АДМИНИСТРАЦИЯ НОВОСИБИРСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ

# РАСПОРЯЖЕНИЕ

05.12.2024 г. г.Новосибирск № 418-ра

## Об организации работы со средствами криптографической защиты информации в администрации Новосибирского района Новосибирской области

В целях обеспечения организации учета, хранения и эксплуатации средств криптографической защиты информации, применяемых в администрации Новосибирского района Новосибирской области:

1. Назначить ответственным за эксплуатацию средств криптографической защиты информации (далее – СКЗИ) в администрации Новосибирского района Новосибирской области заместителя главы администрации - начальника управления организационно-контрольной работы администрации Новосибирского района Новосибирской области Полевую И.А.

2. Утвердить:

- Правила эксплуатации СКЗИ в администрации Новосибирского района Новосибирской области (Приложение 1);
- Инструкцию ответственного за эксплуатацию СКЗИ в администрации Новосибирского района Новосибирской области (Приложение 2);
- Инструкцию пользователя СКЗИ в администрации Новосибирского района Новосибирской области, согласно (Приложение 3);
- Типовую форму Перечня лиц, допущенных к работе со СКЗИ в администрации Новосибирского района Новосибирской области (Приложение 4);
- Порядок доступа в помещения, в которых ведется обработка персональных данных и размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях (Приложение 5);
- Типовую форму Перечня лиц, имеющих доступ в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (Приложение 6).

3. Начальнику отдела контрольной работы – общественной приемной Главы Новосибирского района Новосибирской области управления организационно-контрольной работы администрации Новосибирского района Новосибирской области Митюшкиной А.Н. ознакомить работников администрации Новосибирского района Новосибирской области с настоящим распоряжением.

4. Контроль за исполнением распоряжения возложить на заместителя главы администрации - начальника управления организационно-контрольной работы администрации Новосибирского района Новосибирской Полевую И.А.

Глава района А.Г.Михайлов

ПРИЛОЖЕНИЕ № 1
к распоряжению администрации
Новосибирского района
Новосибирской области
от 05.12.2024 № 413-ра

# ПРАВИЛА
## эксплуатации средств криптографической защиты информации в администрации Новосибирского района Новосибирской области

### 1. Общие положения

1.1. Настоящие Правила эксплуатации средств криптографической защиты информации в администрации Новосибирского района Новосибирской области (далее – администрация) определяют порядок учета, хранения, использования, ввода в эксплуатацию, вывода из эксплуатации и уничтожения средств криптографической защиты информации (далее также – СКЗИ, криптосредства), а также порядок действий сотрудников администрации при компрометации криптографических ключей в целях обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием СКЗИ.

1.2. В настоящих Правилах применяются следующие термины и определения:

- информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;
- 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;
- криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;
- закрытый ключ – криптоключ, который хранится пользователем системы в тайне;
- ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;
- исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей;
- 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 происшествия, связанные с криптоключами и ключевыми

носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам;

- 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 администрации, непосредственно допущенные к работе с СКЗИ;

- контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств, границей контролируемой зоны может быть: периметр охраняемой территории, ограждающие конструкции охраняемого здания, охраняемой части здания;

- спецпомещения – помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

1.3. К криптографическим (шифровальным) средствам защиты информации, включая документацию на эти средства, относятся:

- средства шифрования – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

- средства имитозащиты – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

- средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций, создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

- средства кодирования – средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

- средства изготовления ключевых документов – аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

- ключевые документы – электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических)

средствах;

- аппаратные шифровальные (криптографические) средства – устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

- программные шифровальные (криптографические) средства – программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

- программно-аппаратные шифровальные (криптографические) средства – устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

1.4. Настоящие Правила в своем составе, терминах и определениях основываются на положениях следующих нормативных правовых актов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- Приказ ФСБ России 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» (далее – Приказ ФСБ России от 10.07.2014 № 378);

- 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»;

- иные нормативные правовые акты и методические документы по эксплуатации шифровальных (криптографических) средств.

1.5. В администрации должны использоваться только СКЗИ, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации и имеющие сертификат ФСБ России.

1.6. Класс СКЗИ определяется в соответствии с Приказом ФСБ России от 10.07.2014 № 378, а также иными нормативными правовыми актами по эксплуатации шифровальных (криптографических) средств.

1.7. Для организации и обеспечения работ по учету, хранению и эксплуатации СКЗИ приказом назначается ответственный за эксплуатацию СКЗИ.

## 2. Порядок допуска пользователей к работе с СКЗИ

2.1. При установке СКЗИ ответственным за эксплуатацию СКЗИ оформляется Акт ввода СКЗИ в эксплуатацию по форме согласно Приложению 1 к настоящим Правилам.

2.2. Для работы с СКЗИ допускаются сотрудники администрации, включенные в Перечень лиц, допущенных к работе со средствами криптографической защиты информации.

2.3. Перечень лиц, допущенных к работе со средствами криптографической защиты информации, утверждается распоряжением администрации.

2.4. Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами по эксплуатации СКЗИ, локальными актами администрации по вопросам эксплуатации СКЗИ, данными Правилами и проходит инструктаж по правилам работы с СКЗИ.

2.5. Инструктаж по правилам работы с СКЗИ и оформление Заключения о допуске пользователя СКЗИ к самостоятельной работе осуществляют ответственный за эксплуатацию СКЗИ или уполномоченные сотрудники организаций, осуществляющих поставку и ввод в эксплуатацию средств криптографической защиты.

2.6. Пользователь считается допущенным к СКЗИ после оформления Заключения о допуске пользователя СКЗИ к самостоятельной работе по форме согласно Приложению 2 к настоящим Правилам.

## 3. Учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

3.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в соответствующем Журнале по форме согласно Приложению 3 к настоящим Правилам.

3.2. Поэкземплярный учет СКЗИ ведет ответственный за эксплуатацию СКЗИ в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета СКЗИ). 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.

3.3. 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.

3.4. Все экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов выдаются пользователям СКЗИ под расписку в Журнале учета СКЗИ.

3.5. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под подпись в соответствующем Журнале поэкземплярного учета СКЗИ. Такая передача между пользователями СКЗИ осуществляется с разрешения Ответственного за эксплуатацию СКЗИ. Пользователи СКЗИ несут персональную ответственность за сохранность СКЗИ.

## 4. Хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

4.1. Дистрибутивы СКЗИ, ключевые документы, эксплуатационная и техническая документация к СКЗИ хранятся у ответственного за эксплуатацию СКЗИ, если иное не предусмотрено производственной необходимостью.

4.2. Хранение выданных пользователям СКЗИ ключевых документов, эксплуатационной и технической документации, дистрибутивов СКЗИ должно осуществляться в надежно запираемых шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

4.3. Ключевые носители могут храниться в тубусах (пеналах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

4.4. Замочные скважины вышеуказанных хранилищ, а также тубусы (пеналы) для хранения ключевых носителей должны быть оборудованы приспособлениями для опечатывания. Печати, предназначенные для опечатывания хранилищ и тубусов (пеналов), должны находиться у ответственных за эти хранилища, тубусы (пеналы).

4.5. Учет хранилищ СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведет ответственный за эксплуатацию СКЗИ в журнале учета хранилищ СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета хранилищ).

4.6. Порядок учета ключей для доступа к хранилищам:

- один экземпляр ключа от хранилища должен находиться у ответственного за эксплуатацию СКЗИ, другой – у ответственного за хранилище;
- дубликаты ключей хранилищ, переданные ответственному за эксплуатацию СКЗИ, хранятся в сейфе;
- количество комплектов ключей и их номера от спецпомещений и от хранилищ указываются в соответствующем Журнале по форме согласно Приложению 4 к настоящим Правилам;
- в Журнале учета хранилищ фиксируется факт первичной выдачи ключа от спецпомещений и хранилищ, возможна повторная выдача ключа (в случае смены замка и других обстоятельствах) и сдача ключа при увольнении сотрудника или смене должностных обязанностей (переводе в иное структурное подразделение);

- дубликаты ключей от спецпомещений хранятся у ответственных лиц в соответствии с утвержденными локальными актами администрации, регламентирующими порядок обеспечения пропускного и внутриобъектового режимов;

- при увольнении, либо при назначении иного лица ответственным за хранилище, сотрудник обязан сдать имеющиеся у него ключи от механического замка хранилища ответственному за эксплуатацию СКЗИ;

- при увольнении или переводе в иное структурное подразделение пользователь СКЗИ обязан сдать имеющиеся у него ключи от спецпомещений своему непосредственному руководителю;

- пользователям СКЗИ запрещено передавать кому-либо ключи от хранилищ и спецпомещений кроме как в случаях, предусмотренных настоящими Правилами.

- Тубусы (пеналы), предназначенные для хранения ключевых носителей, подлежат учету в Журнале учета хранилищ.

4.7. 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. Опечатывание производит ответственный за эксплуатацию СКЗИ либо лицо, проводившее ввод в эксплуатацию СКЗИ. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

4.8. Вскрытие аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ, оборудованных средствами контроля за их вскрытием, для проведения ремонта и (или) технического обслуживания должно осуществляться в присутствии ответственного за эксплуатацию СКЗИ.

4.9. При необходимости передачи аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ в сторонние организации для проведения ремонтно-восстановительных или иных работ, осуществляется предусмотренная эксплуатационной и технической документацией к СКЗИ процедура изъятия (удаления программного обеспечения) СКЗИ из аппаратных средств, с которыми они функционировали, и уничтожение криптоключей (исходной ключевой информации), хранящейся в аппаратных СКЗИ.

## 5. Мероприятия при компрометации криптоключей

5.1. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, относятся следующие:

- утрата (хищение) ключевых носителей с криптографическими ключами, в том числе с последующим их обнаружением;

- возникновение подозрений относительно утечки информации или ее искажения (подмены, подделки);

- нарушение целостности печатей на хранилищах СКЗИ и ключевых

документов (при использовании процедуры опечатывания хранилищ);

- утрата ключей от хранилищ СКЗИ и ключевых документов (при нахождении в них ключевых носителей);

- нарушение правил хранения криптографических ключей;

- ошибки при нарушении криптографических операций (например, отрицательный результат по результатам проверки электронной подписи);

- несанкционированное и безучетное копирование ключевой информации;

- передача секретных ключей по линиям связи в открытом виде;

- временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

5.2. О нарушениях, которые могут привести к компрометации криптоключей или передававшейся (хранящейся) с их использованием информации, пользователи СКЗИ обязаны сообщать ответственному за эксплуатацию СКЗИ. В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

5.3. В случае возникновения обстоятельств, указанных в п.5.1 настоящих Правил, пользователь СКЗИ обязан незамедлительно прекратить применение скомпрометированных криптоключей (обмен электронными документами/ формирование электронной подписи и пр.) и информировать о факте возможной компрометации используемых криптоключей ответственного за эксплуатацию СКЗИ.

5.4. Решение о компрометации криптографических ключей принимает ответственный за эксплуатацию СКЗИ.

5.5. Криптоключи, которые были скомпрометированы или в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи подлежат выводу из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. Проведение мероприятий по выводу из действия криптоключей/отзыву сертификата ключа электронной подписи пользователя СКЗИ обеспечивается ответственным за эксплуатацию СКЗИ.

5.6. Сертификат скомпрометированного ключа электронной подписи, подлежит хранению ответственным за эксплуатацию СКЗИ в течение срока хранения электронных документов для проведения (в случае необходимости) расследований, связанных с применением электронной подписи.

## 6. Порядок вывода из действия и уничтожения СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, криптоключей (исходной ключевой информации) и ключевых носителей

6.1. Неиспользуемые или выведенные из действия криптоключи и ключевые документы подлежат уничтожению.

6.2. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной

ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

6.3. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (компакт-дисков, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

6.4. Ключевые носители многократного использования после стирания (разрушения) хранимых на них криптоключей (исходной ключевой информации) подлежат возврату в орган криптографической защиты (иную организацию, предоставившую СКЗИ во временное пользование на основании заключенного договора, контракта или соглашения и (или) осуществлявшую ввод в эксплуатацию СКЗИ) либо по их указанию могут быть уничтожены на месте.

6.5. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

6.6. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

6.7. Ключевые документы должны быть уничтожены в порядке и в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения отражается в Журнале учета СКЗИ.

6.8. Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

6.9. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно

удалена (стерта).

6.10. Вывод из эксплуатации СКЗИ осуществляется ответственным за эксплуатацию СКЗИ. По результатам уничтожения СКЗИ оформляется Акт вывода из эксплуатации СКЗИ по форме согласно Приложению 5 к настоящим Правилам и (или) Акт уничтожения криптографических ключей, содержащихся на ключевых носителях, и ключевых документов оформляется Акт об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов по форме согласно Приложению 6 к настоящим Правилам.

6.11. Вывод из эксплуатации иных СКЗИ осуществляется в порядке согласно заключенным договорам, контрактам или соглашениям.

6.12. После уничтожения СКЗИ, ключевых документов и/или ключевых носителей, а также вывода из эксплуатации СКЗИ ответственный за эксплуатацию СКЗИ вносит необходимые отметки в Журнал учета СКЗИ.

## 7. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним

7.1. Размещение, специальное оборудование, охрана и организация режима в спецпомещениях, должны обеспечивать сохранность СКЗИ и носителей ключевой, аутентифицирующей и парольной информации СКЗИ, а также исключать возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

7.2. Обеспечение безопасности используемых СКЗИ, хранящихся СКЗИ и (или) носителей ключевой, аутентифицирующей и парольной информации СКЗИ от уничтожения, изменения, копирования, а также от иных неправомерных действий достигается в том числе установлением правил доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

7.3. При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

7.4. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

7.5. Техническое обслуживание оборудования, функционирующего с СКЗИ, и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В иных случаях пользователи СКЗИ по согласованию с ответственным за эксплуатацию СКЗИ

обязаны предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

7.6. Для предотвращения просмотра защищаемой информации извне спецпомещений окна должны быть защищены шторами, либо жалюзи или с использованием иных средств/методов.

7.7. В спецпомещениях для хранения ключевых документов, эксплуатационной и технической документации, носителей дистрибутивов СКЗИ необходимо иметь достаточное число надежно запираемых хранилищ (в том числе индивидуального пользования), оборудованных приспособлениями для опечатывания. Ключи от этих хранилищ подлежат учету и хранению в порядке согласно настоящим Правилам.

7.8. В обычных условиях опечатанные хранилища могут быть вскрыты только самими ответственными за хранилища, указанным в Журнале учета хранилищ.

7.9. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилища или спецпомещения посторонних лиц, или в случае утраты ключа от хранилища и спецпомещения о случившемся должно быть немедленно сообщено заместителю главы администрации Новосибирского района Новосибирской области осуществляющему координацию и контроль по вопросам информатизации или иному уполномоченному лицу и ответственному за эксплуатацию СКЗИ. При необходимости вызываются работники правоохранительных органов и принимаются меры по охране места происшествия до их прибытия (спецпомещения не вскрываются, сотрудники администрации и посетители в спецпомещения не допускаются). По результатам анализа случившегося, необходимо дать оценку возможности компрометации хранящихся ключевых и других документов, составить Акт об обнаружении признаков, указывающих на возможное проникновение посторонних лиц в спецпомещения по форме согласно Приложению 7 к настоящим Правилам, и принять, при необходимости, меры к локализации последствий компрометации информации и к замене скомпрометированных криптоключей.

7.10. При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок размещения СКЗИ, хранения ключевых и других документов в хранилище или спецпомещении, от которого утрачен ключ, до замены замка или изменения секрета замка устанавливает руководитель соответствующего структурного подразделения администрации по согласованию с ответственным за эксплуатацию СКЗИ, при этом должны быть обеспечены условия, исключающие бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.11. Установленный режим охраны спецпомещений должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящих Правил. Правила допуска сотрудников и посетителей в спецпомещения в рабочее и нерабочее время должны учитывать специфику и условия работы конкретных пользователей СКЗИ.

7.12. Двери спецпомещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода пользователей СКЗИ и посетителей в сопровождении ответственных лиц.

7.13. Ключи от входных дверей спецпомещений учитывают и выдают пользователям СКЗИ под расписку в Журнале учета хранилищ.

7.14. В случае возникновения нештатной ситуации (в том числе событий чрезвычайного характера) необходимо в обязательном порядке известить о случившемся ответственного за эксплуатацию СКЗИ и заместителю главы администрации Новосибирского района Новосибирской области осуществляющему координацию и контроль по вопросам информатизации или уполномоченное лицо.

## 8. Контроль за соблюдением порядка использования СКЗИ

8.1. Текущий контроль за организацией и обеспечением порядка использования СКЗИ возлагается на ответственного за эксплуатацию СКЗИ в пределах его полномочий, предусмотренных Инструкцией ответственного за эксплуатацию средств криптографической защиты информации в администрации.

8.2. Ответственный за эксплуатацию СКЗИ должен обобщать результаты всех видов контроля за организацией и обеспечением порядка использования СКЗИ в администрации, анализировать причины выявленных недостатков, разрабатывать меры по их профилактике, контролировать выполнение рекомендаций, содержащихся в актах проверок контролирующих организаций.

ПРИЛОЖЕНИЕ № 1
к Правилам эксплуатации средств

криптографической защиты
информации в Новосибирского района
Новосибирской области

ФОРМА

**АКТ**
**ввода в эксплуатацию средств криптографической защиты информации**

Настоящий акт составлен о том, что произведена установка и настройка изделия:

*Наименование средства криптографической защиты информации*

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 средства криптографической защиты информации*:

- серийный номер дистрибутива: _____;
- регистрационный (учетный) номер СКЗИ: _____;

размещено на аппаратном средстве (№ системного блока): _____ и в соответствии с эксплуатационной и технической документацией на СКЗИ <*Наименование 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 СКЗИ <*Наименование СКЗИ*> учтен в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов [полное_наименование_ОИОГВ.родительный].

Первичный инструктаж по использованию СКЗИ проведен со специалистом:

_____

*(Должность, ФИО)*

_____

Ответственный за эксплуатацию
СКЗИ:

_____ _____

*(подпись)* *(ФИО)*

«___» _____ 20 ___ г.

ПРИЛОЖЕНИЕ № 2
к Правилам эксплуатации средств
криптографической защиты
информации в Новосибирского района
Новосибирской области

ФОРМА

**ЗАКЛЮЧЕНИЕ**
**о допуске пользователя СКЗИ к самостоятельной работе**

«  » _____ 20 г.

Пользователь СКЗИ:

_____

*(должность, ФИО, наименование организации)*

_____

_____

(далее – пользователь СКЗИ) 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, прошел обучение правилам эксплуатации и обеспечения безопасности

_____

*(наименование средства криптографической защиты информации)*

Пользователь СКЗИ обязуется:

не разглашать сведения конфиденциального характера, к которым допущен, рубежи их защиты, в том числе, сведения о криптоключах;

соблюдать требования к обеспечению безопасности сведений конфиденциального характера с использованием СКЗИ;

сообщать ответственному за эксплуатацию СКЗИ 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 ответственного за эксплуатацию СКЗИ 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: пользователь к самостоятельной работе с СКЗИ допущен.

С заключением ознакомлен(а):

_____ _____

(подпись) (ФИО)

Ответственный за эксплуатацию
СКЗИ:

_____ _____

(подпись) (ФИО)

ПРИЛОЖЕНИЕ № 3
к Правилам эксплуатации средств
криптографической защиты
информации в Новосибирского района
Новосибирской области

ФОРМА

**ЖУРНАЛ**
**поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов**

Журнал начат «____» _____
20 ___ г.

Журнал завершен «____» _____
20 ___ г.

Журнал составлен на _____ листах

| № п/п | Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов | Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов | Номера экземпляров (криптографические номера) ключевых документов | Отметка о получении | | Отметка о выдаче | |
|---|---|---|---|---|---|---|---|
| | | | | 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. лиц, 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. лиц, производивших изъятие (уничтожение) | Номер акта или расписка об уничтожении | |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |

ПРИЛОЖЕНИЕ № 4
к Правилам эксплуатации средств
криптографической защиты
информации в Новосибирского района
Новосибирской области

ФОРМА

**ЖУРНАЛ**
**учета хранилищ средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов**

Журнал начат «____» _____
20 ___ г.

Журнал завершен «____» _____
20 ___ г.

Журнал составлен на _____ листах

| № п/п | Наименование хранилища (помещение, сейф, металлический шкаф) | Инвентарный номер хранилища | Местонахождение (подразделение, номер кабинета) | Что хранится (документы, изделия) | Ф.И.О. ответственного за хранилище |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |

| Количество комплектов ключей от помещения, хранилища и их номера1 | Расписка о получении ключа (ФИО, номер комплекта ключей, подпись получившего ключ, дата получения ключа), тубуса(пенала) (ФИО, номер печати, подпись получившего тубус (пенал), дата получения тубуса (пенала)) | Расписка о возврате ключа (ФИО, номер комплекта ключей, подпись принявшего ключ, дата возврата ключа), тубуса (пенала) (ФИО, номер печати, подпись принявшего тубус (пенал), дата возврата тубуса (пенала)) | Примечание |
|---|---|---|---|
| 6 | 7 | 8 | 9 |
| | | | |
| | | | |
| | | | |

[1] Для тубусов (пеналов) в графе ставится прочерк

ПРИЛОЖЕНИЕ № 5
к Правилам эксплуатации средств
криптографической защиты
информации в Новосибирского района
Новосибирской области

ФОРМА

**АКТ**
**вывода из эксплуатации средств**
**криптографической защиты информации**

Настоящий акт составлен о том, что перечисленные в нем средства криптографической защиты информации (СКЗИ) уничтожены с предварительным стиранием программного обеспечения СКЗИ, и произведено стирание информации, оставшейся в устройствах памяти оборудования.

| № п/п | Наименование СКЗИ, эксплуатационной и технической документации к ним | Регистрационный номер СКЗИ, эксплуатационной и технической документации к ним | Номер аппаратного средства |
|---|---|---|---|
| | | | |
| | | | |

Регистрационные данные на СКЗИ сверены с записями в настоящем Акте, уничтожение СКЗИ выполнено в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

Узлы и детали аппаратных средств передать для дальнейшей эксплуатации.

В журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов [полное_наименование_ОИОГВ.родительный] внесены соответствующие записи.

Ответственный за эксплуатацию
СКЗИ:

_____ _____
(подпись) (ФИО)

«___» _____ 20 ___ г.

ПРИЛОЖЕНИЕ № 6
к Правилам эксплуатации средств
криптографической защиты
информации в Новосибирского района
Новосибирской области

ФОРМА

**АКТ № _____**
**об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов**

Настоящий акт составлен о том, что произведено уничтожение нижеуказанных криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

| № п/п | Наименование носителя криптографических ключей, ключевых документов | Номер (идентификатор) криптографического ключа, наименование документа | ФИО владельца ключа (документа) | Примечание |
|---|---|---|---|---|
| | | | | |
| | | | | |

Всего уничтожено _____

криптографических ключей на _____ ключевых носителях.

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.

Ответственный за эксплуатацию
СКЗИ:

_____ _____
(подпись) (ФИО)

«___» _____ 20 ___ г.

ПРИЛОЖЕНИЕ № 7
к Правилам эксплуатации средств
криптографической защиты
информации в Новосибирского района
Новосибирской области

ФОРМА

**АКТ**
**об обнаружении признаков, указывающих на возможное проникновение посторонних лиц в помещения администрации Новосибирского района Новосибирской области**

«  » 20 г.

_____
_____

*(должность, фамилия, имя, отчество должностного лица)*

в связи с обнаружением

_____

_____
_____

в присутствии:

_____
_____

_____
_____

*(должность, фамилии, имена, отчества иных лиц, присутствовавших при осмотре)*

произвел осмотр помещения (*в котором ведется обработка информации ограниченного доступа (в том числе персональных данных) и размещены используемые средства криптографической информации (СКЗИ), хранятся СКЗИ*

*и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ*[2]), расположенного по адресу:

_____

_____

В ходе осмотра обнаружено:

_____

_____

_____

_____

_____

Подписи лиц, принимавших участие (присутствовавших) при проведении осмотра:

| _____ | _____ | _____ |
|---|---|---|
| (должность) | (подпись) | (ФИО) |
| _____ | _____ | _____ |
| (должность) | (подпись) | (ФИО) |
| _____ | _____ | _____ |
| (должность) | (подпись) | (ФИО) |

_____

[2] Уточнить, оставить нужное

ПРИЛОЖЕНИЕ № 2
к распоряжению администрации
Новосибирского района
Новосибирской области
от 05.12.2024 № 412-рк

# ИНСТРУКЦИЯ
## ответственного за эксплуатацию средств криптографической защиты информации в администрации Новосибирского района Новосибирской области

### 1. Общие положения

1.1. Настоящая Инструкция определяет основные права и обязанности ответственного за эксплуатацию средств криптографической защиты информации (далее – СКЗИ, криптосредства), применяемых в администрации Новосибирского района Новосибирской области.

1.2. Ответственный за эксплуатацию СКЗИ назначается распоряжением администрации Новосибирского района Новосибирской области.

1.3. Ответственный за эксплуатацию СКЗИ получает указания от заместителя главы администрации Новосибирского района Новосибирской области осуществляющему координацию и контроль по вопросам информатизации или иного уполномоченного лица и подотчетно ему.

1.4. Ответственный за эксплуатацию СКЗИ в своей деятельности руководствуется действующими нормативными правовыми актами в сфере (области) применения шифровальных (криптографических) средств, эксплуатационной и технической документации на СКЗИ, локальными актами администрации Новосибирского района Новосибирской области (далее – администрация) по вопросам эксплуатации СКЗИ и настоящей Инструкцией.

1.5. Ответственный за эксплуатацию СКЗИ отвечает за организацию, обеспечение функционирования и безопасности СКЗИ, применяемых в администрации.

### 2. Обязанности ответственного за эксплуатацию СКЗИ

2.1. Ответственный за эксплуатацию СКЗИ обязан:

2.1.1. Соблюдать требования правовых актов администрации по вопросам эксплуатации СКЗИ, а также актов администрации, устанавливающих порядок обработки и обеспечения безопасности защищаемой информации.

2.1.2. Знать и обеспечивать реализацию норм действующего законодательства Российской Федерации в сфере (области) применения шифровальных (криптографических) средств, в том числе обработки и обеспечения безопасности защищаемой информации с использованием СКЗИ.

2.1.3. Обеспечивать исполнение принятых администрацией обязательств в соответствии с заключенными соглашениями, касающимися обеспечения функционирования и порядка эксплуатации СКЗИ.

2.1.4. Контролировать соблюдение условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним.

2.1.5. Обеспечивать поддержание в актуальном состоянии правовых актов администрации по вопросам эксплуатации СКЗИ, Перечень лиц, допущенных к работе с СКЗИ в администрации, и лиц, имеющих доступ в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

2.1.6. Обеспечивать надежное хранение эксплуатационной и технической документации к СКЗИ, ключевых документов.

2.1.7. Осуществлять ведение Журнала учета хранилищ СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

2.1.8. Вести поэкземплярный учет используемых в администрации СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета СКЗИ).

2.1.9. Обеспечивать пломбирование (опечатывание) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ.

2.1.10. Организовывать установку, настройку, ввод в эксплуатацию и вывод из эксплуатации СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ.

2.1.11. Контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) и фиксировать факт уничтожения/вывода из эксплуатации в Журнале учета СКЗИ.

2.1.12. Организовывать обучение и проводить инструктаж пользователей СКЗИ по правилам работы с СКЗИ.

2.1.13. Контролировать оформление и при необходимости оформлять Заключение о допуске пользователя СКЗИ к самостоятельной работе.

2.1.14. Контролировать исполнение пользователями СКЗИ требований Инструкции пользователя СКЗИ администрации, а также требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации в пределах своей компетенции.

2.1.15. Соблюдать требования к обеспечению безопасности информации, обрабатываемой в администрации, безопасности СКЗИ и ключевых документов к ним.

2.1.16. Не разглашать информацию, к которой он допущен, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты.

2.1.17. Инициировать проведение проверок по фактам ставших известными попыток посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним, о фактах утраты или недостачи СКЗИ, ключевых документов к ним, личных печатей, ключей от хранилищ (сейфов, металлических шкафов, ящиков индивидуального пользования), помещений, в которых размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, и о других фактах, которые свидетельствуют о возможной компрометации криптографических ключей и могут привести к нарушению конфиденциальности информации ограниченного доступа, при необходимости в случае подтверждения факта компрометации криптографических ключей обеспечивать информирование всех заинтересованных участников информационного обмена о факте компрометации ключевой информации.

2.1.18. Обеспечить выведение из действия криптоключей, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

2.1.19. Осуществлять координацию и контроль действий пользователей СКЗИ по восстановлению скомпрометированных криптоключей.

2.1.20. Инициировать проведение служебных расследований по фактам компрометации криптоключей, а также в целях выявления причин нарушения требований безопасности функционирования СКЗИ.

2.1.21. Обобщать результаты всех видов контроля за организацией и обеспечением порядка использования СКЗИ в администрации, анализировать причины выявленных нарушений, разрабатывать меры по их профилактике и предотвращению возможных негативных последствий подобных нарушений, контролировать выполнение рекомендаций, содержащихся в актах проверок контролирующих организаций.

2.1.22. Сдать своему непосредственному руководителю СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы, личную печать, ключи от хранилищ и помещений, в которые допущен ответственный за эксплуатацию СКЗИ, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

## 3. Права ответственного за эксплуатацию СКЗИ

3.1. Ответственный за эксплуатацию СКЗИ имеет право:

3.1.1. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения возложенных на него обязанностей.

3.1.2. Получать доступ к информации, материалам, техническим средствам, и помещениям, необходимый для надлежащего исполнения своих прав и обязанностей.

3.1.3. Проходить обучение (переподготовку) по вопросам, связанным с исполнением возложенных на него обязанностей в области обеспечения учета,

хранения и эксплуатации СКЗИ и защиты информации, обрабатываемой в информационных системах администрации, с использованием СКЗИ.

3.1.4. Требовать от сотрудников администрации соблюдения требований законодательства Российской Федерации, правовых актов администрации в области применения шифровальных (криптографических) средств, в том числе обработки и обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием СКЗИ.

3.1.5. Проводить и (или) организовывать проверки соблюдения в администрации условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ.

3.1.6. Инициировать проведение и принимать участие в служебных расследованиях по фактам нарушения сотрудниками администрации установленных правил эксплуатации СКЗИ.

3.1.7. Требовать прекращения сотрудниками администрации обработки информации с использованием СКЗИ в случае установления фактов нарушения правил эксплуатации СКЗИ или нарушения функционирования СКЗИ.

3.1.8. Привлекать в случае необходимости при проведении служебных расследований сотрудников администрации, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.

3.1.9. Вносить предложения по вопросам использования СКЗИ, устранению выявленных нарушений правил эксплуатации СКЗИ и предупреждению подобного рода нарушений.

## 4. Ответственность

4.1. Ответственный за эксплуатацию СКЗИ несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

- неисполнение либо ненадлежащее исполнение своих должностных обязанностей;
- нарушения в работе информационных систем администрации, вызванные его неправомерными действиями или неправильным использованием предоставленных прав;
- нарушение законодательства Российской Федерации, правовых актов администрации, устанавливающих порядок работы с СКЗИ;
- превышение должностных полномочий и злоупотребление ими;
- применение к администрации штрафных санкций по вине ответственного за эксплуатацию СКЗИ;
- совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

ПРИЛОЖЕНИЕ № 3
к распоряжению администрации
Новосибирского района
Новосибирской области
от 05.12.2024 № 488-рс

# ИНСТРУКЦИЯ
## пользователя средств криптографической защиты информации в администрации Новосибирского района Новосибирской области

### 1. Общие положения

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации администрации Новосибирского района Новосибирской области (далее – Инструкция) определяет права и обязанности пользователей средств криптографической защиты информации (далее – СКЗИ).

1.2. Пользователями СКЗИ являются работники (сотрудники) администрации Новосибирского района Новосибирской области (далее – администрация), включенные в Перечень лиц, допущенных к работе с СКЗИ в администрации, утвержденный локальным актом администрации.

1.3. Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами в сфере (области) применения шифровальных (криптографических) средств, локальными актами администрации по вопросам эксплуатации СКЗИ, настоящей Инструкцией и проходит обучение правилам работы с СКЗИ.

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

1.5. Инструктаж по правилам работы с СКЗИ и оформление Заключения о допуске пользователя СКЗИ к самостоятельной работе осуществляют уполномоченные сотрудники организаций, осуществляющих ввод в эксплуатацию СКЗИ или ответственный за эксплуатацию СКЗИ в администрации.

1.6. Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту СКЗИ от несанкционированного использования, а также за сохранность полученных под расписку в соответствующем журнале СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

### 2. Обязанности и права пользователя СКЗИ

2.1. Пользователь СКЗИ обязан:

- соблюдать требования по обеспечению безопасности функционирования СКЗИ;
- обеспечить конфиденциальность информации ограниченного

распространения, доступной ему по роду выполняемых функциональных обязанностей, в том числе сведений о криптоключах;

- обеспечить хранение ключевых документов, эксплуатационной и технической документации, дистрибутивов СКЗИ, опечатываемых тубусов (пеналов) в надежно запираемых шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;

- сообщать ответственному за эксплуатацию СКЗИ о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать ответственному за эксплуатацию СКЗИ в администрации, а при его отсутствии руководителю соответствующего структурного подразделения СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы, ключевые носители, личные печати;

- сдать имеющиеся у него ключи от замков хранилищ ответственному за эксплуатацию СКЗИ, а при его отсутствии руководителю соответствующего структурного подразделения при увольнении, либо при назначении другого лица ответственным за хранилище;

- сдать имеющиеся у него ключи от помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения) ответственному за эксплуатацию СКЗИ, а при его отсутствии руководителю соответствующего структурного подразделения при увольнении или переводе в иное структурное подразделение;

- немедленно уведомлять своего непосредственного руководителя и ответственного за эксплуатацию СКЗИ о компрометации криптоключей, фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от Помещений, хранилищ, личных печатей, удостоверений, пропусков и о других фактах, которые могут привести к разглашению защищаемой информации, а также о причинах и условиях возможной утечки таких сведений;

- незамедлительно прекратить применение скомпрометированных криптоключей (обмен электронными документами/формирование электронной подписи и пр.) и обеспечить вывод из действия криптоключей, в отношении которых возникло подозрение в компрометации, а также действующих совместно с ними других криптоключей;

- немедленно прекратить работу с СКЗИ в случае обнаружения на рабочей станции посторонних программ (в том числе вредоносного программного обеспечения), о произошедшем известить ответственного за эксплуатацию СКЗИ и ответственного за защиту информации в администрации;

- в пределах своей компетенции предоставлять по требованию ответственного за эксплуатацию СКЗИ информацию, необходимую при проведении служебных расследований по фактам компрометации криптоключей, а также в целях выявления причин нарушения требований безопасности функционирования СКЗИ.

2.2. Пользователю СКЗИ запрещается:

- осуществлять несанкционированное и безучётное копирование ключевой информации;

- хранить ключевые носители вне хранилищ и помещений, гарантирующих их сохранность и конфиденциальность ключевой информации;

- передавать ключевые носители лицам, к ним не допущенным;

- во время работы оставлять ключевые носители без присмотра (например, на рабочем столе или в разъеме системного блока персонального компьютера);

- выводить ключевую информацию на печать, дисплей монитора или иное средство визуализации данных;

- записывать на ключевые носители постороннюю информацию;

- вносить какие-либо изменения в программное обеспечение СКЗИ;

- устанавливать и эксплуатировать стороннее программное обеспечение, которое может нарушить функционирование СКЗИ.

- использовать бывшие ранее в работе ключевые носители для записи новой ключевой информации без предварительного гарантированного уничтожения ранее хранящейся на них информации;

- использовать ключевые носители, выведенные из действия;

- передавать кому-либо ключи от хранилищ и Помещений, а также личные печати кроме как в случаях, предусмотренных настоящей Инструкцией.

2.3. Пользователь СКЗИ имеет право:

- знакомиться с локальными актами администрации, регламентирующими процессы обработки и обеспечения безопасности защищаемой информации;

- требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения возложенных на него обязанностей;

- получать доступ к информации, материалам, техническим средствам, и в помещения, необходимый для надлежащего исполнения своих прав и обязанностей;

- проходить обучение по вопросам, связанным с исполнением возложенных на него обязанностей в области эксплуатации СКЗИ;

- уничтожать использованные непосредственно им (предназначенные для него) ключевые документы с обязательным уведомлением ответственного за эксплуатацию СКЗИ, если иное не предусмотрено эксплуатационной и технической документацией на СКЗИ, договорами или соглашениями, заключенными с организациями, осуществлявшими ввод в эксплуатацию СКЗИ;

- вносить предложения заместителю главы администрации Новосибирского района Новосибирской области осуществляющему координацию и контроль по вопросам информатизации, по вопросам использования СКЗИ, по устранению выявленных нарушений правил эксплуатации СКЗИ и предупреждению подобного рода нарушений.

## 3. Ответственность

3.1. Пользователь СКЗИ несет предусмотренную законодательством

Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

- неисполнение либо ненадлежащее исполнение возложенных на него обязанностей;

- превышение, злоупотребление или неправильное использование предоставленных полномочий, предусмотренных настоящей Инструкцией;

- нарушение законодательства Российской Федерации, правовых актов администрации Новосибирского района Новосибирской области (далее – правовых актов района), устанавливающих порядок работы с СКЗИ;

- применение к администрации штрафных санкций по вине пользователя СКЗИ;

- совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

ПРИЛОЖЕНИЕ № 4
к распоряжению администрации
Новосибирского района
Новосибирской области
от 05.12.2024 № 412-рк

ТИПОВАЯ ФОРМА

**ПЕРЕЧЕНЬ ЛИЦ,**
**допущенных к работе со средствами криптографической защиты информации в администрации Новосибирского района Новосибирской области**

| № п/п | ФИО работника | Должность | Структурное подразделение |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |

ПРИЛОЖЕНИЕ № 5
к распоряжению администрации
Новосибирского района
Новосибирской области
от 05.12.2024 № 418-рк

# ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ, в которых ведется обработка персональных данных и размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях

## 1. Общие положения

1.1. Настоящий Порядок регламентирует условия и порядок осуществления доступа в помещения администрации Новосибирского района Новосибирской области (далее – администрация), в которых ведется обработка информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), и размещены используемые средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях (далее – Помещения) в целях организации режима обеспечения безопасности информации, препятствующего возможности неконтролируемого проникновения или пребывания в вышеуказанных помещениях лиц, не имеющих прав доступа в эти помещения.

1.2. Для обеспечения доступа сотрудников администрации в вышеуказанные Помещения предусматривается комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности администрации.

1.3. Реализация комплекса мер, направленных на поддержание и обеспечение настоящего Порядка, возлагается на сотрудников администрации.

1.4. В случае нарушения настоящего Порядка сотрудники могут быть привлечены к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

## 2. Порядок доступа в Помещения

2.1. Обеспечение безопасности информации от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении информации достигается, в том числе установлением правил доступа в Помещения.

2.2. Размещение информационных систем, в которых обрабатывается информация, СКЗИ, эксплуатационной и технической документации к ним,

ключевых документов, хранилищ материальных носителей персональных данных, должно осуществляться в пределах контролируемой зоны, границы которой устанавливаются распоряжением администрации.

2.3. Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации и средств защиты информации, криптосредств и ключевых документов к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих Помещениях посторонних лиц и просмотра ведущихся там работ.

2.4. Для предотвращения просмотра извне защищаемой информации окна Помещений должны быть защищены шторами или жалюзи.

2.5. Должны обеспечиваться контроль и управление физическим доступом в Помещения:

- в Помещения допускаются только сотрудники администрации в соответствии с Перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, и Перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Перечни лиц);

- в нерабочее время пребывание в Помещениях вышеуказанных сотрудников администрации разрешается только на основании служебных записок (или иных разрешающих документов/указаний руководителя);

- в рамках внутреннего контроля должен проводиться контроль санкционирования и учета физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, СКЗИ, а также в помещения и сооружения, в которых они установлены (контроль актуальности Перечней лиц);

- нахождение в Помещениях лиц, не включенных в Перечни лиц, возможно только в присутствии уполномоченных сотрудников администрации. Время нахождения в Помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в Помещении.

2.6. Помещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей Помещений на замок и их открытие только для санкционированного прохода.

2.7. Ключи от входных дверей Помещений учитывают и выдают только работникам (сотрудникам) администрации, включенным в Переченях лиц,

2.8. Сотрудники администрации, указанные в Перечнях лиц, не должны покидать Помещение, не убедившись, что доступ посторонних лиц к защищаемой информации невозможен. Запрещается оставлять материальные носители с защищаемой информацией без присмотра в незапертом Помещении.

2.9. При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в Помещения, немедленно ставятся в известность ответственный за организацию обработки персональных данных, ответственный за защиту информации, ответственный за эксплуатацию СКЗИ, непосредственный руководитель соответствующего

структурного подразделения администрации. При необходимости вызываются работники правоохранительных органов и принимаются меры по охране места происшествия до их прибытия (Помещения не вскрываются, сотрудники администрации и посетители в Помещения не допускается). Дальнейшие действия определяются характером произошедшего инцидента.

2.10. По результатам анализа случившегося, необходимо дать оценку возможности компрометации хранящихся ключевых и других документов, составить акт об обнаружении признаков, указывающих на возможное проникновение посторонних лиц в Помещения администрации и принять при необходимости меры к локализации последствий компрометации информации и к замене скомпроментированных криптоключей.

2.11. При утрате ключа от входной двери в Помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей, соответствующие сведения вносятся в Журнал учета хранилищ. Порядок размещения СКЗИ, хранения ключевых и других документов в Помещении, от которого утрачен ключ, до замены замка или изменения секрета замка устанавливает руководитель соответствующего структурного подразделения администрации по согласованию с ответственным за эксплуатацию СКЗИ, при этом должны быть обеспечены условия, исключающие бесконтрольный доступ, а также непреднамеренное уничтожение СКЗИ, ключевых и иных документов.

2.12. В случае возникновения нештатной ситуации, событий чрезвычайного характера необходимо в обязательном порядке известить о случившемся заместителю главы администрации Новосибирского района Новосибирской области осуществляющему координацию и контроль по вопросам информатизации

2.13. Сотрудники органов министерства по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и аварийных служб, врачи «скорой помощи» и сотрудники правоохранительных органов допускаются в Помещения в сопровождении сотрудников администрации, включенных в Перечни лиц, имеющих доступ в помещения, или сотрудников службы охраны.

ПРИЛОЖЕНИЕ № 6
к распоряжению администрации
Новосибирского района
Новосибирской области
от 05.12.2024 № 412-рс

ТИПОВАЯ ФОРМА

**ПЕРЕЧЕНЬ ЛИЦ, ИМЕЮЩИХ ДОСТУП В ПОМЕЩЕНИЯ, где размещены используемые средства криптографической защиты информации, хранятся средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации**

| № п/п | ФИО работника | Должность | Структурное подразделение администрации | Адрес расположения и номера помещений (кабинетов), в которые разрешен доступ |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Лист ознакомления

с распоряжением от _____ № _____

«Об организации работы со средствами криптографической защиты информации в администрации Новосибирского района Новосибирской области»

| № п/п | ФИО | Дата ознакомления | Подпись |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |
| 11. | | | |
| 12. | | | |
| 13. | | | |
| 14. | | | |
| 15. | | | |
| 16. | | | |
| 17. | | | |
| 18. | | | |
| 19. | | | |
| 20. | | | |
| 21. | | | |
| 22. | | | |
| 23. | | | |
| 24. | | | |
| 25. | | | |
| 26. | | | |
| 27. | | | |
| 28. | | | |
| 29. | | | |
| 30. | | | |
| 31. | | | |
| 32. | | | |
| 33. | | | |
| 34. | | | |
| 35. | | | |
| 36. | | | |
| 37. | | | |
| 38. | | | |
| 39. | | | |
| 40. | | | |