УТВЕРЖДАЮ
Директор МБОУ «Луковниковская СОШ им. вице-адмирала В.А.Корнилова»
Приказ № 40 от 24.03.2023 года

_____ / О.М.Васильева
М.П.

ИНСТРУКЦИЯ

о порядке допуска сотрудников к самостоятельной работе с средствами криптографической защиты информации в Автоматизированной системе управления сферой образования Тверской области

1 Общие положения

1.1 Инструкция о порядке допуска сотрудников к самостоятельной работе с средствами криптографической защиты информации 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:

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

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

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

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

1.3.10 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.

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

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

1.3.13 Модель угроз – перечень возможных угроз.

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

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

2 Обязанности пользователей криптосредств

2.2 Пользователи криптосредств допускаются к работе с ними только после ознакомления под подпись с настоящей Инструкцией, Инструкцией о порядке учета и выдачи СКЗИ, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов, Инструкцией по обращению с сертифицированными ФСБ России СКЗИ,

другими документами, регламентирующими организацию и обеспечение безопасности информации.

2.3 При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

2.4 Пользователи криптосредств обязаны:

2.4.6 Не нарушать конфиденциальность закрытых ключей.

2.4.7 Не допускать снятие копий с ключевых документов, содержащих закрытые ключи.

2.4.8 Не допускать вывод закрытых ключей на дисплей (монитор) ПЭВМ или принтер.

2.4.9 Не допускать записи на ключевой документ посторонней информации.

2.4.10 Не допускать установки ключевых документов в другие ПЭВМ.

2.4.11 Обеспечить конфиденциальность информации о криптосредствах, других мерах защиты.

2.4.12 Точно соблюдать требования к к обеспечению безопасности криптосредств и ключевых документов к ним.

2.4.13 Хранить ключевые документы к криптосредствам в защищаемых хранилищах.

2.4.14 Сдавать ключевые документы к криптосредствам при увольнении или отстранении от исполнения обязанностей.

2.4.15 Своевременно выявлять и сообщать администратору безопасности АСУ СО ТО о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним.

2.4.16 Немедленно уведомлять администратора безопасности АСУ СО ТО и принимать меры по предупреждению нарушения конфиденциальности защищаемой информации при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности информации ограниченного доступа.

3 Порядок проведения инструктажа и допуска к работе с СКЗИ

3.2 Инструктаж сотрудников Учреждения проводится администратором безопасности АСУ СО ТО:

3.2.6 Вводный инструктаж – при приеме сотрудника на работу.

3.2.7 Периодический инструктаж – при необходимости, но не реже чем один раз в 3 года.

3.3 Факты проведения инструктажа сотрудников отмечаются в Журнале регистрации пользователей СКЗИ.

3.4 После прохождения инструктажа сотрудник допускается к самостоятельной работе с СКЗИ и несет персональную ответственность в соответствии с положениями настоящей Инструкции.

4 Ответственность и контроль

4.2 Текущий контроль за организацией и обеспечением порядка допуска сотрудников к самостоятельной работе с СКЗИ возлагается на администратора безопасности АСУ СО ТО в пределах его полномочий.

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

4.4 Администратор безопасности АСУ СО ТО несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности информации ограниченного доступа с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

Лист ознакомления

№ п/п	Должность	Фамилия, Имя, Отчество	Дата ознакомления	Подпись