следующего за датой поступления заявления (электронной заявки) на отзыв регистрационного свидетельства.

124. Заявления на отзыв регистрационного свидетельства рассматриваются УЦ незамедлительно, не позднее рабочего дня, следующего за датой поступления заявления.

125. УЦ для проверки доверяющими сторонами статуса регистрационных свидетельств обеспечивает их информацией о том, как найти соответствующий COPS, интерфейс хранилища и службу OCSP

126. COPS являются едиными, в том смысле, что они содержат, при их наличии, отозванные регистрационные свидетельства служб и серверов УЦ, в том числе службы OCSP и сервера метки времени, а также отозванные регистрационные свидетельства владельцев.

127. Если доверяющая сторона не проверяет статус регистрационных свидетельств с помощью опубликованного действующего COPS, она должна проверять статус регистрационных свидетельств, запрашивая службу OCSP или обращаясь в хранилище УЦ.

128. Действующий COPS и служба OCSP УЦ, дающие возможность доверяющим сторонам в режиме онлайн получать информацию об отзыве и иных статусах регистрационных свидетельств, доступны публично. УЦ обеспечивает доверяющие стороны информацией о том, как найти действующий COPS и службу OCSP. В дополнение к этому, информация о статусе регистрационных



свидетельств может быть получена доверяющими сторонами из хранилища по протоколу LDAP.

129. Информация о статусе регистрационных свидетельств доступна через СОРС, в хранилище по протоколу LDAP или на официальном информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz>, а также через службу OCSP.

130. Сервисы статуса регистрационных свидетельств УЦ доступны круглосуточно и непрерывно, за исключением времени плановых и профилактических работ.

131. Участники информационных систем, обслуживаемых УЦ, извещаются о компрометации или подозрении в компрометации закрытых ключей УЦ любыми целесообразными способами.

132. В случае обоснованного подозрения о компрометации закрытого ключа владелец и соответствующего регистрационного свидетельства обязаны немедленно отозвать регистрационное свидетельство.

133. Владелец, используемого в информационных системах Общества, кроме того, обязан в случае компрометации закрытых ключей или увольнения работника, имевшего доступ к закрытым ключам, отозвать соответствующие этим ключам регистрационные свидетельства и для их замены запросить выпуск новых регистрационных свидетельств. Новые ключевые пары и регистрационные свидетельства должны быть введены в действие незамедлительно, в случае увольнения работника – не позднее дня увольнения.

134. Владелец может прекратить обслуживание в УЦ:

- расторгнув действующий договор;
- отзывая регистрационное свидетельство до окончания срока его действия.

135. Услуги по временной приостановке и возобновлению действия регистрационного свидетельства УЦ не предоставляет.

136. Услуги по депонированию и восстановлению закрытого ключа владельца УЦ не предоставляет.

5. Контроль объектов, управления и функционирования

5.1. Физический контроль

137. Детальные меры физического контроля и безопасности, реализуемые в УЦ, документально утверждены. Эти документы содержат конфиденциальную информацию Общества и не публикуются. Общий обзор этих мер приведен в данной главе.

138. Общество подвергало и планирует далее регулярно подвергать выполнение этих мер независимому аудиту в соответствии с параграфом 8 Регламента.

139. Информационная система УЦ обеспечена несколькими дата-центрами (основной и резервный), расположенными на разных объектах в целях резервирования и восстановления функционирования в случае чрезвычайной ситуации.



140. Условия размещения оборудования УЦ в основном и резервном дата-центрах выбраны с учетом, действующим в Республике Казахстан требований к системам бесперебойного функционирования технических средств и информационной безопасности³.

141. Для обеспечения безопасности УЦ проводятся организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также обеспечения информационной безопасности, установлены и действуют соответствующие правила и инструкции для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

142. Защита информации от несанкционированного доступа осуществляется на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении регламентных и ремонтных работ.

143. Системы УЦ защищены минимум тремя уровнями физической безопасности, доступ на вышестоящие уровни невозможен без корректного прохождения нижестоящих.

144. Доступ на каждый уровень контролируется в соответствии с прогрессивной ограничительной шкалой привилегий физического доступа. Важные эксплуатационные процедуры УЦ, в том числе любые процедуры, связанные с жизненным циклом регистрационных свидетельств, такие как аутентификация, проверки, выпуск, выполняются на верхнем уровне безопасности. Для доступа на каждый уровень необходимо использовать бесконтактную карту работника. Физический доступ автоматически протоколируется и контролируется видеозаписью. Передвижение по контролируемой территории УЦ посетителей и работников, не имеющих на то соответствующих полномочий, запрещено.

145. Система физической безопасности имеет в своем составе дополнительные уровни для безопасного управления ключами, которые защищают криптографические устройства, в том числе онлайн, а также ключевой материал. Онлайн криптографические устройства используются в помещениях с ограниченным доступом, остальные хранятся в сейфах, контейнерах и хранилищах. Открытие и закрытие помещений и контейнеров на этих уровнях протоколируется в контрольных целях. Доступ к криптографическим устройствам и ключевому материалу ограничен требованиями разделения обязанностей.

146. Деятельность УЦ ведется в физически защищенных условиях, которые сдерживают, предотвращают и выявляют несанкционированное использование, доступ, раскрытие конфиденциальной информации и систем. УЦ также имеет возможности (запасной объект) для восстановления на случай

³ На дату утверждения Постановление Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах. Зарегистрировано в Реестре государственной регистрации нормативных правовых актов Республики Казахстан 18 апреля 2018 года под № 16772



чрезвычайных ситуаций. Запасной объект имеет многоуровневую систему физической безопасности, как и основной.

147. УЦ, имея безопасный внешний запасной объект, поддерживает резервное хранение и электропитание критических системных данных и любой другой конфиденциальной информации, включающей данные контроля.

148. Все носители производственного программного обеспечения и данных, протоколов и резервных копий хранятся на защищенных объектах с надлежащим уровнем физического и логического контроля доступа, предусматривающего доступ ответственного персонала и защиту от случайного повреждения (вследствие пожара, наводнения или электромагнитного излучения и т.п.).

149. УЦ выполняет резервное копирование важных системных данных, контрольных протоколов и другой конфиденциальной информации. Носители резервных копий хранятся на запасном объекте и защищаются физически.

150. Помещения дата-центров оснащены системами:

- охранной сигнализации;
- контроля и управления доступом;
- видеонаблюдения;
- гарантированного электропитания;
- электрического заземления;
- микроклимата;
- пожарной сигнализации;
- газового автоматического пожаротушения.

5.2. Процедурный контроль

151. Работники, которым поручается управлять инфраструктурой безопасности, рассматриваются как «ответственный персонал», обслуживающий «ответственные участки». Соискатели на роль ответственного персонала (назначения на ответственный участок) в соответствии с Политикой должны соответствовать утвержденным типовым квалификационным требованиям к должностям работников Общества.

152. К разряду ответственного персонала относятся работники Общества, имеющие доступ или контролирующую аутентификацию и криптографические операции, которые могут существенно влиять на:

- проверку информации из заявлений на выпуск регистрационных свидетельств;
- прием, отказ в приеме или иную обработку заявлений на выпуск или отзыв регистрационных свидетельств;
- выпуск или отзыв регистрационных свидетельств.

153. Ответственный персонал, включает в себя, но не ограничивается:

- персоналом обслуживания клиентов;
- персоналом, выполняющим криптографические операции;
- персоналом управления информационной безопасностью;
- персоналом системного администрирования;



- инженерным персоналом;
- управляющими инфраструктуры безопасности.

154. Перечисленные категории работников Общества считаются ответственным персоналом, занимающим ответственные участки. Претенденты на должности, относящиеся к разряду ответственного персонала, то есть на работу на ответственном участке, обязаны предоставить документы, определенные Трудовым Кодексом Республики Казахстан.

155. В УЦ установлены, поддерживаются и обеспечиваются строгие процедуры контроля, гарантирующие разделение и ответственное исполнение обязанностей, выполнение наиболее важных задач несколькими ответственными лицами.

156. К числу наиболее важных задач, требующих выполнения несколькими лицами, относятся доступ и управление криптографическими устройствами и их ключевым материалом.

157. Процедуры внутреннего контроля построены так, что как минимум двое работников из числа ответственного персонала требуются для физического или логического доступа к устройству. Доступ к криптографической аппаратуре в течение всего ее жизненного цикла, от входной проверки и приемки до окончательного логического и/или физического уничтожения, осуществляется строго несколькими ответственными лицами одновременно. С момента ввода в модуль действующих ключей осуществляется дополнительный контроль для разделения физического и логического доступа к устройству. Лица, имеющие физический доступ к модулям, не хранят «частей секрета» и наоборот.

158. Ввод и проверка данных, необходимых для выпуска регистрационного свидетельства, осуществляются одним или более чем одним ответственным работником УЦ, центра регистрации или заявителя с применением средств автоматизации проверки.

159. Генерация регистрационных свидетельств на основе введенных данных представляет собой автоматизированный процесс, включающий проверку полномочий инициатора.

160. Для всех работников Общества, претендующих на должности, входящие в разряд ответственного персонала, проводится процедура идентификации, в ходе которой при личном (физическом) присутствии претендента ответственный персонал кадровой службы или службы безопасности проверяет документы, удостоверяющие личность.

161. После решения ответственного руководителя о зачислении работника в разряд ответственного персонала, ему выдается персональное устройство и права доступа на соответствующие объекты, а также электронные средства для доступа и выполнения специализированных функций в информационных системах УЦ.

162. Функции, требующие разделения обязанностей, включают в себя, но не ограничиваются:

- администрированием операционных систем серверов УЦ;
- администрированием криптографических модулей;



- администрированием прикладного программного обеспечения на серверах УЦ;
- администрированием web-модулей интерфейса клиентов УЦ;
- администрированием базы данных клиентов УЦ;
- установкой, монтажом, пуско-наладкой основного оборудования.

5.3. Контроль персонала

163. Претендент на должность, входящую в разряд ответственного персонала, в соответствии с Трудовым Кодексом Республики Казахстан обязан подтвердить наличие базовой подготовки и образования предъявлением документа об образовании, квалификации, наличии специальных знаний или профессиональной подготовки, а наличие практического опыта – предъявлением документа, подтверждающего трудовой стаж.

164. Ограничений на частоту и последовательность перемещений работников УЦ по службе не накладывается, за исключением квалификационных требований к должностям в УЦ.

165. Работники и руководители УЦ повышают свою квалификацию путем прохождения обучения или сертификации в определенном наборе тем. Тематика обучения ежегодно согласовывается менеджментом Общества на предмет соответствия функциям персонала и актуальности.

166. Общество обеспечивает свой персонал необходимым обучением и документацией, необходимой для компетентного и удовлетворительного исполнения обязанностей.

167. Ответственность работников УЦ за несанкционированный доступ к служебной информации и иные нарушения требований информационной безопасности предусмотрена трудовым договором и должностными инструкциями.

168. В случае обнаружения несанкционированного доступа или подозрения о нем, системный администратор вместе с сотрудником безопасности могут приостановить доступ к системам со стороны нарушителя (подозреваемого). Дальнейшие дисциплинарные санкции определяются руководством Общества.

169. Все функции и работы УЦ выполняются силами штатных специалистов. Допускается привлечение контрагентов в рамках договоров поставки и технической поддержки аппаратного и программного обеспечения информационной системы УЦ. Привлечение внештатных сотрудников (в форме не трудовых договоров, а договоров гражданско-правового характера) к выполнению функций и работ УЦ не предусмотрено.

170. Для оказания услуг технической поддержки контрагентами, все работы на защищенных объектах, допускается только в сопровождении и под постоянным контролем ответственного персонала, согласно списку специалистов контрагента, предварительно согласованному с менеджментом Общества.



5.4. Процедуры контрольного протоколирования

171. УЦ в обязательном порядке регистрирует все события в контрольных протоколах информационной системы УЦ.

172. Структура записи контрольного протокола, включает в себя следующие элементы:

- дата и время записи;
- порядковый номер записи;
- идентичность сущности, вызвавшей запись;
- тип события;
- источник записи.

173. Структура записи событий в конкретном протоколе соответствует эксплуатационной документации программного обеспечения целевых функций УЦ и общесистемного программного обеспечения. В случае отсутствия в протоколе какой-либо из перечисленных категорий информации, связанные с этим риски минимизируются другими техническими или организационными мерами.

174. УЦ регистрирует следующие события или данные:

- события, связанные с жизненным циклом ключей УЦ, включая, но не ограничиваясь их генерацией, восстановлением и уничтожением, а также созданием, хранением и уничтожением их резервных копий;
- события, связанные с жизненным циклом регистрационных свидетельств, включая, но не ограничиваясь получением запросов на выпуск и изменение статуса регистрационных свидетельств, генерацией и изменением статуса регистрационных свидетельств, генерацией и выпуском СОРС;
- события, связанные с жизненным циклом программных аппаратных комплексов HSM, включая, но не ограничиваясь их получением, вводом в эксплуатацию, использованием, сервисным обслуживанием, ремонтом, выводом из эксплуатации и уничтожением;
- данные, связанные с заявлениями на выпуск регистрационных свидетельств, включая вид и номер документа, идентифицирующего заявителя, данные должностного лица УЦ, проверившего и подтвердившего данные заявлений, дата и время обработки;
- иные важные с точки зрения безопасности события, включая, но не ограничиваясь сеансами администрирования систем УЦ (дата, время, цели, в том числе, изменение профилей, доступ к контрольным протоколам и т.п.), инцидентами (сбой систем, отказы аппаратного обеспечения и другие аномалии).

175. Ключи и данные активации не записываются в автоматические контрольные протоколы в явном виде.

176. УЦ также осуществляет систематизацию и хранение материалов заявлений на выпуск и отзыв регистрационных свидетельств, включая доверенности, уполномочивающие представителей юридических лиц, и другие материалы.

177. Контрольные протоколы систем УЦ ведутся в Обществе непрерывно, подлежат ежесуточному резервному копированию, ежемесячному



архивированию и сдаче в архив в соответствии с параграфом 5.5 Регламента, где хранятся в течение регламентированного срока.

178. Протоколы событий, сервиса облачной ЭЦП для хранения закрытых ключей пользователей в УЦ, ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Используемый для этого блокчейн доступен в сети Интернет.

179. Перед записью на машинный носитель архивная копия контрольных протоколов зашифровывается и снабжается кодом аутентификации.

5.5. Ведение архива

180. УЦ ведет архив:

- контрольных протоколов в соответствии с параграфом 5.4 Регламента;
- регистрационных свидетельств, включая отозванные регистрационные свидетельства и регистрационные свидетельства с истекшим сроком действия;
- информации о жизненном цикле регистрационных свидетельств, включая заявления об их отзыве и СОРС;
- запросы на выпуск и отзыв регистрационных свидетельств в формате PKCS#7;
- СОРС.

181. Записи контрольных протоколов должны иметь отметку о дате и времени. Регистрационные свидетельства, заявки и запросы на их выпуск и изменение статуса, СОРС имеют отметки о дате и времени создания, заверенные электронной цифровой подписью.

182. Доступ к архиву имеет только ответственный персонал УЦ. Проверка архивной информации регламентирована и проводится путем пробного восстановления в соответствии параграфом 5.7 Регламента.

183. Хранение и резервное копирование носителей архивной информации осуществляется в соответствии с внутренним нормативными документом Общества.

184. Утилизация носителей архивной информации осуществляется в соответствии с внутренним нормативными документом Общества.

5.6. Смена ключей УЦ

185. Ключевые пары УЦ имеют срок действия. По окончании срока их действия закрытые ключи и их резервные копии уничтожаются по акту комиссией.

186. Новые ключи удостоверяющего центра генерируются либо на замену истекающим, либо в дополнение к действующим в целях обеспечения ввода в эксплуатацию новых сервисов.



187. Смена ключей осуществляется заблаговременно до истечения срока их действия, в соответствии с внутренним документом Общества⁴.

188. Для обеспечения плавности перехода владельцев со старой ключевой пары УЦ на новую, процедура смены ключей УЦ состоит в следующем:

- УЦ с определенного момента, не позднее, чем за 1 (один) год до истечения срока действия регистрационного свидетельства УЦ, прекращает выпускать регистрационные свидетельства владельцев, подписанные закрытым ключом, который соответствует данному регистрационному свидетельству УЦ;

- с указанного момента по положительно рассмотренным заявлениям владельцев выпускаются регистрационные свидетельства, подписанные новой ключевой парой УЦ.

- при этом УЦ продолжает подписывать СОРС ключом, срок действия которого завершается, вплоть до того момента, когда истечет срок действия последнего регистрационного свидетельства, подписанного с его помощью.

189. Сформированные новые регистрационные свидетельства доводятся до сведения доверяющих сторон путем публикации в хранилище.

5.7. Восстановление после компрометации и происшествий

190. Общество, на случай чрезвычайных происшествий, связанных с природным или человеческим фактором, имеет безопасный внешний запасной объект (резервный дата-центр). Внешний запасной объект имеет уровень физической защиты, эквивалентный основному объекту.

191. Оборудование УЦ в дата-центрах (основной и резервный) обеспечивается резервированным подключением к сети с использованием нескольких каналов.

192. В Обществе разработан, утвержден и прошел учебную проверку детальный план восстановления функционирования деятельности УЦ, нацеленный на смягчение последствий каких-либо природных или техногенных бедствий. План восстановления функционирования регулярно рассматривается с целью актуализации.

193. План восстановления функционирования предназначен для возобновления сервисов информационных систем и ключевых бизнес-функций. Резервный дата-центр Общества защищен физически и контролируется в эксплуатационном плане в соответствии с утвержденными нормативными документами в целях обеспечения безопасного и надежного резервирования работы.

194. Общество обеспечено запасным оборудованием и резервными копиями программного обеспечения систем своего УЦ на резервном дата-центре. Для восстановления функционирования в соответствии с параграфом 6.2 Регламента созданы и хранятся резервные копии закрытых ключей УЦ.

195. Резервная и основная базы данных регулярно синхронизируются с определенной частотой. Принципы физической защиты резервного

⁴ На дату публикации «Правила обращения с программно-аппаратными модулями HSM удостоверяющего центра акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан»



оборудования аналогичны по уровню принципам, приведенным в параграфе 5.1 Регламента.

196. Резервная копия следующих данных создается и хранится на безопасном внешнем запасном объекте:

- заявки на выпуск, отзыв и изменение статуса;
- запросы на выпуск и отзыв регистрационных свидетельств;
- контрольные протоколы ИС и ОС;
- базы всех выпущенных регистрационных свидетельств, включая отозванные регистрационные свидетельства и регистрационные свидетельства с истекшим сроком действия.

197. В целях проверки возможностей непрерывной деятельности, в случае чрезвычайных происшествий, не реже одного раза в год, проводится пробное восстановление информации УЦ из архива.

198. Проверка готовности резервного оборудования УЦ проверяется переключением работы информационной системы УЦ между основным и резервным дата-центрами не реже одного раза в год.

199. Случаи повреждения вычислительных, программных ресурсов и/или данных УЦ должны обрабатываться в порядке, регламентированном для управления инцидентами, резервного копирования, архивирования и восстановления данных.

200. В случае стихийного бедствия или техногенной аварии, требующей временного или постоянного прекращения функционирования основного объекта УЦ, уполномоченные работники Общества инициируют приведение в действие Плана восстановления функционирования.

201. План определяет порядок восстановления сервисов информационных систем и основных функций УЦ в течение 24 (двадцати четырех) часов после происшествия.

202. Восстановление следующих функций осуществляется в течение не более чем 2 (двух) часов:

- выпуск регистрационных свидетельств;
- отзыв регистрационных свидетельств;
- публикация сведений об отзыве регистрационных свидетельств.

203. В соответствии с Планом службы информационной безопасности и операционные службы оценивают ситуацию, корректируют План с учетом складывающейся обстановки и реализуют его с санкции ответственного руководителя Общества.

204. Компрометация закрытого ключа удостоверяющего центра относится к категории чрезвычайных инцидентов и должна влечь за собой введение в действие Плана восстановления функционирования в соответствии с данным параграфом. В этом случае регистрационные свидетельства ключей УЦ в соответствии с указанным планом должны подлежать незамедлительному отзыву.

205. При необходимости отзыва регистрационного свидетельства УЦ выполняются следующие процедуры:



- информация об изменении статуса регистрационного свидетельства УЦ (отзыве) доводится до доверяющих сторон через СОРС в соответствии с параграфом 4.9 Регламента;

- предпринимаются иные целесообразные меры для дополнительного уведомления об отзыве всех заинтересованных участников обслуживаемых УЦ информационных систем;

206. УЦ генерирует новые ключевые пары в соответствии с параграфом 6.1 Регламента, за исключением случаев прекращения деятельности УЦ в соответствии с параграфом 5.8 Регламента.

5.8. Прекращение работы удостоверяющего центра

207. В случае необходимости прекращения деятельности УЦ предпринимает все меры, необходимые для заблаговременного уведомления об этом владельцев, доверяющих сторон и других заинтересованных лиц. В случае принятия решения о прекращении деятельности УЦ разрабатывает план прекращения деятельности с целью минимизации неудобств для клиентов, владельцев и доверяющих сторон. План прекращения может включать в себя следующие вопросы:

- уведомление с информацией о статусе УЦ для сторон, которых касается прекращение, в том числе доверяющих сторон и владельцев;
- оплата стоимости такого уведомления;
- сохранение архивов УЦ на период, предусмотренный законодательством и соответствующей Политикой;
- продолжение сервисов поддержки клиентов;
- продолжение сервисов отзыва, таких как выпуск СОРС или поддержка онлайн услуг проверки статуса;
- отзыв действующих не отозванных регистрационных свидетельств, при необходимости;
- выпуск заменяющих регистрационных свидетельств удостоверяющим центром-правопреемником или, при необходимости, возврат средств тем владельцам, чьи действующие не отозванные регистрационные свидетельства отзываются в соответствии с планом прекращения;
- дальнейшее местонахождение закрытых ключей УЦ и криптографических модулей, содержащих эти закрытые ключи;
- положения, необходимые для передачи сервисов УЦ его правопреемнику.

208. Для минимизации неудобств для клиентов, по согласованию с владельцами, возможна передача в другие удостоверяющие центры сведений, необходимых для продолжения обслуживания владельцев. Если в течение указанных 30 (тридцать) дней вопросы продолжения обслуживания владельцев другим удостоверяющим центром не решены, соответствующие регистрационные свидетельства отзываются и хранятся в архиве УЦ в соответствии с законодательством Республики Казахстан.



6. Контроль технической безопасности

6.1. Генерация и установка ключевых пар

209. Генерация ключевых пар проводится только с помощью средств криптографической защиты информации, криптографическая стойкость которых подтверждена сертификатом соответствия действующему в Республике Казахстан стандарту, определяющему общие технические требования к средствам криптографической защиты информации.

210. Генерация ключевых пар УЦ, проводится только несколькими выделенными и предварительно обученными специалистами из числа ответственного персонала. При этом используются криптографические модули (средства криптографической защиты информации), которые соответствуют не ниже, чем второму уровню безопасности согласно указанному стандарту. По каждой процедуре генерации ключевой пары УЦ составляется протокол, который датируется и подписывается лицами, принимавшими в ней участие. Протоколы хранятся в целях учета и контроля в течение определенного времени, установленного нормативными документами Общества.

211. В случае если владелец генерирует свою ключевую пару самостоятельно, процедура доставки закрытого ключа владельцу не применима.

212. В противном случае закрытый ключ генерируется непосредственно на защищенном носителе.

213. Ключевые пары первичной инициализации для владельцев могут генерировать сотрудники УЦ, центра регистрации или заявителя.

214. Владельцы могут доверить генерацию собственной ключевой пары другому лицу при обязательном условии создания закрытого ключа непосредственно на защищенном носителе ключевой информации, исключающем возможность доступа к закрытому ключу, его несанкционированного изменения или использования. В остальных случаях владельцы генерируют собственные ключевые пары самостоятельно, в этом случае в доставке закрытого ключа владельцу нет необходимости.

215. Доступ к закрытым ключам владельцев со стороны работников или систем УЦ должен быть исключен, за исключением закрытых ключей первичной инициализации.

216. При передаче открытого ключа для подписания в УЦ, он должен доставляться способом, исключающим возможность подмены по пути следования. При этом заявитель, центр регистрации должны быть в состоянии подтвердить факт владения владельцем, соответствующим закрытым ключом. Приемлемым механизмом доставки открытого ключа владельца в УЦ является электронный документ в формате PKCS#10 или PKCS#7, переданный с использованием доступных каналов связи.

217. Генерация ключей для заявителей, желающих защищенно хранить свои закрытые ключи в УЦ, проводится автоматически (не требует непосредственного участия работника УЦ, за исключением системного администрирования, контроля работоспособности и пр.) в отдельном аппаратном криптографическом модуле (HSM), соответствующем не ниже, чем третьему уровню безопасности согласно Стандарту (в соответствии с Правилами



облачной ЭЦП). Указанный отдельный модуль предназначен только для работы с закрытыми ключами владельцев (создание, хранение и использование) и не выполняет никаких иных технологических функций УЦ (выпуск/отзыв регистрационных свидетельств, выпуск СОРС, сервис OCSP, сервис метки времени и пр.).

218. Открытый ключ УЦ вручается доверяющим сторонам в форме регистрационного свидетельства. Владельцы могут запросить регистрационное свидетельство из рук в руки в УЦ, центре регистрации или как часть цепочки к собственному регистрационному свидетельству. Регистрационные свидетельства УЦ также доступны на официальном информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz>. Проверка аутентичности регистрационного свидетельства может быть осуществлена средствами электронной цифровой подписи.

219. УЦ регистрирует ключи, предназначенные для использования в соответствии с:

- государственным стандартом ГОСТ 34.310-2004 (ЭЦП), которые имеют размеры:

- закрытый ключ – 256 бит;
- открытый ключ – 512 бит;
- стандартом СТ РК ГОСТ Р 34.10-2015 (ЭЦП):
 - закрытый ключ – 512 бит;
 - открытый ключ – 1024 бит;
- алгоритмом RSAsha2:
 - закрытый ключ – 2048 бит;
 - открытый ключ – 2048 бит.

6.2. Защита закрытого ключа и инженерный контроль криптографического модуля

220. УЦ реализует комплекс физических, логических и организационных мер, обеспечивающий безопасность собственных закрытых ключей.

221. Владельцы обязаны принимать необходимые меры, предотвращающие потерю, разглашение, изменение и несанкционированное использование своих закрытых ключей.

222. Для генерации и хранения ключевых пар удостоверяющего центра использует криптографические модули, сертифицированные на соответствие действующему в Республике Казахстан стандарту, определяющему общие технические требования к средствам криптографической защиты информации не ниже, чем по второму уровню безопасности.

223. УЦ реализует организационно-технические меры, которые требуют для выполнения важных криптографических операций участия нескольких специалистов из числа ответственного персонала. УЦ использует для закрытых ключей данные активации в форме разделения на «части секрета», которые хранятся выделенными для этого работниками из числа ответственного персонала, так называемыми «хранителями секрета». Для восстановления



закрытого ключа требуется некоторое регламентированное пороговое значение частей секрета (m) из их общего числа (n).

224. Резервирование ключевой информации специализированных HSM, предназначенные для обработки закрытых ключей владельцев регистрационных свидетельств, осуществляется по схеме с разделением секрета (в случае применения указанной процедуры) в соответствии с требованиями Правил облачной ЭЦП.

225. УЦ не депонирует закрытые ключи удостоверяющего центра.

226. УЦ создает резервные копии закрытых ключей удостоверяющего центра в целях обеспечения возможности их восстановления на случай чрезвычайных происшествий и сбоев в работе. Порядок создания резервных копий регламентирован.

227. Резервные копии закрытых ключей УЦ защищены от модификации и разглашения как физическими, так и криптографическими средствами. Уровень данной защиты не должен быть меньше, чем уровень защиты криптографических модулей в условиях основного и запасного объектов УЦ.

228. В ходе резервного копирования ключевые пары выгружаются из аппаратных криптографических модулей в зашифрованном виде, а в ходе восстановления – зашифрованные ключевые пары загружаются в них. Их хранение и использование регламентировано.

229. Резервные копии закрытых ключей УЦ, утратившие актуальность вследствие замены или истечения срока действия, не подлежат архивному хранению и уничтожаются (удаляются) согласно внутреннему документу Общества⁷.

230. В целях обеспечения непрерывности функционирования информационной системы УЦ, закрытые ключи в аппаратных криптографических модулях (HSM) после их генерации или восстановления из резервной копии остаются активированными до момента уничтожения (удаления).

231. В случае необходимости носители закрытых ключей УЦ уничтожаются таким способом, который гарантирует отсутствие остаточной информации о ключе и исключает возможность его восстановления. В частности, используется штатная функция криптографических модулей, удаляющая ключи. Данные процедуры регламентированы и оформляются документально.

232. Меры защиты от разглашения, искажения, подмены и несанкционированного использования своих закрытых ключей, размещенных на защищенных носителях ключевой информации, и данных их активации на всем протяжении их жизненного цикла, от генерации до уничтожения, владельцы принимают самостоятельно, в соответствии с требованиями законодательства, Политики и Регламента.

233. УЦ рекомендует владельцам в работе со своими закрытыми ключами в течение всего их жизненного цикла использовать защищенные носители

⁷ На дату публикации «Правил обращения информации с ограниченным доступом»



ключевой информации, например, смарт-карты или аппаратные токены, которые закрытый ключ никогда не покидает.

234. Владелец, используемых в информационных системах Общества, кроме того, запрещается записывать на носители закрытых ключей постороннюю информацию или иным образом применять указанные носители не по назначению. В нерабочее время носители их закрытых ключей должны находиться в личном сейфе либо в сейфе прямого начальника.

235. Все закрытые ключи, которые используются в информационных системах Общества, должны быть защищены, поэтому обладатели закрытых ключей в соответствии с Политикой должны предпринимать необходимые меры, предотвращающие их потерю, разглашение, изменение или несанкционированное использование.

236. Владелец, используемых в информационных системах Общества, рекомендуется иметь резервную копию соответствующих им закрытых ключей, которая должна храниться в личном сейфе или в запечатанном конверте в сейфе прямого руководителя с указанием на конверте владельца.

237. Резервное копирование закрытого ключа владельцем иных информационных систем, обслуживаемых Обществом, запрещается.

238. Архивное хранение закрытых ключей не допускается.

6.3. Другие особенности управления ключевыми парами

239. Все открытые ключи, когда-либо удостоверенные УЦ, архивируются в соответствии с параграфом 5.5 Регламента.

240. Период использования регистрационного свидетельства заканчивается при истечении срока его действия или отзыве. Период использования ключевой пары совпадает с периодом использования, соответствующего регистрационного свидетельства, за тем исключением, что она может и далее использоваться в целях расшифрования или проверки электронной цифровой подписи.

241. Владельцы и пользователи регистрационных свидетельств не должны использовать свои ключевые пары после истечения срока их действия никак кроме указанных выше случаев.

242. Срок действия регистрационных свидетельств владельцев регистрационных свидетельств в информационных системах, обслуживаемых Обществом, составляет 1 (один) год, за исключением сертификации аутентификации сервера, срок действия которых не должен превышать 3 (трех) лет.

243. Срок действия регистрационных свидетельств первичной инициализации не превышает 30 (тридцать) суток.

244. Срок действия остальных регистрационных свидетельств, выпускаемых УЦ, составляет 1 (один), 2 (два) или 3 (три) года по выбору владельца.

245. Срок действия регистрационных свидетельств УЦ составляет 20 (двадцать) лет и исчисляется с даты и времени его генерации. Действие любого



регистрационного свидетельства заканчивается с истечением срока его действия или в случае его отзыва.

246. Для владельцев сроки использования их ключевых пар совпадают со сроками использования соответствующих регистрационных свидетельств, за исключением того, что они могут использоваться и дольше, в целях расшифрования или проверки электронной цифровой подписи.

247. УЦ не выпускает регистрационные свидетельства, срок действия которых превышает срок действия, соответствующего регистрационного свидетельства УЦ, который необходимо использовать для проверки. В связи с этим, срок использования закрытого ключа УЦ обязательно короче, чем срок действия, соответствующего регистрационного свидетельства. В частности, срок использования закрытого ключа УЦ не может превышать 17 (семнадцать) лет, то есть срок действия соответствующего регистрационного свидетельства (20 лет) минус срок действия самого «длинного» регистрационного свидетельства владельца (3 года).

248. По окончании периода использования ключевой пары владельцы и УЦ обязаны прекратить любое использование этой ключевой пары. Исключение составляет вышеуказанные случаи, а также потребность УЦ в подписи информации об отзыве регистрационных свидетельств в период до истечения срока действия последнего регистрационного свидетельства, который выпущен с помощью данной ключевой пары.

249. Для непрерывной работы в информационных системах, которые требуют наличия регистрационных свидетельств, выпущенных УЦ, пользователь должен своевременно генерировать новые ключевые пары и запрашивать выпуск новых регистрационных свидетельств на замену истекающим.

6.4. Данные активации

250. Участники должны защищать данные активации своих закрытых ключей от потери, хищения, изменения, разглашения или несанкционированного использования.

251. Закрытые ключи владельцев УЦ используются непосредственно на защищенном носителе ключевой информации или в отдельном аппаратном криптографическом модуле (HSM) УЦ, предназначенном только для работы с закрытыми ключами владельцев (создание, хранение и использование) в соответствии с Правилами облачной ЭЦП. В обоих случаях, невозможность разглашения, изменения или несанкционированного использования закрытых ключей гарантируется производителем устройств.

252. Для использования своего закрытого ключа владельцу необходимо создать и применять данные активации в форме пароля.

253. Данные активации закрытых ключей УЦ подлежат разделению секрета. Части секрета генерируются в соответствии с требованиями параграфа 6.2. Регламента. Создание и передача частей секрета протоколируется.

254. В соответствии с Политикой и внутренней политикой безопасности УЦ применяет к данным активации собственных закрытых ключей процедуры



разделения секрета. УЦ обеспечивает процедуры и средства, позволяющие хранителям секрета избежать потери, хищения, изменения, разглашения или несанкционированного использования частей секрета, которые у них находятся. Хранителям секрета запрещается:

- копировать, разглашать и передавать части секрета третьим лицам или, как бы то ни было, несанкционированно использовать их;
- разглашать посторонним лицам свой статус хранителя секрета.

255. Хранители секрета УЦ подписывают соглашение, устанавливающее их ответственность, и обязаны защищать доверенные им части секрета.

256. УЦ настоятельно рекомендует владельцам хранить закрытые ключи в зашифрованном виде и защищать их с помощью аппаратных токенов и/или сильных паролей. Приветствуется использование владельцами комбинированных механизмов аутентификации, например пароля и аппаратного токена, токена и биометрического принципа, биометрического принципа и пароля.

257. Данные активации закрытых ключей УЦ выводятся из использования с применением процедур, защищающих от потери, хищения, модификации, разглашения или несанкционированного использования закрытых ключей, активируемых этими данными. Не подлежащие дальнейшему хранению данные активации выводятся из использования путем перезаписи или физического уничтожения.

6.5. Контроль компьютерной безопасности

258. УЦ обеспечивает контроль используемых вычислительных ресурсов, программного обеспечения и данных от несанкционированного доступа с помощью систем, которые фиксируют показатели, перечисленные в параграфе 5.4. Регламента.

259. Серверы, работающие в УЦ, удовлетворяют следующим требованиям:

- серверы для подписи регистрационных свидетельств, СОРС, ответов (квитанций) службы OCSP, TSP изолирована от неавторизованного доступа;
- операционные системы серверов поддерживаются на высоком уровне защиты, при регулярном применении всех рекомендованных и соответствующих пакетов защиты и обновлений, в том числе антивирусных;
- ведется мониторинг с целью обнаружения несанкционированных программных изменений;
- количество запущенных на сервере системных служб операционных систем сведено к минимуму.

260. Доступ к основным серверам разрешен только назначенным администраторам УЦ. Работники НПК, не являющиеся администраторами УЦ, пользователи общих приложений, не имеют доступа к системным или технологическим учетным записям.

261. Основные сети, используемые для обслуживания участников инфраструктуры открытых ключей, логически отделены от остальных компонент. Это разделение исключает любой сетевой доступ, кроме доступа через определенные прикладные процессы. Прямой доступ к базам данных,



обеспечивающим хранилище УЦ, ограничен минимально необходимой группой администраторов информационной системы УЦ.

262. УЦ использует межсетевые экраны для защиты основных сетей от внутреннего и внешнего вмешательства и ограничивает содержание и источники сетевой активности, которая может влиять на основные системы.

263. Средства криптографической защиты информации, которые используются участниками информационных систем, обслуживаемых УЦ, должны быть сертифицированы на соответствие действующим в Республике Казахстан основным техническим требованиям. Специальных требований по сертификации иных компонентов используемых вычислительных систем и программного обеспечения не выдвигается.

6.6. Технический контроль жизненного цикла

264. Все прикладное программное обеспечение, которое использует в своей деятельности УЦ, является лицензионным, исключительные права на него не принадлежат Обществу.

265. УЦ выступает заказчиком используемого программного обеспечения. УЦ самостоятельно определяет требования к его разработке, включая требования к среде разработки, корректности и качеству результирующего программного обеспечения.

266. Работоспособность и целостность технических и программных средств УЦ обеспечивается системой организационных и технических мер, основанных на разделении прав использования указанных средств, доступа к ним, а также к техническим средствам, необходимым для доступа.

267. Обязательства по обеспечению надлежащего функционирования указанного программного обеспечения выполняет поставщик по договору (сервисная организация).

268. В целях апробации любых изменений в информационной системе УЦ имеет и поддерживает ее тестовый контур, обеспеченный необходимым минимумом вычислительной техники, средств криптографической защиты информации и лицензий на использование программного обеспечения.

6.7. Средства управления сетевой безопасностью

269. Функции УЦ выполняются в сетях, защищаемых в регламентированном порядке от несанкционированного доступа, вмешательства и DDOS-атак.

270. Схема взаимодействия модулей (компонент) удостоверяющего центра с пояснительной запиской отражена в соответствующем документе.

6.8. Метки времени

271. Регистрационные свидетельства, СОРС, ответы квитанции (службы) OCSP, контрольные протоколы, содержащие информацию о выпуске и изменении статуса регистрационных свидетельств, содержат информацию о дате и времени их создания, и заверяется электронной цифровой подписью.



7. Профили регистрационных свидетельств, СОРС и ОССП

7.1. Профиль регистрационного свидетельства

272. Регистрационные свидетельства, выпускаемые УЦ, соответствуют рекомендациям ITU-T X.509 v3 и IETF RFC 5280.

273. Основные поля и расширения, содержащиеся в регистрационных свидетельствах, вместе с требованиями к их содержанию и синтаксису, а также указываемые в регистрационных свидетельствах криптографические алгоритмы и их объектные идентификаторы на официальном информационном ресурсе Общества в сети Интернет по адресу: <https://npck.kz>.

274. Все регистрационные свидетельства, выпускаемые УЦ, имеют номер версии v3.

275. Имена, которые указываются в регистрационных свидетельствах, выпускаемых УЦ, соответствуют требованиям параграфа 3.1 Регламента и соответствующей Политики в соответствии с форматом имен ITU-T X.520.

276. Используемые имена должны соответствовать формату DN-имен, определенных рекомендациями (ITU-T) X.501.

277. Объектные идентификаторы политики регистрационных свидетельств, соответствующие информационным системам, в которых применяются выпущенные УЦ регистрационные свидетельства, установлены в соответствие с параграфом 1.4 Регламента. Расширение «certificatePolicies» заполняется в соответствии с указанным параграфом.

278. Квалификаторы политики в регистрационных свидетельствах, выпускаемых УЦ, содержат ссылки на Регламент и Политику через перечень всех используемых УЦ объектных идентификаторов политики.

7.2. Профиль СОРС

279. УЦ формирует СОРС в соответствии с рекомендациями (ITU-T) X.509 v3 и (IETF) RFC 5280.

280. Основные поля и расширения, содержащиеся в СОРС, вместе с требованиями к их содержанию приведены на официальном информационном ресурсе Общества в сети Интернет по адресу: <https://npck.kz>.

281. Все СОРС, выпускаемые УЦ, имеют номер версии v2.

7.3. Профиль ОССП

282. Для получения информации о статусе регистрационных свидетельств, выпущенных УЦ, предоставляет сервис ОССП в формате версии 1 согласно рекомендациям (IETF) RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP» (Онлайн протокол статуса сертификатов интернет-инфраструктуры открытых ключей X.509).

283. Предоставляемый сервис ОССП обрабатывает все расширения запросов, определенные рекомендациями (IETF) RFC 2560.



8. Проверка деятельности

284. Аккредитация удостоверяющего центра осуществляется сроком на 3 (три) года в соответствии с правовым актом уполномоченного органа.

285. Деятельность Общества подлежит регулярным проверкам со стороны уполномоченного органа по управлению Общества в лице Национального Банка Республики Казахстан (далее – Национальный Банк). В частности, в ходе проверок может:

- рассматриваться актуальность и соблюдение действующих документально закреплённых требований: политики безопасности, включая требования по безопасности на объектах Общества, договорных обязательств. Может оцениваться надёжность и эффективность системы внутреннего контроля;

- проводиться анализ вероятности потенциальных угроз для штатного режима деятельности, уязвимостей в системах обеспечения, оценка их возможных последствий, выработка мер совершенствования организации работы. Может оцениваться эффективность управления рисками.

286. Частота и основания проведения проверок Общества со стороны Национального Банка определяется нормативными правовыми актами Национального Банка.

287. Тематика проверок Общества со стороны Национального Банка определяется в соответствии с нормативными правовыми актами Национального Банка.

288. После получения отчёта о проверке деятельности, при выявлении в ней нарушений и недостатков, формы их устранения и исключения определяются в соответствии с нормативными правовыми актами Национального Банка.

289. Если выявленные нарушения и недостатки представляют непосредственную угрозу безопасности и целостности информационных систем, обслуживаемых УЦ, то составляется План устранения недостатков и реализуется в месячный срок, в ходе которого УЦ принимает решения о необходимости:

- отзыва регистрационных свидетельств и/или публикации уведомления о компрометации;
- приостановления функционирования сервисов;
- исключения неполноценных сервисов из сферы действия Политики и прекращения действия соответствующих договоров.

290. Для менее серьёзных нарушений и недостатков в результате оценки их значимости определяется комплекс мер, который может планомерно реализовываться в течение длительного периода времени.

291. О результатах устранения нарушений и недостатков, выявленных в ходе проверки Национального Банка, УЦ информирует Национальный Банк Республики Казахстан в соответствии с нормативными правовыми актами Национального Банка.



9. Прочие коммерческие и юридические вопросы

9.1. Тарифы

292. УЦ предоставляет своим клиентам следующие услуги:

- выпуск регистрационных свидетельств владельцев по заявлениям юридических и физических лиц, включая:
 - регистрацию заявлений;
 - выдачу ключевых пар первичной инициализации;
 - создание регистрационных свидетельств владельцев;
- отзыв регистрационных свидетельств;
- размещение регистрационных свидетельств, Политики, Регламента и иной интересующей клиентов информации в публично доступном хранилище. Актуализация информации в хранилище;
- публикация в хранилище СОПС;
- предоставление информации о статусе регистрационных свидетельств в режиме онлайн по протоколу OSCP (служба OSCP);
- привязка данных к реальному времени в режиме онлайн по протоколу TSP (услуги сервера метки времени);
- подтверждение принадлежности, подлинности и действительности выпущенных регистрационных свидетельств по заявлениям заинтересованных сторон.

293. Оплате подлежат услуги УЦ, связанные с выпуском регистрационных свидетельств. Актуальная информация о тарифах на выпуск регистрационных свидетельств доступна на информационном ресурсе Общества в сети Интернет по адресу <https://npck.kz>.

294. За остальные услуги, указанные в параграфе 9.1 Регламента, УЦ отдельную плату не взимает, их стоимость входит в цену договора на оказание услуг в конкретных информационных системах.

295. При этом отдельная плата не взимается за регистрацию заявлений владельцев и выдачу им ключевых пар первичной инициализации, их стоимость включена в тариф на выпуск основного регистрационного свидетельства.

296. УЦ не взимает плату за доступность регистрационных свидетельств доверяющим сторонам через хранилище или иными способами.

297. УЦ не взимает плату за доступность доверяющим сторонам списков отозванных регистрационных свидетельств, указанных в Регламенте, через хранилище или иными способами.

298. УЦ не взимает плату за доступность доверяющим сторонам службы OSCP, указанной в Регламенте, или иных возможных способов получения информации о статусе регистрационных свидетельств.

9.2. Финансовая ответственность

299. Общество несет финансовую ответственность за комплекс предоставляемых услуг по использованию информационных систем (МСПД, ФАСТИ и др.) в рамках договора с клиентом о возможности использования конкретной системы из числа указанных. Отдельной финансовой



ответственности за услуги удостоверяющего центра в комплексе услуг по использованию конкретной информационной системы Общества не несет.

300. Общество не несет финансовой ответственности перед доверяющими сторонами, не являющимися владельцами.

301. Ответственность участников инфраструктуры открытых ключей, обслуживаемой УЦ, установлена законодательством Республики Казахстан.

302. Ответственность персонала Удостоверяющего центра и центров регистрации установлена трудовым договором и должностными инструкциями.

303. Выполнение обязанностей и функций, а также риски ответственности УЦ перед владельцами и доверяющими сторонами обеспечиваются финансовыми ресурсами Общества.

9.3. Конфиденциальность коммерческой информации

304. Следующая информация считается и хранится как конфиденциальная:

- материалы заявлений на выпуск регистрационных свидетельств;
- закрытые ключи первичной инициализации;
- транзакционные материалы;
- контрольные протоколы;
- отчеты о проверках деятельности (внутренних и аудиторских) УЦ;
- планы восстановления функционирования;
- меры безопасности, контролирующие функционирование аппаратного и программного обеспечения, администрирование служб регистрационных свидетельств и регистрации.

305. Участники информационных систем, обслуживаемых УЦ, признают, что регистрационные свидетельства, информация об их отзыве или иная информация о статусе регистрационных свидетельств, публичная часть хранилища и содержащаяся в них информация не рассматриваются в качестве конфиденциальной информации. Информация, не перечисленная в данном параграфе, не рассматривается как конфиденциальная, если иное не предусмотрено действующим законодательством Республики Казахстан.

306. УЦ защищает известную ему конфиденциальную информацию от компрометации и разглашения третьим сторонам.

9.4. Конфиденциальность персональных данных

307. Любой владелец признает, что, подавая заявление на выпуск регистрационного свидетельства в УЦ или центр регистрации он дает согласие на размещение содержащейся в нем информации о себе в публичном доступе. Заявление на выпуск регистрационного свидетельства 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.

308. УЦ обеспечивает защиту персональных данных участников инфраструктуры открытых ключей в соответствии с законодательством Республики Казахстан по вопросам персональных данных и их защиты.



9.5. Права интеллектуальной собственности

309. В своей деятельности УЦ использует программное обеспечение, авторские и исключительные имущественные права на которое не принадлежат Обществу. Порядок использования программного обеспечения определяется условиями лицензий, приобретенных Обществом.

310. Общество оставляет за собой права интеллектуальной собственности на регистрационные свидетельства, которые он выпускает, и на информацию об их статусе. При этом Общество не запрещает копирование и распространение регистрационных свидетельств на неисключительной безвозмездной основе, при соблюдении условий полноты копирования и использования регистрационных свидетельств. Общество также не запрещает использование информации о статусе регистрационных свидетельств для выполнения функций доверяющей стороны.

311. Заявители на выпуск регистрационных свидетельств сохраняют все свои права на все торговые и тому подобные марки и имена в выпущенных регистрационных свидетельствах.

312. Участники информационных систем, обслуживаемых УЦ, признают право интеллектуальной собственности Общества на Регламент и другую документацию Общества, регламентирующую деятельность УЦ.

313. Закрытые ключи, которые соответствуют регистрационным свидетельствам, выпущенным УЦ, составляют собственность владельцев в независимости от физических носителей, на которых хранятся эти ключевые пары и которыми они защищаются. В частности, открытые ключи, регистрационные свидетельства и части секрета закрытых ключей УЦ, являются собственностью Общества.

9.6. Гарантии и заверения

314. УЦ гарантирует:

- отсутствие в выпущенных регистрационных свидетельствах умышленных искажений фактов, внесенных УЦ или известных ему;
- отсутствие в информации регистрационных свидетельств случайных ошибок, допущенных УЦ вследствие халатности при рассмотрении заявлений на выпуск или создании регистрационных свидетельств;
- соответствие регистрационных свидетельств требованиям законодательства Республики Казахстан, существенным требованиям Политики и Регламента;
- соответствие сервисов отзыва регистрационных свидетельств и использования хранилища требованиям законодательства Республики Казахстан, существенным требованиям Политики и Регламента во всех существенных аспектах.

315. УЦ обязан выполнять условия гарантий и заверений владельца и доверяющей стороны, изложенные в данном параграфе.

316. Центры регистрации обязаны выполнять условия гарантий и заверений владельца и доверяющей стороны, изложенные в данном параграфе, а также гарантировать соблюдение следующих условий:



- отсутствие в выпущенных регистрационных свидетельствах умышленных искажений фактов, внесенных их работниками или владельцами;
- отсутствие в информации регистрационных свидетельств известных им случайных ошибок, допущенных их работниками или владельцами вследствие халатности;
- владельцы указанных регистрационных свидетельств ознакомлены с Регламентом, соответствующей ему Политикой, и от них центром регистрации получено письменное обязательство выполнять требования и нести ответственность, предусмотренные этими документами для доверяющих сторон.

317. Владельцы обязаны выполнять условия гарантий и заверений доверяющей стороны, изложенные в данном параграфе, условий о предоставлении услуг УЦ, а также гарантировать соблюдение следующих условий:

- отсутствие в выпущенных регистрационных свидетельствах умышленных искажений фактов, внесенных их работниками или владельцами;
- отсутствие в информации регистрационных свидетельств известных им случайных ошибок, допущенных владельцем вследствие халатности;
- владельцы указанных регистрационных свидетельств ознакомлены с Политикой, соответствующим ей Регламентом, и на них владельцем возложены обязанности и выполнять требования и нести ответственность, предусмотренные этими документами для владельцев и доверяющих сторон.

318. Доверяющие стороны гарантируют то, что они:

- обладают достаточным объемом информации, чтобы принимать обоснованные решения в отношении той степени, в которой они хотят опираться на информацию из регистрационного свидетельства;
- несут исключительную ответственность за принятие решений, опираться или не опираться на эту информацию;
- принимают правовые последствия нарушений обязательств доверяющей стороны в условиях Политики.

9.7. Отказ от гарантий

319. Общество не несет дополнительной гарантийной ответственности, включая ответственность за товарную пригодность и соответствие, кроме той, которая включена в договоры на оказание услуг в конкретных информационных системах, если иное не предусмотрено действующим законодательством Республики Казахстан.

9.8. Ограничение ответственности

320. Общество несет финансовую ответственность за комплекс предоставляемых услуг по использованию информационных систем Общества перед клиентами в рамках договоров о возможности использования конкретной системы из числа указанных.

321. Иная ответственность УЦ, центров регистрации, владельцев регистрационных свидетельств и доверяющих сторон предусмотрена Кодексом Республики Казахстан «Об административных правонарушениях» (Статья 640.



Нарушение законодательства Республики Казахстан об электронном документе и электронной цифровой подписи).

322. При этом участники инфраструктуры открытых ключей не несут ответственности за не прямой, особый, случайный, вытекающий ущерб и упущенную выгоду.

9.9. Компенсации

323. В части, не противоречащей законодательству Республики Казахстан, центры регистрации обязаны возмещать расходы, связанные:

- с подтверждением ошибочной, вводящей в заблуждение или заведомо ложной информации в заявлениях на выпуск регистрационного свидетельства;
- с сокрытием существенных фактов в заявлениях на выпуск регистрационного свидетельства, если оно является результатом непреднамеренного или умышленного введения в заблуждение или бездействия.

324. В части, не противоречащей законодательству Республики Казахстан, владельцы обязаны возмещать расходы, связанные с:

- представлением ошибочной, вводящей в заблуждение или заведомо ложной информации в заявлении на выпуск или отзыв регистрационного свидетельства;
- сокрытием существенных фактов в заявлении на выпуск или отзыв регистрационного свидетельства, если оно является результатом непреднамеренного или умышленного введения в заблуждение или бездействия;
- принятием мер защиты собственного закрытого ключа, приведшим к его компрометации, утере, разглашению, изменению или несанкционированному использованию;
- использованием в составе своего отличительного имени названий, нарушающих права интеллектуальной собственности третьих лиц.

325. В части, не противоречащей законодательству Республики Казахстан, доверяющие стороны обязаны возмещать расходы, связанные с:

- нарушением своих договорных обязательств о выполнении обязанностей доверяющей стороны;
- несоответствующим обстоятельствам доверием к регистрационному свидетельству;
- принятием мер по проверке регистрационного свидетельства с целью определения его отзыва и сроков действия.

9.10. Вступление в силу и прекращение действия

326. Регламент вступает в силу с момента опубликования на интернет-ресурсе Общества. Изменения и дополнения в Регламент также вступают в силу с момента опубликования на интернет-ресурсе Общества.

327. С момента прекращения действия Регламента участники информационных систем, обслуживаемых Обществом, остаются связанными его условиями по всем регистрационным свидетельствам до момента истечения периода их действия.



9.11. Индивидуальные уведомления и связь с участниками

328. Участники информационных систем, обслуживаемых Обществом, для связи друг с другом вправе использовать любые целесообразные методы, соответствующие критичности и предмету взаимодействия, если иное не определено соглашением между сторонами.

9.12. Изменения и дополнения

329. Общество оставляет за собой право без предварительного уведомления вносить несущественные изменения и дополнения в Регламент, включая, но не ограничиваясь исправлением опечаток, изменением адресов ссылок и контактной информации. Решения о том, являются ли данные изменения и дополнения существенными или нет, принимаются по исключительному усмотрению Общества.

330. Изменения и дополнения к Регламенту оформляются в виде отдельного документа, содержащего либо актуальный текст Регламента, либо уведомление об изменениях и дополнениях в его актуальный текст.

331. Общество отвечает за определение необходимости изменения объектных идентификаторов Политики для приведения их в соответствие с измененным содержанием Регламента.

332. Общество может запрашивать предложения о внесении изменений и дополнений в Регламент у участников обслуживаемых информационных систем. Общество предварительно публикует предлагаемые существенные изменения и дополнения к Регламенту на своем официальном информационном ресурсе в сети Интернет, предусматривая при этом срок их рассмотрения.

333. Если иное не указано особо, период рассмотрения предлагаемых существенных изменений и дополнений к Регламенту составляет 21 (двадцать один) календарный день со дня опубликования. Участники информационных систем, обслуживаемых Обществом, вправе подавать свои замечания и предложения в Общество в период рассмотрения.

334. Общество рассматривает все поданные замечания и предложения по предложенным изменениям и дополнениям. При этом Общество вправе:

- ввести исходные изменения и дополнения в действие в полном объеме;
- составить и опубликовать новую редакцию предлагаемых изменений и дополнений;
- отозвать проект изменений и дополнений в Регламент.

335. Не отозванные и не скорректировавшиеся изменения и дополнения по истечении периода их рассмотрения публикуются как вступившие в силу.

336. Несмотря на возможное наличие противоречий в проекте, если Общество считает, что существенные изменения или дополнения к Регламенту требуются немедленно в целях предотвращения нарушения безопасности обслуживаемых информационных систем, Общество вправе внести их путем утверждения и опубликования в хранилище, тем самым вводя в действие с момента опубликования.



9.13. Положения о разрешении споров

337. Споры между участниками информационных систем, обслуживаемых УЦ, разрешаются в соответствии с положениями действующих договоров между сторонами, и/или законодательства Республики Казахстан.

338. Если спор не решен таким способом он подлежит разрешению в судебном порядке по месту нахождения Общества.

9.14. Юрисдикция

339. Юрисдикцией для Регламента является законодательство Республики Казахстан.

9.15. Соответствие действующему законодательству

340. К участникам ИОК: удостоверяющему центру, центрам регистрации, владельцами и пользователями регистрационных свидетельств (владельцам 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 СКЗИ);
- 3) платежей и платежных систем;
- 4) персональных данных и их защиты.

9.16. Прочие положения

341. В случае если часть положений Регламента будет признана неосуществимой судом или уполномоченным государственным органом, остальная ее часть сохраняет силу.

342. В случае наступления обстоятельств непреодолимой силы (форс-мажор) участники ИОК: УЦ, центры регистрации, владельцы и пользователи регистрационных свидетельств (владельцы и доверяющие стороны), - руководствуются соответствующими положениями действующих между ними договоров (при наличии).

