

УТВЕРЖДЕНЫ
приказом департамента
информатизации и развития
телекоммуникационных технологий
Новосибирской области
от 18.04.2018 № 50-Д

**Методические рекомендации по учету и эксплуатации средств
криптографической защиты информации**

Оглавление

1. Общие положения	2
2. Получение СКЗИ.....	3
3. Документы по учету СКЗИ.....	4
4. Организация учета и использования СКЗИ	5
5. Эксплуатация СКЗИ.....	6
Акты приема-передачи СКЗИ, справочно-ключевых дистрибутивов СКЗИ (типовые формы)	7
Приказ о назначении ответственного за эксплуатацию СКЗИ (типовая форма)..	9
Инструкция по обеспечению безопасности эксплуатации СКЗИ (типовая форма)	10
Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (пример заполнения)	20
Журнал учета лиц, допущенных к работе с СКЗИ (типовая форма и пример заполнения).....	23
Журнал учета ключей от помещений, в которых размещены СКЗИ (типовая форма и пример заполнения).....	26
Журнал учета печатей (типовая форма и пример заполнения)	29
Журнал учета хранилищ СКЗИ (типовая форма и пример заполнения).....	31
Журнал учета журналов (типовая форма и пример заполнения)	33
Акт ввода в эксплуатацию СКЗИ (типовая форма и пример заполнения).....	35
Заключение о допуске пользователя СКЗИ к самостоятельной работе (типовая форма и пример заполнения).....	38
Акт об уничтожении СКЗИ	40
(типовая форма и пример заполнения)	40

1. Общие положения

Настоящие Методические рекомендации по учету и эксплуатации средств криптографической защиты информации (далее – Методические рекомендации) подготовлены на основании Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», постановления Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», приказа Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава 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», приказа Федеральной службы безопасности Российской Федерации от 01.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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».

В Методических рекомендациях рассматриваются учет и эксплуатация средств криптографической защиты информации (далее – СКЗИ), определенных п. 2 Положения, утвержденного постановлением Правительства Российской Федерации от 16.04.2012 № 313.

2. Получение СКЗИ

2.1. В государственных органах Новосибирской области, в областных исполнительных органах государственной власти Новосибирской области (далее – ОИОГВ), в подведомственных им учреждениях, в территориальных органах ОИОГВ, в органах местного самоуправления Новосибирской области (далее – ОМСУ) и подведомственных им учреждениях должны использоваться только СКЗИ, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации и имеющие сертификат ФСБ России.

2.2. ОИОГВ, ОМСУ, подведомственные им государственные и муниципальные учреждения, территориальные органы ОИОГВ, государственные органы Новосибирской области (далее – Организации) и приобретают право на использование СКЗИ следующими способами.

2.2.1. Приобретение СКЗИ у организации, имеющей лицензию на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) (далее – организация-лицензиат).

Документами, подтверждающими право использования СКЗИ, являются государственные и муниципальные контракты, договоры, сублицензионные договоры Организаций с организациями-лицензиатами.

Владельцем СКЗИ является Организация. Дистрибутивы и формуляры на СКЗИ хранятся у владельца СКЗИ.

2.2.2. Передача СКЗИ, приобретенных в рамках исполнения мероприятий Государственных программ Новосибирской области, на ответственное хранение и использование по договору безвозмездного временного пользования от областного исполнительного органа государственной власти Новосибирской области, уполномоченного на создание государственных информационных систем, формирование государственных информационных ресурсов и обеспечение доступа к информации о деятельности областных исполнительных органов государственной власти Новосибирской области (далее – уполномоченный орган), имеющего лицензию на деятельность, указанную в подпункте 2.2.1., либо от подведомственного уполномоченному органу государственного учреждения, являющегося организацией-лицензиатом.

Документами, подтверждающими право использования СКЗИ, являются договоры об ответственном хранении и использовании СКЗИ Организаций с

владельцем СКЗИ (с уполномоченным органом либо с подведомственным уполномоченному органу государственным учреждением, являющимся организацией-лицензиатом).

Дистрибутивы и формуляры на СКЗИ хранятся у владельца СКЗИ.

В этом случае Организация заключает Соглашение об обеспечении функционирования СКЗИ с подведомственным уполномоченным органу государственным учреждением, являющимся организацией-лицензиатом.

2.2.3. Получение СКЗИ Организациями как конечными потребителями от ОИОГВ и ОМСУ, которым они подведомствены, при закупке СКЗИ у организации-лицензиата для конечных потребителей.

Документами, подтверждающими право использования СКЗИ, являются государственные и муниципальные контракты, договоры, сублицензионные договоры ОИОГВ и ОМСУ, которым подведомствены конечные потребители, с организациями-лицензиатами, и акты приема-передачи СКЗИ, справочно-ключевых дистрибутивов СКЗИ между организацией-лицензиатом и конечным потребителем, которые рекомендуется оформлять в соответствии с приложением 1 к настоящим Методическим рекомендациям.

Владельцем СКЗИ является Организация. Дистрибутивы и формуляры на СКЗИ хранятся у владельца СКЗИ.

2.2.4. Получение СКЗИ от федеральных органов государственной власти и их территориальных органов в Новосибирской области, в Сибирском федеральном округе (далее – ФОИВ) на основании официального обращения соответствующего органа.

Документами, подтверждающими право использования СКЗИ, являются официальные обращения ФОИВ и акты приема-передачи СКЗИ, справочно-ключевых дистрибутивов СКЗИ.

В этом случае Организациям рекомендуется заключение с ФОИВ соглашения об обеспечении функционирования СКЗИ.

2.3. Организации при использовании СКЗИ должны иметь в наличии следующие документы:

- документ, подтверждающий право использования СКЗИ;
- техническая и эксплуатационная документация на СКЗИ;
- дистрибутив и формуляр на СКЗИ (в случаях, указанных в п.п.2.2.1., 2.2.3.) или Соглашение об обеспечении функционирования СКЗИ (в случае, указанном в п.п. 2.2.2., 2.2.4.).

3. Документы по учету СКЗИ

3.1. Организации при использовании СКЗИ оформляют следующие распорядительные документы и ведут журналы учета:

3.1.1. Приказ о назначении ответственного за эксплуатацию СКЗИ (типовая форма приведена в приложении 2 к Методическим рекомендациям);

3.1.2. Инструкция по обеспечению безопасности эксплуатации СКЗИ (типовая форма приведена в приложении 3 к Методическим рекомендациям);

3.1.3. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (по форме согласно

приложению 2 к Инструкции, утвержденной приказом ФАПСИ от 13.06.2001 № 152, пример заполнения приведён в приложении 4 к Методическим рекомендациям);

3.1.4. Журнал учета лиц, допущенных к работе со СКЗИ (типовая форма и пример заполнения приведены в приложении 5 к Методическим рекомендациям);

3.1.5. Журнал учета ключей от помещений, в которых размещены СКЗИ (типовая форма и пример заполнения приведены в приложении 6 к Методическим рекомендациям);

3.1.6. Журнал учета печатей (типовая форма и пример заполнения приведены в приложении 7 к Методическим рекомендациям);

3.1.7. Журнал учета хранилищ (типовая форма и пример заполнения приведены в приложении 8 к Методическим рекомендациям);

3.1.8. Журнал учета журналов (типовая форма и пример заполнения приведены в приложении 9 к Методическим рекомендациям);

3.1.9. Дело с материалами по СКЗИ, в которое приобщаются Инструкция по обеспечению безопасности эксплуатации СКЗИ, приказ о назначении ответственного за эксплуатацию СКЗИ, заключения о допуске пользователей к самостоятельной работе со СКЗИ, акты ввода в эксплуатацию СКЗИ, акты об уничтожении СКЗИ и другие документы по эксплуатации СКЗИ в Организации.

3.2. Инструкция по обеспечению безопасности эксплуатации СКЗИ (п. 3.1.2.) утверждается руководителем Организации. Формы журналов (п.п. 3.1.4-3.1.8) утверждаются приказом Организации.

4. Организация учета и использования СКЗИ

4.1. Ответственный за эксплуатацию СКЗИ, назначенный приказом руководителя Организации, обеспечивает учет СКЗИ в соответствии с Инструкцией по обеспечению безопасности эксплуатации СКЗИ, утвержденной приказом руководителя Организации на основании типовой инструкции, разработанной уполномоченным органом (далее – Инструкция).

4.2. Сотрудники Организации допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому руководителем Организации, после проведения инструктажа и оформления Заключения о допуске пользователя СКЗИ к самостоятельной работе. Ответственный за эксплуатацию СКЗИ ведет учет пользователей СКЗИ, знакомит пользователей СКЗИ с Инструкцией и фиксирует факт ознакомления в Листе ознакомления с Инструкцией. Пользователи СКЗИ обязаны соблюдать требования Инструкции.

4.3. Помещения, в которых используются СКЗИ (далее – спецпомещения), должны являться контролируемой зоной (пространством, в котором осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств). Границей контролируемой зоны могут быть периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, помещения.

Ключи от помещений, в которых используются СКЗИ, учитываются в журнале (п. 3.1.5).

Для помещений, в которых используются СКЗИ, руководителем Организации:

- утверждается перечень лиц, имеющих право доступа в помещение;
- организуется режим обеспечения безопасности, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в эти помещения;
- утверждаются правила доступа в помещения в рабочее и нерабочее время, а также во нештатных ситуациях.

5. Эксплуатация СКЗИ

5.1. Эксплуатация СКЗИ должна осуществляться в соответствии с документацией на СКЗИ и требованиями, установленными нормативными правовыми актами, регулирующими отношения в соответствующей области.

5.2. Допуск пользователей к работе со СКЗИ производится на основании заключения о допуске к самостоятельной работе со СКЗИ. Сведения о пользователе СКЗИ вносятся в Журнал учета лиц, допущенных к работе со СКЗИ (п. 3.1.4.).

Для использования сотрудником СКЗИ на средство вычислительной техники оформляются:

5.2.1. Акт ввода в эксплуатацию СКЗИ (типовая форма и пример заполнения приведены в приложении 10 к Методическим рекомендациям);

5.2.2. Заключение о допуске пользователя СКЗИ к самостоятельной работе (типовая форма и пример заполнения приведены в приложении 11 к Методическим рекомендациям).

Документы 5.2.1-5.2.2 оформляются организацией-лицензиатом ФСБ России.

5.3. Хранение СКЗИ, размещенных на отчуждаемых от средств вычислительной техники носителях (программно-аппаратные комплексы хранения ключевой информации и др.), должно осуществляться в запираемых и опечатываемых индивидуальных шкафах (сейфах, ячейках).

При отсутствии условий хранения таких СКЗИ в запираемых и опечатываемых индивидуальных шкафах (сейфах, ячейках) хранение осуществляется в индивидуальных опечатываемых колбах в запираемом индивидуальном шкафу (ячейке, ящике), находящихся в спецпомещении.

5.4. При выводе СКЗИ из эксплуатации оформляется Акт об уничтожении СКЗИ (типовая форма приведена в приложении 12 к Методическим рекомендациям) и делается соответствующая отметка в журнале поэкземплярного учета СКЗИ (п.3.1.3).

Приложение 1
к Методическим рекомендациям

Акты приема-передачи СКЗИ, справочно-ключевых дистрибутивов СКЗИ (типовые формы)

АКТ ПРИЁМА-ПЕРЕДАЧИ
(для линейки изделий ПК «ViPNet Client»)

№ _____ - _____

« _____ » _____ 20__ г.

Организация-лицензиат ФСБ России _____ (далее – Лицензиат), и _____ (далее – _____), составили и подписали настоящий Акт приёма-передачи о том, что Лицензиат передал, а _____ принял:

Наименование, товарный знак, марка (модель)	Ед. измерения	Кол-во	Серийный номер
CD-диск с ключевой информацией	шт.		

Передал:

/ _____

Принял:

/ _____

АКТ ПРИЁМА-ПЕРЕДАЧИ
(для линейки изделий ПАК «ViPNet Coordinator HW»)

№ _____ - _____

« ____ » _____ 20__ г.

Организация-лицензиат ФСБ России _____ (далее – Лицензиат), и
 _____ (далее – _____), составили и подписали настоящий Акт приёма-передачи
 о том, что Лицензиат передал, а _____ принял:

Наименование, товарный знак, марка (модель)	Ед. измерения	Кол-во	Серийный номер
CD-диск с ключевой информацией	шт.		
Изделие ПАК «ViPNet Coordinator HW», модификация изделия HW_____, аппаратная платформа HW____ Q_	шт.		Лицензионный номер ПАК: _____ Учетный номер СКЗИ: _____

Передал:

/ _____

Принял:

/ _____

Приложение 2
к Методическим рекомендациям

Приказ о назначении ответственного за эксплуатацию СКЗИ (типовая форма)

<НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ>

ПРИКАЗ

№

О назначении ответственного за эксплуатацию
средств криптографической защиты информации в <наименование
организации>

В связи с использованием средств криптографической защиты информации и иных шифровальных (криптографических) средств (далее – СКЗИ) в <наименование организации>, в целях обеспечения организации учета, хранения и эксплуатации СКЗИ, в соответствии с требованиями приказа ФСБ России от 01.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», «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,

приказываю:

1. Назначить <Фамилия Имя Отчество>, <должность>, ответственным за эксплуатацию СКЗИ в организации. Во время временного отсутствия обязанности ответственного за эксплуатацию СКЗИ возлагать на <Фамилия Имя Отчество>, <должность>.

2. Ответственному за эксплуатацию СКЗИ при организации учета, хранения и эксплуатации СКЗИ руководствоваться действующими нормативными правовыми актами и методическими документами по эксплуатации СКЗИ, эксплуатационной и технической документацией на СКЗИ.

3. Контроль за исполнением данного приказа оставляю за собой.

<Должность руководителя>

<И.О. Фамилия>

Приложение 3
к Методическим рекомендациям

Инструкция по обеспечению безопасности эксплуатации СКЗИ (типовая форма)

УТВЕРЖДАЮ

<Должность>

_____ <И.О. Фамилия>

« _____ » _____ 20__ г.

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации
средств криптографической защиты информации
в <наименование организации>

1. Термины и определения

1.1. В настоящей инструкции по обеспечению безопасности эксплуатации средств криптографической защиты информации в <наименование организации> (далее – Инструкция) применяются следующие термины и определения:

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

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;

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;

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);

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие процессы, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам;

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

Персональный компьютер (ПК) – вычислительная машина, предназначенная для эксплуатации пользователем в рамках исполнения должностных обязанностей.

Ответственный за эксплуатацию СКЗИ – сотрудник, осуществляющий организацию учета, хранения и эксплуатации СКЗИ, в том числе обеспечения работ по техническому обслуживанию СКЗИ и управлению криптографическими ключами;

Пользователи СКЗИ – сотрудники <наименование организации>, непосредственно допущенные к работе с СКЗИ.

2. Общие положения

2.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ и криптографических ключей, а также порядок изготовления, смены, уничтожения и действий сотрудников <наименование организации> (далее – Организация) при компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

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

2.3. Все действия с СКЗИ осуществляются в соответствии с эксплуатационной документацией на СКЗИ.

2.4. Организация использует сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

2.5. Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях следующих нормативных правовых актов:

- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказ 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»;
- Приказ ФСБ от 010.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- иные нормативные правовые акты и методические документы по эксплуатации шифровальных (криптографических) средств.

2.6. Для организации и обеспечения работ по учету, хранению и эксплуатации СКЗИ, в том числе работ по техническому обслуживанию СКЗИ и управлению криптографическими ключами приказом Организации назначается ответственный за эксплуатацию СКЗИ.

Ответственный за эксплуатацию СКЗИ осуществляет:

- поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;
- учет пользователей СКЗИ;
- контроль за соблюдением условий использования СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;
- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;
- разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

2.7. Обучение пользователей правилам работы с СКЗИ осуществляет ответственный за эксплуатацию СКЗИ.

2.8. Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на ответственного за эксплуатацию СКЗИ.

2.10. Ответственный за эксплуатацию СКЗИ и Пользователи должны быть ознакомлены с настоящей Инструкцией.

3. Порядок допуска пользователей к работе с СКЗИ

3.1. Перечень сотрудников, привлекаемых к работе с СКЗИ, утверждается приказом руководителя Организации.

3.2. Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами (п.2.5), данной инструкцией и проходит обучение правилам работы с СКЗИ, которое проводит ответственный за эксплуатацию СКЗИ.

3.3. Пользователь считается допущенным к СКЗИ после оформления Заключения о допуске пользователя СКЗИ к самостоятельной работе.

4. Учет СКЗИ, порядок ведения дел и журналов

4.1. СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

4.2. Поэкземплярный учет СКЗИ ведет ответственный за эксплуатацию СКЗИ в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним (далее – Журнал). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

4.3. Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптографических ключей, то его каждый раз следует регистрировать отдельно.

4.4. Ответственный за эксплуатацию СКЗИ ведет журналы:

4.4.1. Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

4.4.2. Журнал учета лиц, допущенных к работе с СКЗИ;

4.4.3. Журнал учета ключей от помещений, в которых размещены СКЗИ;

4.4.4. Журнал учета печатей;

4.4.5. Журнал учета хранилищ СКЗИ;

4.4.6. Журнал учета журналов.

Каждый журнал имеет собственную нумерацию, нумерованные листы; журнал должен быть сброшюрован и прошит, прошивка скреплена печатью. Журнал ведется до полного окончания, после чего:

- заводится следующий том журнала, при этом записи в разных томах журнала имеют сквозную нумерацию;

- на титульном листе законченного журнала заполняются сведения о завершении его ведения, журнал хранится у ответственного эксплуатации СКЗИ до передачи в архив в соответствии с номенклатурой дел Организации.

4.5. В Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов учитываются все используемые СКЗИ: установленные программные и программно-аппаратные СКЗИ, дистрибутивы СКЗИ, ключевые дистрибутивы СКЗИ и т.д. Для установленных программных и программно-аппаратных СКЗИ отметки о подключении (установке) проставляет организация, имеющая лицензию ФСБ России на данный вид деятельности, либо вписываются реквизиты акта ввода в эксплуатацию СКЗИ.

4.6. В Журнале учета лиц, допущенных к работе с СКЗИ в организации, при заполнении вносится перечень СКЗИ, к работе с которыми допущен пользователь на основании заключений о допуске пользователя СКЗИ к самостоятельной работе.

4.7. В Журнале учета ключей от помещений, в которых размещены СКЗИ, отражается первичная выдача ключа от помещения, в котором используются СКЗИ, возможная повторная выдача ключа (в случае смены замка и других обстоятельствах) и сдача ключа при увольнении сотрудника или смене должностных обязанностей.

Дубликаты ключей от помещений, в которых размещены СКЗИ, ответственный за эксплуатацию СКЗИ хранит в своем кабинете, в запираемом индивидуальном шкафу (ячейке, ящике). Дубликаты ключей должны быть помещены в конверты (пеналы), опечатанные сотрудниками, работающими в этих помещениях. Дубликат ключа от кабинета ответственного за эксплуатацию СКЗИ хранится у руководителя Организации.

4.8. Ответственный за эксплуатацию СКЗИ ведет дело с материалами по СКЗИ (далее – Дело), в которое приобщаются все документы по эксплуатации СКЗИ, кроме журналов:

- документы, подтверждающие право использования СКЗИ;
- акты ввода в эксплуатацию СКЗИ;
- заключения о допуске пользователя СКЗИ к самостоятельной работе;
- акты об уничтожении СКЗИ

и иные документы, связанные с эксплуатацией СКЗИ.

Приобщаемые в Дело материалы отражаются в описи, неотъемлемой части Дела, и нумеруются в хронологическом порядке поступления.

5. Хранение СКЗИ и криптографических ключей

5.1. Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под роспись в Журнале пользователям СКЗИ, несущим персональную ответственность за их сохранность.

5.2. При необходимости пользователю выдается документация по эксплуатации СКЗИ с последующим возвратом ответственному за эксплуатацию СКЗИ;

5.3. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у ответственного за эксплуатацию СКЗИ. Криптографические ключи хранятся у пользователей СКЗИ. Хранение осуществляется в закрываемых на замок металлических хранилищах пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение или в опечатанном пенале (тубусе). Металлические шкафы должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками и приспособлениями для опечатывания. Один экземпляр ключа от хранилища должен находиться у ответственного за эксплуатацию СКЗИ, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе.

5.4. Пользователи СКЗИ могут осуществлять хранение рабочих и резервных криптографических ключей, предназначенных для применения в случае неработоспособности рабочих криптографических ключей. Резервные криптографические ключи могут также находиться на хранении у ответственного за эксплуатацию СКЗИ.

5.5. На ключевые носители с изготовленными криптографическими ключами наклеиваются наклейки, содержащие надписи: на один ключевой носитель – «Рабочий»; на другой ключевой носитель – «Резервный».

5.6. Ключевой носитель с наклейкой «Резервный» помещается в конверт и опечатывается пользователем и ответственным за эксплуатацию СКЗИ.

5.7. Все полученные экземпляры криптографических ключей должны быть выданы под роспись в Журнале. Резервные криптографические ключи могут находиться на хранении у ответственного за эксплуатацию СКЗИ.

5.8. Ключевые носители с неработоспособными криптографическими ключами ответственный за эксплуатацию СКЗИ принимает от пользователя под роспись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

5.10. При необходимости замены наклейки на ключевом носителе (стирание надписи реквизитов) пользователь передает его ответственному за эксплуатацию СКЗИ, который в присутствии пользователя снимает старую наклейку и приклеивает новую наклейку с такими же учетными реквизитами.

5.10. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

На метке опечатывания проставляется номер, дата ее нанесения и подпись (или пломба с индивидуальными номерами) лица, проводившего опечатывание. Номер метки должен фигурировать в Акте ввода в эксплуатацию СКЗИ.

Опечатывание производит ответственный за эксплуатацию СКЗИ либо лицо, проводившее ввод в эксплуатацию СКЗИ:

- для СКЗИ, введенных в эксплуатацию до утверждения настоящей Инструкции, опечатывание может быть проведено ответственным за эксплуатацию СКЗИ;

- при вводе в эксплуатацию новых СКЗИ опечатывание производит лицо, которое проводит ввод в эксплуатацию СКЗИ.

5.11. СКЗИ и криптографические ключи могут доставляться специальной (фельдъегерской) связью или курьером, имеющим доверенность, подписанную руководителем Организации, на право получения СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и криптографическим ключам во время доставки.

5.12. Для пересылки СКЗИ и криптографические ключи помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптографические ключи персылают в отдельном пакете с пометкой «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения целостности упаковок и оттисков печати.

5.13. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей составляется Акт приема-передачи (Опись) документов, в котором указывается: что посылается и в каком количестве, учетные номера СКЗИ, криптографических ключей или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Акт приема-передачи (Опись) документов вкладывается в упаковку.

5.14. Полученную упаковку вскрывает только лицо, для которого она предназначена. Если содержимое полученной упаковки не соответствует указанному в Акте приема-передачи (Описи) документов или сама упаковка и оттиск печати - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то должен быть составлен акт о произшедшем нарушении. Полученные с такими отправлениями СКЗИ и криптографические ключи до получения указаний от руководителя Организации применять не разрешается.

5.15. При обнаружении бракованных криптографических ключей ключевой носитель с такими ключами следует возвратить для установления причин произошедшего и их устранения в дальнейшем. В этом случае необходимо получить новые криптографические ключи.

5.16. Ключевые носители совместно с Журналом должны храниться ответственным за эксплуатацию СКЗИ в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Журнал совместно с

другими документами, при этом ключевые носители и Журнал должны быть помещены в отдельную папку.

5.17. На время отсутствия ответственного за эксплуатацию СКЗИ должен быть назначен сотрудник его замещающий.

5.18. При необходимости криптографические ключи сдаются на временное хранение ответственному за эксплуатацию СКЗИ.

6. Использование СКЗИ и криптографических ключей

6.1. Криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

6.2. Криптографический ключ невозможно использовать, если истек срок действия.

6.3. Для обеспечения контроля доступа к СКЗИ системный блок ПЭВМ опечатывается ответственным за эксплуатацию СКЗИ.

6.4. Пользователь должен периодически проверять сохранность оборудования и целостность печатей на ПЭВМ. В случае обнаружения «посторонних» (незарегистрированных) программ или выявления факта повреждения печати на системном блоке ПЭВМ работа должна быть прекращена. По данному факту проводится служебное расследование и осуществляются работы по анализу и ликвидации последствий данного нарушения.

6.5. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному за эксплуатацию СКЗИ и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности носителей криптографических ключей ответственный за эксплуатацию СКЗИ выполняет в присутствии пользователя.

6.6. В случае, если рабочие криптографические ключи потеряли работоспособность, то по просьбе пользователя ответственный за эксплуатацию СКЗИ, вскрывает конверт (коробку) с резервными криптографическими ключами, делает копию ключевого носителя, используя резервные криптографические ключи, помещает резервные криптографические ключи в конверт (коробку), а на новый ключевой носитель наклеивает наклейку с надписью «Рабочий».

6.7. В экстренных случаях, не терпящих отлагательства, вскрытие конверта (коробки) с резервными криптографическими ключами может осуществляться комиссационно с последующим уведомлением ответственного за эксплуатацию СКЗИ о факте вскрытия конверта с криптографическими ключами. На конверте делается запись о вскрытии с указанием даты и времени вскрытия конверта и подписью пользователя. Вскрытый конверт вместе с неработоспособными криптографическими ключами сдаются ответственному за эксплуатацию СКЗИ.

6.8. Вскрытие системного блока ПЭВМ, на которой установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного за эксплуатацию СКЗИ.

7. Обязанности пользователей СКЗИ

7.1. Пользователи СКЗИ обязаны:

- не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
- сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
- соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
- сообщать сотруднику, ответственному за эксплуатацию СКЗИ, о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять сотрудника, ответственного за эксплуатацию СКЗИ, 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 сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

7.2. Пользователь несет ответственность за то, чтобы на ПК, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование СКЗИ. На ПК, оборудованном СКЗИ, программное обеспечение должно быть лицензионным.

7.3. При обнаружении на ПК, оборудованном СКЗИ, посторонних программ или вирусов, работа с СКЗИ на данном рабочем месте должна быть прекращена. Незамедлительно организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

7.4. Все полученные обладателем информации ограниченного доступа экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

7.5. Не допускается:

- разглашать информацию ограниченного доступа, к которой был допущен Пользователь СКЗИ;
- разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;
- выводить ключевую информацию на дисплей и(или) принтер;
- вставлять ключевой носитель в порт ПК при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в порты других ПК;
- записывать на ключевом носителе постороннюю информацию;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

7.6. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать ответственному за эксплуатацию СКЗИ.

8. Действия при компрометации криптографических ключей

8.1. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, но не ограничивающим их, относятся следующие:

- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами;
- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами с последующим их обнаружением;
- увольнение сотрудников, имевших доступ к рабочим и/или резервным криптографическим ключам;
- возникновение подозрений относительно утечки информации или ее искажения;
- нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с рабочими и/или резервными криптографическими ключами, если используется процедура опечатывания сейфов;

- утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами;
- временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

8.2. В случае возникновения обстоятельств, указанных в п. 7.1 настоящей Инструкции, пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей/ключей электронной подписи, по телефону информировать о факте компрометации используемых закрытых криптографических ключей/ключей электронной подписи:

- ответственного за эксплуатацию СКЗИ;
- организацию, от которой получены СКЗИ.

8.3. Решение о компрометации криптографических ключей принимает руководитель Организации на основании письменного уведомления о компрометации, подписанного ответственным за эксплуатацию СКЗИ, с приложением, при необходимости, письменного объяснения пользователя по факту компрометации его криптографических ключей.

8.4. Уведомление должно содержать:

- идентификационные параметры скомпрометированного криптографического ключа;
- фамилию, имя, отчество пользователя СКЗИ, который владел скомпрометированным криптографическим ключом;
- сведения об обстоятельствах компрометации криптографического ключа;
- время и обстоятельства выявления факта компрометации криптографического ключа.

8.5. После принятия решения о компрометации ключа принимаются меры о его изъятии из обращения и замены его на новый. Ответственный за эксплуатацию СКЗИ после получения информации о компрометации криптографического ключа, убеждается в достоверности полученной информации, выводит из действия сертификат ключа проверки электронной подписи, соответствующий скомпрометированному закрытому криптографическому ключу/ключу электронной подписи (прекращает обмен электронными документами с использованием сертификата ключа проверки электронной подписи, соответствующего скомпрометированному закрытому криптографическому ключу/ключу электронной подписи). Проводит работу по отзыву сертификата ключа подписи пользователя. Отозванный сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу пользователя/ключу электронной подписи, помещается в список отзываемых сертификатов.

8.6. Дата, начиная с которой сертификат ключа подписи считается недействительным, устанавливается равной дате формирования списка отзываемых сертификатов, в который был включен отзываемый сертификат ключа подписи.

8.7. Сертификат ключа подписи, соответствующий скомпрометированному закрытому криптографическому ключу/ключу электронной подписи, должен храниться ответственным за эксплуатацию СКЗИ в течение срока хранения электронных документов для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

8.8. Для симметричного закрытого криптографического ключа, используемого для шифрования/дешифрования информации вне инфраструктуры открытых ключей (не имеющего сертификата) после принятия решения о компрометации ключа принимаются меры о его изъятии из обращения и замены его на новый. Ответственный за эксплуатацию СКЗИ после получения информации о компрометации такого закрытого криптографического ключа, убеждается в достоверности полученной информации и обеспечивает смену (увеличение) его варианта.

8.9. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

10. Уничтожение криптографических ключей

10.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

10.2. Уничтожение криптографических ключей на ключевых носителях производится ответственным за эксплуатацию СКЗИ.

10.3. Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

10.4. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:

- установить наличие оригинала и количество копий криптографических ключей;
- проверить внешним осмотром целостность каждого ключевого носителя;
- установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в Журнале поэкземплярного учета;
- убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;
- произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

10.5. В Журнале поэкземплярного учета ответственным за эксплуатацию СКЗИ производится отметка об уничтожении криптографических ключей.

10. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи

10.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи (далее – режимные помещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.

10.2. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

10.3. Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

10.4. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

10.5. Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливает ответственный за эксплуатацию СКЗИ. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции.

10.6. Двери режимных помещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.

10.7. Для предотвращения просмотра извне помещений, где используются СКЗИ, окна должны быть защищены или экраны мониторов должны быть повернуты в противоположную сторону от окна.

10.8. Помещения, в которых используются при работе криптографические ключи, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Сотрудникам, ответственным за охрану здания, необходимо проверять периодически исправность сигнализации с отметкой в соответствующих журналах.

10.10. В обычных условиях помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или ответственным за эксплуатацию СКЗИ или комиссионно сотрудниками с разрешения руководителя Организации.

10.10. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководителю Организации и ответственному за эксплуатацию СКЗИ. Ответственный за эксплуатацию СКЗИ должен оценить возможность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствий компрометации криптографических ключей и к их замене.

10.11. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптографических ключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

10.12. На время отсутствия пользователей указанное оборудование, при наличии такой возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным за эксплуатацию СКЗИ необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

С настоящей инструкцией ознакомлены:

Ответственный за эксплуатацию СКЗИ

(дата)

(подпись)

(фамилия, инициалы)

Пользователи СКЗИ

(дата)

(подпись)

(фамилия, инициалы)

Приложение 4
к Методическим рекомендациям

Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов
(пример заполнения)

Журнал

поэкземплярного учета СКЗИ, эксплуатационной и технической

документации к ним, ключевых документов

в департаменте информатизации и развития телекоммуникационных технологий

Новосибирской области

Том № _____

Журнал (том) начал «____» _____ 20__ г.

Должность

_____ / _____
подпись фамилия, имя, отчество

Журнал (том) завершен «____» _____ 20__ г.

Должность

_____ / _____
подпись фамилия, имя, отчество

Журнал (том) составлен на _____ листах

Н пп	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатаци- онной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптогра- фические 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
1	Дистрибутив СКЗИ ViPNet Client 4 на CD-диске	Client: 782-036254 CSP: 637АЛ-051384	КлКс2-4-053538	ФГУП «НТЦ Атлас»	25.06.2012 акт приема-передачи № 555	Иванов И.И.	25.06.2012 подпись
2	Формуляр ФРКУ.00004-04-30 01 ФО	-	-	ФГУП «НТЦ Атлас»	25.06.2012 акт приема-передачи № 555	Иванов И.И.	25.06.2012 подпись
3	Справочно-ключевой дистрибутив abn_14aa.dst на CD-диске	6/0217	1	Департамент информатизации и развития телекоммуникационных технологий Новосибирской области	15.02.2017 акт приема-передачи № 1802-14	Иванов И.И.	15.02.2017 акт приема- передачи № 1802-14
4	ПК ViPNet Client 3.1	Client: 782-036254 CSP: 637АЛ-051384	КлКс2-4-053538	ФГУП «НТЦ Атлас»	25.06.2012 акт приема-передачи № 555	Петров П.П.	23.02.2017 акт приема- передачи № 2302-3
5	Ключ ЭП на носителе Rutooken (Etoken, USB-flash)	123456 (серийный номер носителя)	CG878K (серийный номер сертификата)	РУЦ НСО / УФК по НСО	20.08.2017 акт № 2008-34/ изготовлен самостоятельно	Иванов И.И.	20.08.2017 акт приема- передачи № 2008-34/ подпись
6	Дистрибутив КриптоПро CSP 4.0 на CD-диске	385С1-001146	10699	Управление Федерального Казначейства по Новосибирской области	12.12.2013 акт № 995	Иванов И.И.	12.12.2013 подпись
7	ПК КриптоПро CSP 4.0	385С1-001146	10699	Управление Федерального Казначейства по Новосибирской области	12.12.2013 акт № 995	Иванов И.И.	12.12.2013 подпись
8	ViPNet Coordinator HW-100C	780-005530	-	Департамент информатизации и развития телекоммуникационных технологий Новосибирской области	Договор ответственного хранения от... № ... либо № акта приема- передачи	ответственный за эксплуатацию СКЗИ	Дата и подпись

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, 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)	
9	10	11	12	13	14	15
не заполняется	не заполняется	не заполняется	26.07.2015	Петров П.П. Иванов И.И.	акт № 777 или подписи	
не заполняется	не заполняется	не заполняется	26.07.2015	Петров П.П. Иванов И.И.	акт № 777 или подписи	
Петров П.П.	23.02.2017 акт ввода в эксплуатацию № 2302-3 или подпись	C2J945015A	16.02.2017	Петров П.П. Иванов И.И.	акт № 55 или подписи	
Петров П.П.	23.02.2017 акт ввода в эксплуатацию № 2302-3 или подпись	C2J945015A	26.07.2015	Петров П.П. Иванов И.И.	акт № 777 или подписи	
Иванов И.И.	Подпись	C2J945015A	30.08.2017	Иванов И.И.	Заявление от 01.08.2017 № 63- 12/32-Вн или подпись	
Петров П.П.	23.02.2017 акт ввода в эксплуатацию № 2302-3 или подпись	C2J945015A	16.02.2017	Петров П.П. Иванов И.И.	акт № 57 или подписи	
Петров П.П.	23.02.2017 акт ввода в эксплуатацию № 2302-3 или подпись	C2J94123A21	16.02.2017	Петров П.П. Иванов И.И.	акт № 58 или подписи	
Петров П.П.	28.02.2017 акт ввода в эксплуатацию № 2802-10	062-18107	26.07.2017	Петров П.П. Иванов И.И.	акт № 59	

Приложение 5
к Методическим рекомендациям

Журнал учета лиц, допущенных к работе с СКЗИ (типовая форма и пример заполнения)

Журнал

учета лиц, допущенных к работе с СКЗИ в Организации

Том № _____

Журнал (том) начат «____» _____ 20____ г.

Должность

_____ / _____ /
подпись *фамилия, имя, отчество*

Журнал (том) завершен «____» _____ 20____ г.

Должность

_____ / _____ /
подпись *фамилия, имя, отчество*

Журнал (том) составлен на _____ листах

№ п/п	Ф.И.О. и должность допущенного к работе с СКЗИ	Наименование СКЗИ	Дата (номер) Заключения о допуске пользователя	Дата и номер приказа о прекращении допуска
1	2	3	4	5
1.	Егоров Е.Е., консультант отдела информационной безопасности	ViPNet Client 3.2	от 01.02.2015 № 21	от 23.06.2016 № 12
2.				

Приложение 6
к Методическим рекомендациям

Журнал учета ключей от помещений, в которых размещены СКЗИ (типовая форма и пример заполнения)

Журнал
учета ключей в Организации

Том № _____
Журнал (том) начат «____» _____ 20____ г.

Должность
_____ / _____
подпись фамилия, имя, отчество

Журнал (том) завершен «____» _____ 20____ г.

Должность
_____ / _____
подпись фамилия, имя, отчество

Журнал (том) составлен на _____ листах

№ п/п	№ каб.	№ ключа	Дата и время выдачи	ФИО, подпись получателя ключа	ФИО, подпись выдавшего ключ	Дата и время сдачи	Подпись сдавшего ключ	Подпись принявшег о ключ	Примечание
1	2	3	4	5	6	7	8	9	10
1.	10	1	01.08.2013, 10:00	Иванов Иван Иванович	Сидоров Савелий Семенович	14.12.2015			В связи с переводом в другой отдел
2.	10	2	22.01.2016, 12:40	Петров Петр Петрович	Сидоров Савелий Семенович				
3.	10	3	05.05.2011	Сидоров Савелий Семенович	Мишин Михаил Михайлович				Опечатан печатью Иванова И.И. № 333
4.	11	1	10.01.2010	Сидоров Савелий Семенович	Мишин Михаил Михайлович				
5.	11	2	10.01.2010	Мишин Михаил Михайлович	Мишин Михаил Михайлович				Опечатан печатью Сидорова С.С. № 2

* Сидоров Савелий Семенович – ответственный за эксплуатацию СКЗИ.

Хранит в своем кабинете, в запираемом индивидуальном шкафу (ячейке, ящике) ключи от помещений Организации, в которых используются СКЗИ, в конвертах, опечатанных указанными в графе 10 сотрудниками; дубликат ключа от кабинета ответственного за эксплуатацию СКЗИ хранится у руководителя Организации Мишина Михаила Михайловича.

В журнале отражается первичная выдача ключа от помещения, в котором используются СКЗИ, и сдача ключа при увольнении сотрудника или смене должностных обязанностей

Приложение 7
к Методическим рекомендациям

Журнал учета печатей (типовая форма и пример заполнения)

Журнал
учета печатей в Организации

Том № _____
Журнал (том) начат «____» _____ 20____ г.
Должность _____ / _____ /
подпись _____ фамилия, имя, отчество _____
Журнал (том) завершен «____» _____ 20____ г.
Должность _____ / _____ /
подпись _____ фамилия, имя, отчество _____
Журнал (том) составлен на _____ листах

№ п/п	№ печати	Дата и время выдачи	ФИО и подпись получателя печати	ФИО и подпись выдавшего печать	Дата и время сдачи	ФИО и подпись забравшего печать
1	2	3	4	5	6	7

№ п/п	№ печати	Дата и время выдачи	ФИО и подпись получателя печати	ФИО и подпись выдавшего печать	Дата и время сдачи	ФИО и подпись забравшего печать
1	2	3	4	5	6	7
1.	2	10.10.2014 14:01	Егоров Е.Е..	Абрамов А.А.	10.11.2016 14:02	Абрамов А.А.

Приложение 8
к Методическим рекомендациям

Журнал учета хранилищ СКЗИ (типовая форма и пример заполнения)

Журнал
учета хранилищ в Организации

Том № _____
Журнал (том) начат «____» _____ 20____ г.
Должность _____ / _____ / _____
подпись _____ фамилия, имя, отчество _____

Журнал (том) завершен «____» _____ 20____ г.
Должность _____ / _____ / _____
подпись _____ фамилия, имя, отчество _____

Журнал (том) составлен на _____ листах

Приложение 9
к Методическим рекомендациям

Журнал учета журналов (типовая форма и пример заполнения)

Журнал
учета журналов в Организации

Том № _____
Журнал (том) начат «____» _____ 20____ г.
Должность _____ / _____ /

подпись *фамилия, имя, отчество*

Журнал (том) завершен «____» _____ 20____ г.

Должность _____ / _____ /

подпись *фамилия, имя, отчество*

Журнал (том) составлен на _____ листах

Приложение 10
к Методическим рекомендациям

Акт ввода в эксплуатацию СКЗИ (типовая форма и пример заполнения)

**Акт
ввода в эксплуатацию средства криптографической защиты информации
(форма для программного СКЗИ)**

« » 20 г.

Настоящий акт составлен о том, что сотрудником *Организация-лицензиат ФСБ России* была проведена установка и настройка средства криптографической защиты информации:

Наименование СКЗИ.

Наименование организации:

Адрес _____
Помещение № _____

Характеристики помещения	Да	Нет
помещение находится в пределах контролируемой зоны		
помещение оборудовано прочной входной дверью с замками		
помещение оснащено охранной сигнализацией		
помещение оснащено пожарной сигнализацией		
окна помещения защищены от просмотра извне.		
исключена возможность неконтролируемого проникновения или пребывания в помещении посторонних лиц		

Изделие *Наименование программного СКЗИ*:

- серийный номер системного блока _____
- регистрационный номер СКЗИ _____
- учетный номер средства электронной подписи _____

размещено на аппаратном средстве (№ системного блока): _____

и в соответствии с эксплуатационной и технической документацией на *Наименование программного СКЗИ* введено в эксплуатацию.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы), место опечатывания (опломбирования) возможно контролировать визуально, номер(а) печати(ей) (пломбира(ов)): _____

Дистрибутив средства криптографической защиты информации *Наименование СКЗИ* учтен в *Наименование подразделения по криптозащите* по адресу *Адрес, кабинет*.

Первичный инструктаж по использованию средства криптографической защиты информации проведен со специалистом:

(должность)

(фамилия, имя, отчество)

Пользователь средства криптографической защиты информации

Представитель *Организации-лицензиата ФСБ России*

должность

должность

Фамилия И.О.

Фамилия И.О.

(подпись)

(ФИО)

(подпись)

(ФИО)

ввода в эксплуатацию средства криптографической защиты информации
(форма для программно-аппаратного СКЗИ)

« » 20 г.

Настоящий акт составлен о том, что сотрудником *Организация-лицензиат ФСБ России* была проведена установка и настройка средства криптографической защиты информации:

Наименование СКЗИ.

Наименование организации:

Адрес _____
Помещение № _____

Характеристики помещения	Да	Нет
помещение находится в пределах контролируемой зоны		
помещение оборудовано прочной входной дверью с замками		
помещение оснащено охранной сигнализацией		
помещение оснащено пожарной сигнализацией		
окна помещения защищены от просмотра извне.		
исключена возможность неконтролируемого проникновения или пребывания в помещении посторонних лиц		

Изделие *Наименование программно-аппаратного СКЗИ*:

- исполнение: _____
- аппаратная платформа: _____
- серийный номер системного блока _____
- учетный номер СКЗИ _____

и в соответствии с эксплуатационной и технической документацией на *Наименование программного СКЗИ* введено в эксплуатацию.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы), место опечатывания (опломбирования) возможно контролировать визуально, номер(а) печати(ей) (пломбира(ов)): _____

Первичный инструктаж по использованию средства криптографической защиты информации проведен со специалистом:

(должность)

(фамилия, имя, отчество)

Пользователь средства криптографической защиты информации

Представитель *Организации-лицензиата ФСБ России*

должность

должность

Фамилия И.О.

(подпись)

(ФИО)

Фамилия И.О.

(подпись)

(ФИО)

Акт
ввода в эксплуатацию средства криптографической защиты информации
(пример заполнения)

« 28 » июня 2017 г.

Настоящий акт составлен о том, что сотрудником департамента информатизации и развития телекоммуникационных технологий Новосибирской области была проведена установка и настройка средства криптографической защиты информации:

VIPNet Client 4.3.2.37273.

Наименование организации: Государственное бюджетное учреждение Новосибирской области «Центр информационных технологий Новосибирской области»

Адрес г. Новосибирск, ул. Красный проспект, д. 18
Помещение № 11

Характеристики помещения	Да	Нет
помещение находится в пределах контролируемой зоны		
помещение оборудовано прочной входной дверью с замками		
помещение оснащено охранной сигнализацией		
помещение оснащено пожарной сигнализацией		
окна помещения защищены от просмотра извне.		
исключена возможность неконтролируемого проникновения или пребывания в помещении посторонних лиц		

Состав ViPNet Client 4.3.2.37273.:

- серийный номер системного блока XYZ123JKS2
- регистрационный номер СКЗИ 782-027266
- учетный номер СКЗИ ViPNet CSP: 782-027267

размещено на аппаратном средстве (№ системного блока): 07955800036

и в соответствии с эксплуатационной и технической документацией на ПК ViPNet Client и СКЗИ ViPNet CSP 4.2 введено в эксплуатацию.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы), место опечатывания (опломбирования) возможно контролировать визуально, номер(а) печати(ей) (пломбира(ов)): 2

Дистрибутив средства криптографической защиты информации ViPNet Client 4.3.2.37273 учтен в отделе информационной безопасности ДИиРТТ НСО по адресу г. Новосибирск, Красный проспект 18, кабинет 541А.

Первичный инструктаж по использованию средства криптографической защиты информации проведен со специалистом:

эксперт 1 категории отдела технической поддержки
(должность)

Исупов Павел Павлович
(фамилия, имя, отчество)

Пользователь средства криптографической защиты информации

Представитель Департамента информатизации и развития телекоммуникационных технологий НСО

эксперт 1 категории

консультант отдела ИБ

(подпись)

(ФИО)

Исупов П.П.

Егоров Е.Е.

(подпись)

(ФИО)

Приложение 11
к Методическим рекомендациям

Заключение о допуске пользователя СКЗИ к самостоятельной работе (типовая форма и пример заполнения)

УТВЕРЖДАЮ
Руководитель учреждения
_____ И.О. Фамилия
_____ дата

ЗАКЛЮЧЕНИЕ

о допуске пользователя СКЗИ к самостоятельной работе

Пользователь СКЗИ <ФИО>, <должность>, <организация/структурное подразделение> в соответствии с Инструкцией 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 при использовании СКЗИ <Наименование СКЗИ> обязуется:

- не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе, сведения о криптоключах;
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать в орган криптографической защиты о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), 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.

Заключение: к самостоятельной работе с СКЗИ <Наименование СКЗИ> допущен

С заключением ознакомлен (а):

Представитель организации-лицензиата ФСБ России¹:

(подпись пользователя)

(фамилия, инициалы)

(фамилия, инициалы)

¹ организации, имеющей лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств...

УТВЕРЖДАЮ
Руководитель ГБУ НСО «ЦИТ НСО»
А.И. Лошаков
28.06.2017

Пользователь СКЗИ Исупов Павел Павлович, эксперт 1 категории отдела технической поддержки государственного бюджетного учреждения Новосибирской области «Центр информационных технологий Новосибирской области», в соответствии с Инструкцией 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 при Президенте РФ от 13.06.2001 № 152 при использовании СКЗИ ViPNet Client 4 обязуется:

- не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе, сведения о криптоключах;
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать в орган криптографической защиты о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), 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.

Заключение: к самостоятельной работе с СКЗИ ViPNet Client 4 допущен

С заключением ознакомлен (а): _____ / Исупов П.П.
 (подпись обучавшегося) _____ (фамилия, инициалы)

Представитель департамента
информатизации и развития
телекоммуникационных
технологий Новосибирской области:

_____ Егоров Е.Е.
 (подпись) _____ (ФИО)

Приложение 12
к Методическим рекомендациям

Акт об уничтожении СКЗИ
(типовая форма и пример заполнения)

АКТ
об уничтожении средств криптографической защиты информации
(форма)

« » 20 г.

№ _____

Настоящий акт составлен о том, что перечисленные в нем СКЗИ уничтожены с предварительным стиранием программного обеспечения СКЗИ и произведено стирание информации (которая может оставаться в устройствах памяти оборудования, в принтерах, сканерах)

№ 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	Номер аппаратного средства
1				

Регистрационные данные на СКЗИ сверены с записями в настоящем Акте, уничтожение СКЗИ выполнено способом их стирания (разрушения) с использованием утилиты Clean.exe в соответствии с требованиями эксплуатационной и технической документации

Узлы и детали аппаратных средств передать для дальнейшей эксплуатации.

Пользователь СКЗИ:

_____ (подпись пользователя)

_____ (фамилия, инициалы)

Представитель *организации-лицензиата ФСБ России*²:

_____ (подпись пользователя)

_____ (фамилия, инициалы)

Отметку об уничтожении ключевых носителей, ключевых документов в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним произвел: _____

_____ (должность, фамилия, инициалы подпись, дата)

² организации, имеющей лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств...

АКТ
об уничтожении средств криптографической защиты информации
(пример заполнения)

«28» июня 2017 г.

№ 2806-1

Настоящий акт составлен о том, что перечисленные в нем СКЗИ уничтожены с предварительным стиранием программного обеспечения СКЗИ и произведено стирание информации (которая может оставаться в устройствах памяти оборудования, в принтерах, сканерах)

№ 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	Номер аппаратного средства
1	ViPNet Client 4	782-027266	1	12171X51002

Регистрационные данные на СКЗИ сверены с записями в настоящем Акте, уничтожение СКЗИ выполнено способом их стирания (разрушения) с использованием утилиты Clean.exe в соответствии с требованиями эксплуатационной и технической документации

Узлы и детали аппаратных средств передать для дальнейшей эксплуатации.

Пользователь СКЗИ:

/ Исупов П.П.

Представитель *организации-лицензиата ФСБ России*³:

(подпись пользователя) / (фамилия, инициалы)
 Егоров Е.Е.
 (подпись пользователя) (фамилия, инициалы)

Отметку об уничтожении ключевых носителей, ключевых документов в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним произвел: Егоров Е.Е. 28.06.2017г.
 (должность, фамилия, инициалы подпись, дата)

³ организации, имеющей лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств...