**АДМИНИСТРАЦИЯ**
**городского округа Анадырь**

# РАСПОРЯЖЕНИЕ

От 19.10.2018 № 179

О назначении ответственного за эксплуатацию средств криптографической защиты информации

Во исполнение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации, для организации обеспечения безопасности конфиденциальной информации с использованием средств криптографической защиты информации,

1. Возложить обязанности ответственного за эксплуатацию средств криптографической защиты информации на начальника отдела информационных технологий и технической защиты информации Управления по организационным и административно-правовым вопросам Администрации городского округа Анадырь.

2. Утвердить:

2.1. Инструкцию ответственного за эксплуатацию средств криптографической защиты информации согласно приложению №1 к настоящему распоряжению;

2.2. Инструкцию пользователя средств криптографической защиты информации согласно приложению №2 к настоящему распоряжению;

2.3. Инструкцию по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации согласно приложению №3 к настоящему распоряжению.

3. Отделу делопроизводства и кадровой работы Управления по организационным и административно-правовым вопросам Администрации городского округа Анадырь (Куркина Ю.В.) ознакомить с настоящим распоряжением муниципальных служащих и работников, не являющихся муниципальными служащими Администрации городского округа Анадырь,

подразделений Администрации городского округа Анадырь, являющихся самостоятельными юридическими лицами, под роспись.

4. Контроль за выполнением настоящего распоряжения оставляю за собой.

Глава Администрации И.В. Давиденко

Приложение №1
к распоряжению Администрации
городского округа Анадырь
от 19.10.2018 № 179

# ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ЭКСПЛУАТАЦИЮ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

## 1. Общие положения

1.1. Настоящая Инструкция ответственного за эксплуатацию средств криптографической защиты информации (далее – СКЗИ) в Администрации городского округа Анадырь, подразделениях Администрации городского округа Анадырь, являющихся самостоятельными юридическими лицами (далее – Администрация) определяет основные обязанности и права ответственного за эксплуатацию СКЗИ.

1.2. Ответственный за эксплуатацию СКЗИ назначается распоряжением Администрации городского округа Анадырь и отвечает за организацию, обеспечение функционирования и безопасности СКЗИ, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.3. Ответственный за эксплуатацию СКЗИ должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных, а также в области защиты информации при ее передаче по открытым каналам связи с использованием СКЗИ.

1.4. В своей деятельности, связанной с обработкой персональных данных, ответственный за эксплуатацию СКЗИ руководствуется настоящей Инструкцией.

## 2. Обязанности ответственного за эксплуатацию СКЗИ

Ответственный за эксплуатацию СКЗИ обязан:

2.1. Соблюдать требования нормативных актов Администрации, устанавливающих порядок работы с персональными данными.

2.2. Осуществлять контроль за организацией, обеспечением функционирования и безопасности СКЗИ:

-контролировать соблюдение условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;

-обеспечивать надежное хранение эксплуатационной и технической документации к СКЗИ, ключевых документов, носителей информации ограниченного распространения;

-вносить предложения по режиму охраны помещений, в которых установлены СКЗИ или хранятся ключевые документы к ним;

-вести Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал) (Приложение №1);

-выдавать пользователям СКЗИ, экземпляры эксплуатационной и технической документации к ним, ключевых документов под расписку в соответствующем Журнале;

-вести на каждого пользователя СКЗИ Лицевой счет (Приложение №2), в котором регистрировать числящиеся за ними СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;

-контролировать передачу СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями СКЗИ и (или) ответственным за эксплуатацию СКЗИ под расписку в соответствующем Журнале;

-пломбировать (опечатывать) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ;

-контролировать получение и доставку СКЗИ, эксплуатационной и технической документации к ним;

-заблаговременно делать заказы на изготовление очередных ключевых документов и рассылку на места использования для своевременной замены действующих ключевых документов;

-контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) под расписку в соответствующем Журнале;

-выводить из действия ключевые документы, в отношении которых возникло подозрение в компрометации;

-принимать решение в чрезвычайных случаях, когда отсутствуют ключевые документы для замены скомпрометированных, об использовании скомпрометированных ключевых документов;

-проводить инструктаж пользователей СКЗИ по правилам работы с СКЗИ и ключевыми документами.

2.3. Требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ с СКЗИ или нарушения функционирования СКЗИ.

2.4. Участвовать в анализе ситуаций, касающихся нарушения условий хранения носителей персональных данных, использования СКЗИ, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

2.5. Контролировать исполнение пользователями СКЗИ требований Инструкции пользователя СКЗИ и прочих нормативных актов Администрации в части обеспечения защиты персональных данных с помощью СКЗИ.

2.6. Принимать все необходимые меры для обеспечения безопасности персональных данных, в случае получения от пользователей информации о фактах утраты, компрометации ключевой информации, в частности, обеспечить выполнение следующих мероприятий:

-в каждом случае, по факту (или предполагаемой) компрометации ключевых документов, проводится служебное расследование; результатом расследования является квалификация или не квалификация данного события как компрометация;

-о факте компрометации ключевой информации пользователями СКЗИ совместно с ответственным за эксплуатацию СКЗИ производится информирование всех заинтересованных участников информационного обмена;

-выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в Журнале;

-для своевременного восстановления связи пользователю СКЗИ выдается новый ключевой документ; для этого создаётся резервный запас ключевых документов, использование которых осуществляется в случаях крайней необходимости по решению ответственного за эксплуатацию СКЗИ.

2.7. Подготавливать копии ключевых документов, которые подлежат основному учету и хранятся в сейфе ответственного за эксплуатацию СКЗИ. Данные копии применяются с разрешения руководителя подразделения Администрации городского округа Анадырь, если по результатам расследования не было установлено факта компрометации.

2.8. Хранить резервные ключевые документы отдельно от рабочих (актуальных), с целью обеспечения невозможности их одновременной компрометации.

2.9. Своевременно информировать ответственного за организацию обработки персональных данных в Администрации о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

## 3. Права ответственного за эксплуатацию СКЗИ

Ответственный за эксплуатацию СКЗИ имеет право:

3.1. Знакомиться с нормативными актами Администрации, регламентирующими процессы обработки персональных данных.

3.2. Требовать от пользователей ИСПДн соблюдения требований нормативных актов Администрации в части обеспечения защиты информации с помощью СКЗИ.

3.3. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных пользователей СКЗИ, в случае выявления нарушений требований по

работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных, или в связи с нарушением функционирования СКЗИ

Приложение №1
к Инструкции ответственного
за эксплуатацию СКЗИ

# ЖУРНАЛ
# ПОЭКЗЕМПЛЯРНОГО УЧЕТА СКЗИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

| № п/п | Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов | Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов | Номера экземпляров (криптографические номера) ключевых документов | Отметка о получении | | Отметка о выдаче | | Отметка о подключении (установке) СКЗИ | | | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | | | Примечание |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | От кого получены | Дата и номер сопроводительного письма | Ф.И.О. пользователя СКЗИ | Дата и расписка в получении | Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку) | Дата подключения (установки) и подписи лиц, произведших подключение (установку) | Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ | Дата изъятия (уничтожения) | Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение) | Номер акта или расписка об уничтожении | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

Приложение №2
к Инструкции ответственного
за эксплуатацию СКЗИ

**ЖУРНАЛ**
**ЛИЦЕВЫХ СЧЕТОВ ПОЛЬЗОВАТЕЛЕЙ СКЗИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ**

**ЛИЦЕВОЙ СЧЕТ №_____**

**Пользователь СКЗИ:** _____

(должность)

_____

(ФИО)

| № п/п | Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов | Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов | Номера экземпляров (криптографические номера) ключевых документов | Дата и номер подтверждения или расписка о получении СКЗИ | Дата и номер подтверждения или расписка о возвращении/уничтожении СКЗИ | Примечание |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |
| | | | | | | |

Приложение №2
к распоряжению Администрации
городского округа Анадырь
от 19.10.2018 № 179

# ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

## 1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (далее - СКЗИ) в Администрации городского округа Анадырь, подразделениях Администрации городского округа Анадырь, являющихся самостоятельными юридическими лицами (далее – Администрация), которые осуществляют работу с применением СКЗИ.

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

Под обращением с СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 (далее - Инструкция ФАПСИ от 13 июня 2001 г. №152) и «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. № 66.

## 2. Термины и определения

Средство криптографической защиты информации (СКЗИ) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты

информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Пользователи СКЗИ – муниципальные служащие и работники Администрации, непосредственно допущенные к работе с СКЗИ.

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Компрометация криптоключей - хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

## 3. Обязанности пользователя

Пользователи средств криптографической защиты обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены;
- соблюдать требования по обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- выполнять инструкции пользователя СКЗИ;
- своевременно сообщать в ответственному за эксплуатацию СКЗИ о нарушениях порядка использования и хранения СКЗИ и ключевых носителей;
- сдать ответственному за эксплуатацию СКЗИ, эксплуатационную и техническую документацию к СКЗИ, ключевые документы и ключевые носители при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.
- немедленно уведомлять ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключевых носителей, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

## 4. Допуск и работа с СКЗИ

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения и подписания обязательства пользователя СКЗИ (Приложение №1). Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией на основании принятых от этих лиц зачетов по программе обучения.

## 5. Учет, выдача и уничтожение СКЗИ и ключевых носителей

5.1. Все СКЗИ и ключевые носители передаются пользователю СКЗИ с отметкой в соответствующих журналах и в его лицевом счете, в котором указывается тип и регистрационный номер экземпляра СКЗИ или ключевого носителя, нанесенный на корпус единицы поэкземплярного учета.

5.2. Изготовление криптографических ключей может производиться ответсвенным за эксплуатацию СКЗИ в присутствии пользователя.

5.3. Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (дискету, ruToken, EToken и др.) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

5.4. В целях обеспечения непрерывности проведения работы плановую смену криптографических ключей следует производить заблаговременно (за 2 (два) месяца до окончания срока действия закрытых криптографических ключей).

5.5. При замене криптографических ключей используют программное обеспечение в соответствии с документами по эксплуатации. Пользователь самостоятельно обязан обновить сертификат ключа подписи. Обновление справочников сертификатов ключей производится путем добавления новых сертификатов ключей подписи из файлов, содержащих сертификаты ключей подписи, предоставляемых ответственным за эксплуатацию СКЗИ. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

5.6. Поэкземплярный учет СКЗИ и ключевых носителей, ведется в соответствующем журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов и в журнале лицевых счетов пользователей СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, который ведет ответственный за эксплуатацию СКЗИ.

5.7. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному за эксплуатацию СКЗИ.

5.8. Уничтожение криптографических ключей пользователя СКЗИ производится с отметкой в журнале поэкземплярного учета СКЗИ и журнале лицевых счетов пользователя СКЗИ или с составлением соответствующего акта, если уничтожается большое количество ключей.

5.9. Криптографические ключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие

криптографические ключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

## 6. Действия при компрометации ключевой информации

6.1. В случае подозрения на компрометацию секретного ключа пользователь СКЗИ обязан уведомить ответственного пользователя СКЗИ о данном факте. Учитывая обстоятельства факта компрометации секретного ключа, ответственный за эксплуатацию СКЗИ принимает решение о кратковременном продолжении использования секретного ключа или вывода его из эксплуатации и сообщает об этом пользователю СКЗИ.

6.2. Пользователь СКЗИ после принятия решения о компрометации секретного ключа обязан сдать все имеющиеся у него экземпляры секретных ключей, поставив отметку в соответствующих журналах о сдаче ключевого носителя.

6.3. В особых случаях, когда немедленная замена секретного ключа невозможна и существует острая необходимость в эксплуатации секретного ключа, пользователь СКЗИ может обратиться с просьбой о приостановке вывода секретного ключа из обращения. При этом пользователь СКЗИ должен до минимума сократить объем и важность электронного документооборота с использованием данного секретного ключа.

## 7. Хранение СКЗИ и ключевой информации

7.1. Пользователи СКЗИ должны хранить инсталлирующие носители СКЗИ, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Пользователи СКЗИ должны предусмотреть также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае выхода из строя действующих криптоключей. Резервные ключевые носители хранятся в спецхранилищах ответственного за эксплуатацию СКЗИ.

7.2. В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей, необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ и должны сдаваться охране вместе с ключами от спецпомещения в отдельных опечатываемых пеналах (тубусах) в конце рабочего дня.

Приложение №1
к Инструкции пользователя
средств криптографической
защиты информации

**ОБЯЗАТЕЛЬСТВА**
**ПОЛЬЗОВАТЕЛЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

Я,_____,
(должность, ФИО)

становясь пользователем средств криптографической защиты информации, добровольно беру на себя следующие обязательства:

- не разглашать и не передавать посторонним лицам сведения конфиденциального характера, которые мне будут доверены или станут известны по работе;
- не распространять сведения о функционировании и порядке обеспечения безопасности СКЗИ и ключевых документах к ним, а также иной конфиденциальной информации, ставшей мне известной в процессе выполнения своих служебных обязанностей;
- неукоснительно выполнять относящиеся к моей деятельности требования по обеспечению безопасности конфиденциальной информации;
- немедленно сообщать ответственному за эксплуатацию СКЗИ о ставших мне известных попытках посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним;
- не использовать знания о защищаемой конфиденциальной информации, СКЗИ, криптоключах к ним для занятий любым видом деятельности, которая может нанести ущерб Администрации городского округа Анадырь;
- в случае увольнения или отстранения от исполнения возложенных обязанностей сдать ответственному за эксплуатацию СКЗИ, СКЗИ, ключевые документы и все носители конфиденциальной информации, которые находились в моём распоряжении;
- немедленно докладывать ответственному за эксплуатацию СКЗИ об утрате или недостаче СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, персональных данных, а также о причинах и условиях возможной утечки таких сведений.

_____ _____
подпись дата

Приложение №3
к распоряжению Администрации
городского округа Анадырь
от 19.10.2018 № 179

# ИНСТРУКЦИЯ
# ПО ВОССТАНОВЛЕНИЮ СВЯЗИ В СЛУЧАЕ КОМПРОМЕТАЦИИ ДЕЙСТВУЮЩИХ КЛЮЧЕЙ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

1. Под компрометацией индивидуального ключа понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность конфиденциальной информации. К событиям, связанным с компрометацией действующих криптографических ключей, относится:

1) утрата (в том числе хищение) ключевых документов (ключевая информация на usb-накопителе, токене) с последующим их обнаружением;

2) увольнение муниципальных служащих, работников Администрации городского округа Анадырь, подразделений Администрации городского округа Анадырь являющихся самостоятельными юридическими лицами, имевших доступ к ключевой информации;

3) передача ключевой информации по линии связи в открытом виде (если это не предусмотрено правилами пользования);

4) нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;

5) возникновение подозрений на утечку информации или ее искажение;

6) не расшифровывание входящих или исходящих сообщений;

7) отрицательный результат при проверке электронной подписи документа;

8) физическое нарушение целостности ключевых документов и (или) печати на спецхранилище (сейф, металлический шкаф, пр.), где хранились ключевые документы;

9) несанкционированное копирование ключевых документов;

10) случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе, случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате злоумышленных действий).

Первые пять событий должны трактоваться как безусловная компрометация действующих ключей, при наличии остальных событий требуется специальное расследование в каждом конкретном случае.

2. При наступлении любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за эксплуатацию СКЗИ.

3. Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия специально назначаемой комиссией во главе с ответственным за эксплуатацию СКЗИ.

Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих ключей.

При установлении факта компрометации действующих ключей, скомпрометированные секретные ключи шифрования и подписи уничтожаются.

4. Для восстановления конфиденциальной связи после компрометации ключей пользователь обращается к ответственному за эксплуатацию СКЗИ с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования и ЭП осуществляется тем же порядком, как и при плановой смене ключей.