Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Самарский государственный экономический университет»

ПРИКАЗ

Самара

№ 464 - ОВ **«06» августа 2024 года**

По общим вопросам

Об эксплуатации средств криптографической защиты информации

В соответствии с Федеральным законом от 14.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом Федерального Агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (далее - приказ ФАПСИ), приказом Федеральной службы безопасности от 09.02.2005 №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (далее – приказ ФСБ) и в целях организации и обеспечения эксплуатации средств криптографической защиты информации, предназначенными для работы с квалифицированной электронной подписью (далее - СКЗИ)

ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по обеспечению безопасности эксплуатации СКЗИ (Приложение 1).
2. Утвердить форму заключения о подготовке и допуске к самостоятельной работе с СКЗИ (Приложение 2).
3. Утвердить форму Журнала учета сотрудников допущенных к работе с СКЗИ (Приложение 3).
4. Утвердить форму Журнала учета ключей квалифицированной электронной подписи (Приложение 4).
5. Утвердить форму Журнала учета лицензий СКЗИ (Приложение 5).
6. Назначить лицом, ответственным за эксплуатацию СКЗИ (далее – Ответственное лицо), начальника отдела информационной безопасности С.П. Ткаченко
7. В период временного отсутствия Ответственного лица ответственность за эксплуатацию СКЗИ на ведущего инженера отдела технического администрирования Д.А. Мишурова.

8. Ответственному лицу при организации и обеспечении работы с СКЗИ и криптографическими ключами руководствоваться:

- приказом Федерального Агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- приказом Федеральной службы безопасности от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
- эксплуатационной и технической документацией на средства криптографической защиты информации.

9. Считать утратившим силу приказ от 11.07.2023г.№448-ОВ.

10. Контроль за исполнением настоящего приказа возложить на проректора по безопасности и управлению хозяйственным комплексом А.А. Максимова.

И.о. ректора Е.А. Кандрашина

Разработал:
Начальник отдела ИБ
С.П. Ткаченко
тел.(846)933-88-09 (вн.502)

Приложение 1
к приказу №464-ОВ от «06» 08 2024 г.

Инструкция
по обеспечению безопасности эксплуатации СКЗИ

1. Термины и определения

1.1. В настоящей инструкции по обеспечению безопасности эксплуатации СКЗИ (далее – Инструкция) применяются следующие термины и определения:

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

Средство криптографической защиты информации (СКЗИ) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении;

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

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

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;

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

Ответственный за эксплуатацию СКЗИ – сотрудник, осуществляющий организацию и обеспечение работ по техническому обслуживанию СКЗИ и управление криптографическими ключами;

Пользователи СКЗИ – работники, непосредственно допущенные к работе с СКЗИ.

2. Общие положения

2.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ, входящих в состав средств криптографической защиты, а также порядок их изготовления, смены, уничтожения и действий сотрудников при компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

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

2.3. СКЗИ эксплуатируются в соответствии с правилами пользования и используют сертифицированные Федеральной службой безопасности России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

2.4. Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях следующих нормативно-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 Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием

СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- Приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

2.5. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом назначается Ответственный за эксплуатацию СКЗИ. Ответственный за эксплуатацию СКЗИ осуществляет:

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

2.6. Обучение пользователей правилам работы с СКЗИ осуществляет Ответственный за эксплуатацию СКЗИ.

2.7. Текущий контроль, обеспечение функционирования СКЗИ возлагается на Ответственного за эксплуатацию СКЗИ.

2.8. Ответственный за эксплуатацию СКЗИ и пользователи СКЗИ должны быть ознакомлены с настоящей Инструкцией под подпись.

3. Порядок допуска пользователей к работе с СКЗИ

3.1. Для работы с СКЗИ привлекаются должностные лица, допущенные к работе с СКЗИ в соответствии с приказом.

3.2. Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами, указанными в пункте 2.5 данной инструкции и проходит обучение правилам работы с СКЗИ, которое проводит Ответственный за эксплуатацию СКЗИ.

3.3. Пользователь считается допущенным к работе с СКЗИ после получения положительного «Заключения о подготовке и допуске к самостоятельной работе со СКЗИ».

4. Учет и хранение СКЗИ и криптографических ключей

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

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

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

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

4.5. При необходимости пользователю выдается документация по эксплуатации СКЗИ с последующим возвратом лицу, Ответственному за эксплуатацию СКЗИ.

4.6. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у Ответственного за эксплуатацию СКЗИ. Криптографические ключи хранятся у пользователей СКЗИ. Хранение осуществляется в закрываемых на замок металлических хранилищах в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение и/или в опечатанном пенале (тубусе). Металлические шкафы

должны быть оборудованы внутренними замками с двумя экземплярами ключей и/или кодовыми замками, и приспособлениями для опечатывания. Один экземпляр ключа от хранилища должен находиться у Ответственного за эксплуатацию СКЗИ. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе.

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

4.8. На ключевые носители с изготовленными криптографическими ключами наклеиваются наклейки, содержащие серийный/учетный номер.

4.9. Резервный ключевой носитель помещается в конверт и опечатывается пользователем и ответственным за эксплуатацию СКЗИ.

4.10. Ключевые носители с неработоспособными криптографическими ключами Ответственный за эксплуатацию СКЗИ принимает от пользователя под подпись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

4.11. При необходимости замены наклейки на ключевом носителе (стирание надписи реквизитов) пользователь передает его ответственному за эксплуатацию СКЗИ, который в присутствии пользователя снимает старую наклейку и приклеивает новую наклейку с учетным номером и записью в Журнале.

4.12. 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.

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

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

4.15. Ключевые носители совместно с Журналом должны храниться у Ответственного за эксплуатацию СКЗИ в сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Журнал совместно с другими документами, при этом ключевые носители и Журнал должны быть помещены в отдельную папку.

4.16. На время отсутствия Ответственного за эксплуатацию СКЗИ приказом ректора назначается сотрудник его замещающий.

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

5. Использование СКЗИ и криптографических ключей

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

5.2. Криптографический ключ невозможно использовать, если истек срок действия лицензии.

5.3. Для обеспечения контроля доступа к СКЗИ системный блок автоматизированного рабочего места (далее – АРМ) опечатывается Ответственным за эксплуатацию СКЗИ.

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

5.5. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения Ответственному за эксплуатацию СКЗИ и предоставить ему носители криптографических ключей для проверки их работоспособности. Проверку работоспособности

носителей криптографических ключей Ответственный за эксплуатацию СКЗИ выполняет в присутствии пользователя.

5.6.В случае если рабочий криптографический ключ потерял работоспособность, то по просьбе пользователя Ответственный за эксплуатацию СКЗИ вскрывает конверт (коробку) с резервными криптографическими ключами, делает копию ключевого носителя, используя резервный криптографический ключ, помещает резервный криптографический ключ в конверт (коробку), а новый ключевой носитель со своим серийным\учетным номером заносит в Журнал и выдает пользователю.

5.7. Вскрытие системного блока АРМ, на которой установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии Ответственного за эксплуатацию СКЗИ.

6. Обязанности пользователей СКЗИ

6.1. Пользователи СКЗИ обязаны:

- не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
- сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
- не разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;
- не выводить ключевую информацию на дисплей и(или) принтер;
- не вставлять ключевой носитель в порт АРМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в порты других АРМ;
- не записывать на ключевом носителе постороннюю информацию;
- не использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).
- сообщать Ответственному за эксплуатацию СКЗИ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять Ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

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

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

6.4. Все полученные обладателем информации ограниченного доступа экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под роспись в Журнале учета СКЗИ, несущим персональную ответственность за их сохранность.

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

7. Действия при компрометации криптографических ключей

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

- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами;
- потеря ключевых носителей с рабочими и/или резервными криптографическими ключами с последующим их обнаружением;
- увольнение сотрудников, имевших доступ к рабочим и/или резервным криптографическим ключам;
- возникновение подозрений относительно утечки информации или ее искажения;
- нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с рабочими и/или резервными криптографическими ключами, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с рабочими и/или резервными криптографическими ключами;
- временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

7.2. В случае возникновения обстоятельств, указанных в п. 7.1 настоящей Инструкции, пользователь обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и информировать Ответственного за эксплуатацию СКЗИ о факте компрометации криптографических ключей.

7.3. Решение о компрометации криптографических ключей принимается на основании письменного уведомления о компрометации, подписанного Ответственным за эксплуатацию СКЗИ, с приложением, при необходимости, письменного объяснения пользователя по факту компрометации его криптографических ключей.

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

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

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

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

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

8. Уничтожение криптографических ключей

8.1. Неиспользованные или выведенные из эксплуатации криптографические ключи подлежат уничтожению.

8.2. Уничтожение криптографических ключей на ключевых носителях производится Ответственным за эксплуатацию СКЗИ.

8.3. Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного

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

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

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

8.5. В Журнале учета СКЗИ производится отметка об уничтожении криптографических ключей.

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

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

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

9.3. Двери Помещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей выдают работникам, имеющим право допуска в Помещения, под роспись. Дубликаты ключей от входных дверей таких Помещений следует хранить в опечатанном тубусе на центральном посту охраны.

9.4. Для предотвращения просмотра извне Помещений окна должны быть защищены или экраны мониторов должны быть повернуты в противоположную сторону от окна.

9.5. Помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания.

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

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

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

Приложение 2
к приказу №464-ОВ от «06» 08 2024 г.

Заключение
о подготовке и допуске к самостоятельной работе
с СКЗИ

_____
(должность, фамилия, имя, отчество сотрудника)

_____
(наименование СКЗИ, по которому осуществлялась подготовка)

Настоящим подтверждается, что пользователь СКЗИ ознакомлен с инструкцией по обеспечению безопасности эксплуатации СКЗИ и со следующими обязанностями:

- не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптоключах;
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать лицу, ответственному за эксплуатацию СКЗИ, сведения 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 исполнения обязанностей, связанных с использованием СКЗИ;
- немедленно уведомлять лицо ответственное 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.

С заключением
ознакомлен(а):

«___» _____ 20__ г. _____ _____
(дата) (подпись) (фамилия, инициалы)

Лицо, ответственное за
эксплуатацию СКЗИ:

«___» _____ 20__ г. _____ _____.
(дата) (подпись) (фамилия, инициалы)

Приложение 3
к приказу №464-ОВ от «06» 08 2024 г.

Журнал учета
сотрудников, допущенных к работе с СКЗИ

Журнал начат «____» _____ 20___ г.
Должность _____

_____/
подпись *фамилия, имя, отчество*

Журнал завершен «____» _____ 20___ г.
Должность _____

_____/
подпись *фамилия, имя, отчество*

Журнал составлен на _____ листах

Приложение 4
к приказу №164-ОВ от «06» 08 2024 г.

Журнал
учета ключей квалифицированной электронной подписи

Журнал начат «____» _____ 20___ г.
Должность _____

_____/
подпись *фамилия, имя, отчество*

Журнал завершен «____» _____ 20___ г.
Должность _____

_____/
подпись *фамилия, имя, отчество*

Журнал составлен на _____ листах

№ п/п	Носитель СКЗИ	Серийный номер СКЗИ / Учетный номер	Номер экземпляра СКЗИ	УЦ изготовивший СКЗИ / ФИО установившего СКЗИ	Номер сертификата/ Владелец	ФИО получившего СКЗИ / Подпись	Дата изготовления СКЗИ	Дата уничтожения СКЗИ/ расписка владельца	Кабинет

Приложение 5
к приказу № 964-ОВ от «06» 08 2024 г.

Журнал
учета лицензий СКЗИ

Журнал начат «____» _____ 20___ г.
Должность _____

_____/
подпись *фамилия, имя, отчество*

Журнал завершен «____» _____ 20___ г.
Должность _____

_____/
подпись *фамилия, имя, отчество*

Журнал составлен на _____ листах

№ п/п	Владелец СКЗИ/Подпись	Имя ПК/ Инв.№	Кабинет	Серийный номер лицензии/ версия ПО	Дата установки