КОМИТЕТ ОБРАЗОВАНИЯ И НАУКИ АДМИНИСТРАЦИИ Г. НОВОКУЗНЕЦКА
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ НЕТИПОВОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
"ЛИЦЕЙ №111"
654007, Россия, г.Новокузнецк, ул.Кирова 35, тел./факс 8(3843)46-82-08,
тел.46-05-33, 45-05-53,e-mail:litcey111@yandex.ru, http://www.liceym111.ru

СОГЛАСОВАНО
председатель профкома
_____ О.В. Митрохина
01.07.2021г.

Полюшко Марина Владимировна
Подписано цифровой подписью: Полюшко Марина Владимировна
Дата: 2021.09.20 12:56:51 +07'00'

УТВЕРЖДАЮ
директор МБ НОУ «Лицей № 111»
_____ М.В. Полюшко
01.07.2021г.

Инструкция № ИБ 10

по обеспечению безопасности эксплуатации средств криптографической защиты информации в информационной системе «МБ НОУ Лицей № 111»

1. Общие положения

1.1. Настоящая Инструкция по обеспечению безопасности эксплуатации средств криптографической защиты информации в информационной системе «**МБ НОУ Лицей № 111**» (далее – Инструкция) определяет порядок учёта, хранения и использования средств криптографической защиты информации (далее – СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и действий сотрудников лицея при компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

1.2. Все действия с СКЗИ должны осуществляться в соответствии с эксплуатационной документацией на СКЗИ.

1.3. Настоящая Инструкция разработана на основе законодательства Российской Федерации, иных правовых актов, а также:

– Приказа ФСБ РФ от 9 февраля 2005 г. № 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 июня 2001 года № 152;

– 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 защищённости, утверждённых приказом ФСБ России от 10 июля 2014 г. № 378.

2. Организация и обеспечение безопасности обработки с использованием шифровальных (криптографических) средств информации

2.1. Для защиты информации, обрабатываемой в информационной системе «**МБ НОУ Лицей № 111**» (далее – ИС), должны использоваться сертифицированные ФСБ России СКЗИ.

2.2. Пользователи СКЗИ допускаются к работе с СКЗИ на основании Перечня лиц (пользователей СКЗИ), допущенных к работе со средствами криптографической защиты информации в ИС, утвержденного руководством лицея.

Пользователи СКЗИ обязаны:

– не разглашать информацию, к которой они допущены, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;

– соблюдать требования к обеспечению безопасности защищаемой информации, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

– сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– немедленно уведомлять ответственного за защиту информации, в том числе за обеспечение безопасности ПДн в ИС, 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 защищаемой информации;

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

2.3. Обеспечение функционирования и безопасности СКЗИ возлагается на ответственного пользователя СКЗИ, имеющего необходимый уровень квалификации, назначаемого приказом руководства лицея (далее – ответственный пользователь СКЗИ).

Допускается возложение функций ответственного пользователя СКЗИ на:

– одного из пользователей СКЗИ;

– на структурное подразделение или должностное лицо (работника), ответственных за защиту информации, назначаемых руководствомлицея.

2.4. Лица, оформляемые на работу в качестве пользователей (ответственных пользователей) СКЗИ, должны быть ознакомлены с настоящей Инструкцией и другими документами, регламентирующими организацию и обеспечение безопасности защищаемой информации при её обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

2.5. Должно быть обеспечено хранение съёмных машинных носителей информации в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае, если на съёмном машинном носителе информации хранится только защищаемая информация в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

2.6. Должен осуществляться поэкземплярный учёт машинных носителей информации, который достигается путём ведения журнала учёта носителей информации с использованием регистрационных (заводских) номеров.

2.7. Текущий контроль за организацией и обеспечением функционирования СКЗИ возлагается на ответственного пользователя СКЗИ.

2.8. Контроль за организацией, обеспечением функционирования и безопасности СКЗИ, предназначенных для защиты информации при её обработке в ИС, осуществляется в соответствии с действующим законодательством Российской Федерации.

3. Порядок обращения со средствами криптографической информации и криптоключами к ним. Мероприятия при компрометации криптоключей

3.1. Пользователи СКЗИ обязаны:

– не разглашать информацию о ключевых документах;

– не допускать снятие копий с ключевых документов;

– не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

– не допускать записи на ключевой носитель посторонней информации;

– не допускать установки ключевых документов в другие ПЭВМ.

3.2. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования СКЗИ, указанные сообщения необходимо передавать только с использованием СКЗИ. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3.3. СКЗИ, используемые для обеспечения безопасности защищаемой информации при её обработке в ИС, подлежат учёту с использованием индексов или условных наименований и регистрационных номеров.

Перечень индексов, условных наименований и регистрационных номеров СКЗИ определяется Федеральной службой безопасности Российской Федерации.

3.4. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учёту. Форма журнала учёта приведена в Приложении № 1. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. 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.

Единицей поэкземплярного учёта ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.5. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учёта пользователям СКЗИ, несущим персональную ответственность за их сохранность.

Ответственный пользователь СКЗИ заводит и ведёт на каждого пользователя СКЗИ лицевой счёт, в котором регистрирует числящиеся за ними СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.

3.6. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ). Типовая форма технического (аппаратного) журнала приведена в Приложении № 2.

3.7. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) ответственным пользователем СКЗИ под расписку в соответствующих журналах поэкземплярного учёта. Такая передача между пользователями СКЗИ должна быть санкционирована ответственным пользователем СКЗИ.

3.8. Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в металлическом хранилище в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в

случае компрометации действующих ключевых документов.

3.9. 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. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

3.10. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными лицеем ответственными пользователями СКЗИ и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и ключевым документам во время доставки.

Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

3.11. Для пересылки СКЗИ и ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают оператора или ответственного пользователя СКЗИ, для которых эти упаковки предназначены. На таких упаковках делают пометку «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

3.12. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать: что посылается и в каком количестве, учётные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

3.13. Полученные упаковки вскрывает только ответственный за защиту информации в ИС или ответственный пользователь СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать – их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к её содержимому, то получатель составляет акт, который высылает отправителю. Полученные с такими отправлениями СКЗИ и ключевые документы до получения указаний от отправителя применять не разрешается.

3.14. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

3.15. Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

3.16. Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно.

Указание о вводе в действие очередных ключевых документов может быть дано

ответственным пользователем СКЗИ только после поступления от всех заинтересованных пользователей СКЗИ подтверждения о получении ими очередных ключевых документов.

3.17. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю СКЗИ или по его указанию должны быть уничтожены на месте.

3.18. Уничтожение криптоключей (исходной ключевой информации) может производиться путём физического уничтожения ключевого носителя, на котором они расположены, или путём стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, 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).

Ключевые носители уничтожают путём 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).

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

3.19. СКЗИ уничтожают (утилизируют) по решению лицея, владеющего СКЗИ, и с уведомлением организации, ответственной в соответствии с ПКЗ-2005 за организацию поэкземплярного учёта СКЗИ.

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.

3.20. 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 надёжно удалена (стёрта).

3.21. Ключевые документы должны быть уничтожены 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 оформляется в соответствующих журналах поэкземплярного учёта. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введённая и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищённом виде данные следует перешифровать на новых криптоключах.

3.22. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под расписку в техническом (аппаратном) журнале.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным пользователем СКЗИ под расписку в соответствующих журналах поэкземплярного учёта, а уничтожение большого объёма ключевых документов может быть оформлено актом. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом (устным сообщением по телефону и т. п.) ответственного пользователя СКЗИ для списания уничтоженных документов с их лицевых счетов.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию СКЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации.

Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведённом уничтожении делаются отметки в соответствующих журналах поэкземплярного учёта.

3.23. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорён в эксплуатационной и технической документации к СКЗИ. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя СКЗИ, согласованного с руководством лицея, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

3.24. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи СКЗИ обязаны сообщать ответственному пользователю СКЗИ и (или) ответственному за защиту информации в ИС.

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

В случаях недостачи, непредъявления ключевых документов, а также неопределённости их местонахождения принимаются срочные меры к их розыску.

3.25. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет лицей.

3.26. Ключевые документы для СКЗИ или исходная ключевая информация для выработки ключевых документов изготавливаются ФСБ России на договорной основе или лицами, имеющими лицензию ФСБ России на деятельность по изготовлению ключевых документов для СКЗИ.

Изготовлять ключевые документы из исходной ключевой информации могут операторы или ответственные пользователи СКЗИ, применяя штатные СКЗИ, если такая возможность предусмотрена эксплуатационной и технической документацией к СКЗИ.

4. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средства криптографической защиты информации или хранятся ключевые документы к ним

4.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность защищаемой информации,

СКЗИ и ключевых документов к ним.

При оборудовании режимных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ. Перечисленные в настоящем документе требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования СКЗИ, согласованными с ФСБ России.

4.2. Режимные помещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время.

4.3. Должно быть обеспечено постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

4.4. 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.

4.5. Приказами руководства лицеяутверждаются:

– правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

– перечень лиц, имеющих право вскрытия помещений;

– перечень лиц, имеющих право доступа в помещения.

4.6. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в журнале учёта хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе (металлическом хранилище) ответственного пользователя СКЗИ.

4.7. При использовании охранной сигнализации, необходимо периодически проверять исправность сигнализации ответственному пользователю СКЗИ совместно с представителем службы охраны или дежурным по лицею с отметкой в соответствующих журналах.

4.8. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя СКЗИ. Дубликат ключа от хранилища ответственного пользователя СКЗИ в опечатанной упаковке должен быть передан на хранение оператору под расписку в соответствующем журнале.

4.9. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале ответственному пользователю СКЗИ или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей СКЗИ, ответственных за эти хранилища.

4.10. При утрате ключа от хранилища или от входной двери в режимное

помещение 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 хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает оператор или ответственный пользователь СКЗИ.

4.11. В обычных условиях опечатанные хранилища могут быть вскрыты только пользователями СКЗИ, ответственным пользователем СКЗИ или ответственным за защиту информации, в том числе за обеспечение безопасности ПДн в ИС. Режимные помещения могут быть вскрыты только сотрудниками, имеющими право вскрытия таких помещений согласно утверждённому списку.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ или ответственному за защиту информации, в том числе за обеспечение безопасности ПДн в ИС. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации защищаемой информации и к замене скомпрометированных криптоключей.

4.12. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования 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 противном случае по согласованию с ответственным пользователем СКЗИ необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

Зам. директора по БЖ А.С. Балахнин