



АДМИНИСТРАЦИЯ ГОРОДА ВЛАДИМИРА

НАЧАЛЬНИК УПРАВЛЕНИЯ ПО ОХРАНЕ ОКРУЖАЮЩЕЙ СРЕДЫ

ПРИКАЗ

30.12.2021

№ 48-н

**Об обращении со средствами криптографической защиты информации в управлении
по охране окружающей среды администрации города Владимира**

В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении 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», приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» **приказываю:**

1. Назначить ответственным за организацию работ по криптографической защите информации в управлении по охране окружающей среды администрации города Владимира начальника отдела экологии управления по охране окружающей среды администрации города Владимира Кириянова Евгения Александровича.

2. Утвердить:

2.1. Инструкцию по обращению со средствами криптографической защиты информации (СКЗИ) в управлении по охране окружающей среды администрации города Владимира (приложение № 1).

2.2. Инструкцию ответственного за организацию работ по криптографической защите информации в управлении по охране окружающей среды администрации города Владимира (приложение № 2).

2.3. Инструкцию пользователей средств криптографической защиты

информации в управлении по охране окружающей среды администрации города Владимира (приложение № 3).

2.4. Форму Перечня пользователей, допущенных к работе с СКЗИ в управлении по охране окружающей среды администрации города Владимира (приложение № 4).

2.5. Форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) в управлении по охране окружающей среды администрации города Владимира (приложение № 5).

2.6. Форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях и ключевых документов в управлении по охране окружающей среды администрации города Владимира (приложение №6).

3. Начальнику отдела экологии управления по охране окружающей среды администрации города Владимира:

3.1. Разместить настоящий приказ на официальном сайте органов местного самоуправления города Владимира в десятидневный срок с даты подписания приказа.

3.2. Ознакомить работников управления по охране окружающей среды администрации города Владимира с настоящим приказом под роспись.

4. Контроль за исполнением приказа оставляю за собой.



С.В. Сухопаров

Приложение № 1

УТВЕРЖДЕНО

приказом начальника управления
по охране окружающей среды

от 30.12.2021 № 48-н

ИНСТРУКЦИЯ

по обращению со средствами криптографической защиты информации (СКЗИ) в управлении по охране окружающей среды администрации города Владимира

1. Общие положения

1.1. Настоящая Инструкция по обращению со средствами криптографической защиты информации (СКЗИ) в управлении по охране окружающей среды администрации города Владимира (далее - Инструкция) разработана в целях регламентации действий сотрудников (работников) управления по охране окружающей среды администрации города Владимира (далее - Управление), допущенных к работе со средствами криптографической защиты информации (далее - СКЗИ), которые осуществляют работы с применением СКЗИ.

1.2. Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов другие действия согласно технической документации на СКЗИ.

1.3 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.

1.4. Данная Инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

1.5. 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 13.06.2001 № 152, Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66, а также Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 № 378.

2. Термины и определения

В целях настоящей Инструкции используются следующие основные термины и определения:

1) **информация ограниченного доступа** - информация, доступ к которой ограничен федеральными законами;

2) **исходная ключевая информация** - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

3) **ключевая информация** - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

4) **ключевой документ** - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию;

5) **ключевой носитель** - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации);

6) **компрометация** - 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;

7) **криптографический ключ (криптоключ)** - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

8) **орган криптографической защиты (ОКЗ)** - структурное подразделение Управления, сотрудник (работник) Управления или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлению мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа;

9) **ответственный за организацию работ по криптографической защите информации** - сотрудник (работник) Управления, отвечающий за реализацию мероприятий связанных с обеспечением в Управлении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа;

10) **персональный компьютер (ПК)** - вычислительная машина, предназначенная для эксплуатации пользователем Управления в рамках исполнения должностных обязанностей;

11) **пользователи СКЗИ** - сотрудники (работники) Управления,

непосредственно допущенные к работе с СКЗИ;

12) **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;

13) **электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. Порядок получения допуска пользователей к работе с СКЗИ

3.1. Для получения допуска к работе с СКЗИ, работнику необходимо пройти обучение правилам работы с СКЗИ и проверку знаний.

3.2. Основанием для допуска пользователя к работе с СКЗИ является внесение его в перечень пользователей СКЗИ, утверждаемый начальником Управления.

3.3. Контроль над реализацией данных мероприятий возлагается на ответственного за организацию работ по криптографической защите информации.

4. Работа с СКЗИ

4.1. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей в присутствии посторонних лиц запрещено. В Управлении должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

4.2. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть промаркированы и должны использоваться, учитываться и храниться в общем порядке. Все копии учитываются за отдельным номером.

4.3. Каждый ключевой документ должен быть зарегистрирован в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) в управлении по охране окружающей среды администрации города Владимира (далее - Журнал поэкземплярного учета СКЗИ).

4.4. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только с разрешения начальника

Управления с соответствующей пометкой в Журнале поэкземплярного учета СКЗИ.

4.5. При обнаружении на рабочей станции с установленным СКЗИ программного обеспечения, не соответствующего объему и сложности решаемых задач на данном рабочем месте, а также вирусных программ, незамедлительно должны быть организованы работы по расследованию инцидента информационной безопасности.

5. Действия в случае компрометации ключей

5.1. О событиях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать ответственному за организацию работ по криптографической защите информации.

5.2. К компрометации ключей относятся следующие события:

- 1) утрата носителей ключа;
- 2) утрата иных носителей ключа с последующим обнаружением;
- 3) возникновение подозрений на утечку ключевой информации или ее искажение;
- 4) нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура, опечатывания сейфов;
- 5) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
- 6) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
- 7) доступ посторонних лиц к ключевой информации;
- 8) другие события утери доверия к ключевой информации, согласно технической документации на СКЗИ.

5.3. В случае компрометации ключа пользователя незамедлительно должны быть приняты меры по отзыву ключа (отзыв ключа электронной подписи в удостоверяющем центре, обновление списков отозванных сертификатов, замена криптоключа пользователя и т.п.), а также проведено расследование по факту компрометации.

5.4. Визуальный осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

5.5. Расследование инцидентов информационной безопасности, связанных с компрометацией ключевых носителей и ключевой документацией, осуществляет (обладатель скомпрометированной информации ограниченного доступа). При необходимости, привлекается орган криптографической защиты.

6. Ответственность лиц, допущенных к работе с СКЗИ

За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 2

УТВЕРЖДЕНО

приказом начальника управления
по охране окружающей среды
от 30.12.2021 № 48-н

ИНСТРУКЦИЯ

ответственного за организацию работ по криптографической защите информации в управлении по охране окружающей среды администрации города Владимира

1. Общие положения

Настоящая Инструкция ответственного за организацию работ по криптографической защите информации в управлении по охране окружающей среды администрации города Владимира (далее - Инструкция) разработана в целях регламентации действия(й) лиц(а), ответственного(ых) за организацию работ по криптографической защите информации (далее - Ответственный), который(е) осуществляет(ют) работы с применением средств криптографической защиты информации (далее - 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 другие действия согласно технической документации на СКЗИ.

Ответственный назначается приказом начальника управления по охране окружающей среды администрации города Владимира (далее - Управление).

Данная Инструкция регламентирует работу с применением СКЗИ 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 13.06.2001 № 152, Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66, а также Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных

данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 № 378.

2. Термины и определения

В целях настоящей Инструкции используются следующие основные термины и определения:

1) **информация ограниченного доступа** - информация, доступ к которой ограничен федеральными законами;

2) **исходная ключевая информация** - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

3) **ключевая информация** - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

4) **ключевой документ** - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию;

5) **ключевой носитель** - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации);

6) **компрометация** - 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;

7) **криптографический ключ (криптоключ)** - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

8) **орган криптографической защиты (ОКЗ)** - структурное подразделение Управления, сотрудник (работник) Управления или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлению мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа;

9) **персональный компьютер (ПК)** - вычислительная машина, предназначенная для эксплуатации пользователем Управления в рамках исполнения должностных обязанностей;

10) **пользователи СКЗИ** - сотрудники (работники) Управления, непосредственно допущенные к работе с СКЗИ;

11) **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;

12) **электронная подпись** - информация в электронной форме, которая

присоединена к другой информации в электронной форме (подписываемой информацией) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. Обязанности Ответственного

3.1. При реализации мероприятий, связанных с обеспечением в Управлении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться действующим законодательством Российской Федерации, Инструкцией по обращению со средствами криптографической защиты информации (СКЗИ) в управлении по охране окружающей среды администрации города Владимира, а также настоящей Инструкцией.

3.2. На Ответственного возлагается проведение следующих мероприятий:

- 1) ведение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- 2) хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним;
- 3) принятие ключевых документов к СКЗИ от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- 4) своевременная актуализация перечня пользователей СКЗИ;
- 5) ежегодная проверка наличия СКЗИ, эксплуатационной и технической документации к ним, согласно Журналу поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) в управлении по охране окружающей среды администрации города Владимира.

3.3. Ответственный обязан:

- 1) не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключях;
- 2) обеспечивать сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;
- 3) обеспечить соблюдение требований к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
- 4) контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;
- 5) немедленно уведомлять непосредственного руководителя о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;
- 6) не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

4. Права Ответственного

В рамках исполнения возложенных на него обязанностей, Ответственный имеет право:

1) требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению со средствами криптографической защиты информации (СКЗИ) в управлении по охране окружающей среды администрации города Владимира и Инструкции пользователей средств криптографической защиты информации в управлении по охране окружающей среды администрации города Владимира;

2) обращаться к непосредственному руководителю с предложением прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

3) инициировать проведение служебных расследований по фактам нарушения в Управлении порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

5. Порядок передачи обязанностей при смене Ответственного

При смене Ответственного должны быть внесены соответствующие изменения в приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен под роспись с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

6. Ответственность за невыполнение настоящей Инструкции

За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 3

УТВЕРЖДЕНО

приказом начальника управления
по охране окружающей средыот 30.12.2021 № 48-н

ИНСТРУКЦИЯ

пользователей средств криптографической защиты информации в управлении по охране окружающей среды администрации города Владимира

1. Общие положения

1.1. Настоящая Инструкция пользователей средств криптографической защиты информации в управлении по охране окружающей среды администрации города Владимира (далее - Инструкция) разработана в целях регламентации действий сотрудников (работников) управления по охране окружающей среды администрации города Владимира (далее - Управление), допущенных к работам с использованием средств криптографической защиты информации (далее - Пользователи).

1.2. Под работами с применением средств криптографической защиты информации (далее - СКЗИ) в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и другие действия согласно технической документации на СКЗИ.

1.3. Данная Инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

1.4. 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 13.06.2001 № 152, Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66, а также Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 № 378.

2. Термины и определения

В целях настоящей Инструкции используются следующие основные термины и определения:

1) **информация ограниченного доступа** - информация, доступ к которой ограничен федеральными законами;

2) **исходная ключевая информация** - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

3) **ключевая информация** - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

4) **ключевой документ** - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию;

5) **ключевой носитель** - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации);

6) **компрометация** - 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;

7) **криптографический ключ (криптоключ)** - совокупность данных, обеспечивающая выбор одного - конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

8) **орган криптографической защиты (ОКЗ)** - структурное подразделение Управления, сотрудник (работник) Управления или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлении мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа;

9) **ответственный за организацию работ по криптографической защите информации** (далее - Ответственный) - сотрудник (работник) Управления, отвечающий за реализацию мероприятий, связанных с обеспечением в Управлении безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа;

10) **персональный компьютер (ПК)** - вычислительная машина, предназначенная для эксплуатации пользователем Управления в рамках исполнения должностных обязанностей;

11) **пользователи СКЗИ** - сотрудники (работники) Управления, непосредственно допущенные к работе с СКЗИ;

12) **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;

13) **электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. Обязанности Пользователей СКЗИ

Пользователи СКЗИ обязаны:

- 1) соблюдать конфиденциальность информации ограниченного доступа, к которой они допущены, в том числе сведения о криптоключях;
- 2) обеспечивать сохранность вверенных ключевых носителей и ключевой документации на них;
- 3) соблюдать требования безопасности информации ограниченного доступа при использовании СКЗИ;
- 4) незамедлительно сообщать Ответственному о ставших им известными попытках получения посторонними лицами доступа к сведениям об используемых СКЗИ, ключевым носителям и ключевой документации;
- 5) при увольнении или отстранении от исполнения обязанностей сдать Ответственному носители с ключевой документацией;
- 6) при подозрении на компрометацию ключевой документации, а также при обнаружении факта утраты или недостачи СКЗИ, ключевых носителей, ключевой документации, хранилищ, личных печатей незамедлительно уведомлять Ответственного.

Пользователям СКЗИ запрещается:

- 1) выводить ключевую информацию на средствах отображения информации (дисплей монитора, печатающие устройства, проекторы и т.п.);
- 2) оставлять ключевые носители с ключевой документацией без присмотра;
- 3) записывать на ключевой носитель информацию, не связанную с работой СКЗИ (текстовые и мультимедиа файлы, служебные файлы и т.п.);
- 4) вносить любые изменения в программное обеспечение СКЗИ.

4. Ответственность Пользователей СКЗИ

За нарушение установленных требований по эксплуатации криптосредств пользователь СКЗИ несет ответственность в соответствии с действующим законодательством Российской Федерации.

OT 30.12.2021 № 48-12

пользователей, допущенных к работе с СКЗИ в управлении по охране окружающей среды администрации города Владимира

УТВЕРЖДАЮ

Начальник управления
по охране окружающей среды

_____ / _____ /
_____ Г.

ПЕРЕЧЕНЬ

пользователей, допущенных к работе с СКЗИ в управлении по охране окружающей среды администрации города Владимира

[illegible]

Приложение № 5

УТВЕРЖДЕНО

приказом начальника управления
по охране окружающей среды
от 30.12.2021 № 48-п

ФОРМА ЖУРНАЛА
поэкземплярного учета СКЗИ, эксплуатационной
и технической документации к ним, ключевых документов
(для обладателя конфиденциальной информации)
в управлении по охране окружающей среды администрации города
Владимира

Лицевая сторона обложки журнала

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной
и технической документации к ним, ключевых документов
(для обладателя конфиденциальной информации)
в управлении по охране окружающей среды администрации города
Владимира

Срок хранения: _____
Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.
На _____ листах

Внутренняя сторона журнала

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатацион ной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографиче ские номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших подключение (установку)	Дата подключения (установки) и подписи лиц, производивших 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	
9	10	11	12	13	14	15

УТВЕРЖДЕНО

приказом начальника управления
по охране окружающей среды

от 30.12.2021 № 48-н

ФОРМА АКТА

об уничтожении криптографических ключей, содержащихся на ключевых носителях и ключевых документов в управлении по охране окружающей среды администрации города Владимира

AKT

об уничтожении криптографических ключей, содержащихся на ключевых носителях и ключевых документов в управлении по охране окружающей среды администрации города Владимира

г.Владимир

« » 20 г.

Настоящий Акт составлен в том, что комиссией в составе:

_____ - _____, председатель комиссии;
(фамилия, инициалы) (должность)

_____, заместитель председателя комиссии;
(фамилия, инициалы) (должность)

_____ - _____, секретарь комиссии;
(фамилия, инициалы) (должность)

Члены комиссии:

_____ - _____;
(фамилия, инициалы) (должность)

_____-_____
(фамилия, инициалы) (должность)

произведено уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров
1	2	3	4	5	6

Всего уничтожено ____ криптографических ключей на ____ ключевых носителях по адресу _____.

(место уничтожения)

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного

использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) в управлении по охране окружающей среды администрации города Владимира.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) в управлении по охране окружающей среды администрации города Владимира подтверждаю:

_____	_____	« ____ » _____ 20__ г.
(фамилия, инициалы председателя комиссии)	(подпись)	
_____	_____	« ____ » _____ 20__ г.
(фамилия, инициалы заместителя председателя комиссии)	(подпись)	
_____	_____	« ____ » _____ 20__ г.
(фамилия, инициалы секретаря комиссии)	(подпись)	
члены комиссии:		
_____	_____	« ____ » _____ 20__ г.
(фамилия, инициалы)	(подпись)	
_____	_____	« ____ » _____ 20__ г.
(фамилия, инициалы)	(подпись)	