

**УТВЕРЖДАЮ**

Директор МБОУ «Луковниковская  
СОШ им. вице-адмирала  
В.А.Корнилова»

Приказ № 40 от 24.03.2023 года

/ О.М.Васильева



## **ИНСТРУКЦИЯ**

### **о порядке учета и выдачи СКЗИ, электронной подписи, эксплуатационно-технической документации и ключевых документов в Автоматизированной системе управления сферой образования Тверской области**

#### **1 Общие положения**

1.1 Инструкция о порядке учета и выдачи СКЗИ, электронной подписи, эксплуатационно-технической документации и ключевых документов в Автоматизированной системе управления сферой образования Тверской области (далее – АСУ СО ТО) Государственного бюджетного учреждения «Центр информатизации образования Тверской области» (далее – Учреждение) регламентирует порядок проведения инструктажей и допуска сотрудников к работе с средствами криптографической защиты информации (далее – СКЗИ), применяемыми для обеспечения безопасности информации ограниченного доступа при ее обработке в АСУ СО ТО.

1.2 К СКЗИ относятся:

1.2.1 Средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

1.2.2 Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

1.2.3 Средства электронной подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи.

1.2.4 Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.2.5 Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

1.2.6 Ключевые документы (независимо от вида носителя ключевой информации).

1.3 В настоящей Инструкции используются следующие понятия и определения:

1.3.4 Доступ к информации – возможность получения информации и ее использования.

1.3.5 Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

1.3.6 Ключевой документ – физический носитель определенной структуры, содержащий криптоключи.

1.3.7 Компрометация криптоключа – утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

1.3.8 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 предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

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

1.3.10 Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

1.3.11 Модель угроз – перечень возможных угроз.

1.3.12 Пользователь криптосредства – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

1.3.13 Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

## **2 Учет СКЗИ и ключевых документов**

2.2 СКЗИ и ключевые документы подлежат поэкземплярному учету.

2.3 Все экземпляры СКЗИ и ключевых документов выдаются пользователям криптосредств под подпись в соответствующем журнале поэкземплярного учета.

2.4 Передача ключевых документов допускается только между пользователями криптосредств и администратором безопасности АСУ СО ТО под подпись в соответствующем Журнале поэкземплярного учета средств криптографической защиты информации,

эксплуатационной и технической документации к ним, ключевых документов. Аналогичная передача между пользователями криптосредств осуществляется с санкции администратора безопасности АСУ СО ТО.

2.5 Для исключения компрометации ключевых документов, на период отсутствия пользователя и в нерабочее время, ключевые документы убираются в защищенные хранилища (сейфы, железные ящики), которые, в свою очередь, закрываются на ключ и опечатываются.

2.6 Учет эксплуатационной и технической документации к криптосредствам:

2.6.4 Эксплуатационная и техническая документация к криптосредствам подлежит поэкземплярному учету.

2.6.5 Все экземпляры эксплуатационной и технической документации к криптосредствам выдаются пользователям криптосредств под роспись.

2.6.6 Передача эксплуатационной и технической документации к криптосредствам допускается только между пользователями криптосредств и администратором безопасности АСУ СО ТО. Аналогичная передача между пользователями криптосредств осуществляется с санкции администратора безопасности АСУ СО ТО.

2.7 Распространение ключевых документов:

2.7.4 Ключевые документы получают лично владельцем криптографического ключа в удостоверяющем центре.

2.8 Плановая смена ключевых документов:

1.1.1 Заказ на изготовление очередных ключевых документов, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

2.9 Внеплановая смена ключевых документов:

2.9.4 Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

### **3 Ответственность и контроль**

3.2 Текущий контроль за организацией и обеспечением учета и выдачи СКЗИ, ключевых документов, эксплуатационной и технической документации возлагается на администратора безопасности АСУ СО ТО в пределах его полномочий

3.3 Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

