Государственное казенное общеобразовательное учреждение
«Михайловская школа – интернат»

УТВЕРЖДАЮ:
Директор
ГКОУ «Михайловская школа-интернат»
_____ И.Ю. Акимова
«26» _____ 2022г.

Инструкция
пользователю по обеспечению безопасности информации при эксплуатации средств криптографической защиты информации «Континент TLS Клиент» пользовательских сегментов государственной информационной системы «Единая информационная система в сфере образования Волгоградской области» в ГКОУ «Михайловская школа-интернат»

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1. Настоящая инструкция определяет порядок обеспечения информационной безопасности при эксплуатации пользователями средств криптографической защиты информации «Континент TLS Клиент» (далее - СКЗИ) при их использовании в составе пользовательских сегментов государственной информационной системы «Единая информационная система в сфере образования Волгоградской области» (далее - АРМ ГИС).
2. Настоящая инструкция является дополнением к эксплуатационной документации на СКЗИ.
3. СКЗИ предназначены для защиты общедоступной информации и информации с ограниченным доступом (в т.ч. персональных данных), не содержащей сведений, составляющих государственную тайну.
4. Работники, использующие СКЗИ, должны быть ознакомлены с настоящей инструкцией и другими нормативными документами, регламентирующими порядок эксплуатации средств криптографической защиты информации под роспись.
5. Период непрерывной работы СКЗИ без выключения питания не должен превышать 3 недели. По окончании этого срока необходимо проводить перезагрузку компьютера с установленным СКЗИ.

2. ПРАВИЛА ЭКСПЛУАТАЦИИ СКЗИ.

1. Со СКЗИ могут использоваться только персональные отчуждаемые электронные ключевые носители с интерфейсом USB (Рутокен и др.) или идентификаторы Touch memory (iButton).
2. Запись посторонней информации на ключевые носители запрещается.
3. Хранение ключевых носителей должно осуществляться в опечатываемых личной печатью пользователя контейнерах (пеналах, дискобоксах и т.п.), шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.
4. Пользователи ГИС несут персональную ответственность за хранение личных ключевых носителей.
5. Пользователи должны использовать надежные пароли (не менее 8 символов) для защиты ключевой информации, размещаемой на ключевых носителях.
6. Срок действия ключей составляет не более 1 года.
7. Мероприятия по плановой замене криптоключей должны осуществляться не позже, чем за 10 дней до окончания срока их действия.

8. В качестве личных ключей пользователей применяются ключи электронной подписи и соответствующие им квалифицированные сертификаты ключей проверки электронной подписи, полученные в государственном казенном учреждении Волгоградской области «Центр информационных технологий Волгоградской области».
9. Ключевые носители с ключами пользователей (далее – ключевые документы) подлежат учету в журнале поэкземплярного учета ключевых документов Абонента.
10. Ключевые документы выводятся из действия в следующих случаях:
- при плановой смене ключевых документов;
- при компрометации ключевых документов;
- при повреждении ключевых документов.
11. Ключевая информация, срок действия которой истек, уничтожается путем переформатирования (очистки) ключевых носителей с использованием средства криптографической защиты информации «КриптоПро CSP», входящего в состав СКЗИ.
12. Выведенная из действия ключевая информация уничтожаются не позднее чем через трое суток после момента ее вывода из действия
13. Уничтожение ключей осуществляется с составлением акта либо под роспись пользователя и администратора информационной безопасности пользовательского сегмента ГИС в журнале поэкземплярного учета ключевых документов.
14. При каждом включении АРМ ГИС пользователь должен проверять сохранность печатей (или иных средств, обеспечивающих возможность контроля вскрытия) системного блока и разъемов рабочей станции.
15. Администратор безопасности пользовательского сегмента ГИС должен периодически (не реже 1 раза в квартал) проводить контроль целостности и легальности установленных копий программного обеспечения на рабочих станциях с установленными СКЗИ.
16. В случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ ГИС должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе администратора безопасности пользовательского сегмента ГИС и представителей подразделения, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.
17. Не допускается оставлять без контроля АРМ ГИС при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе должно осуществляться гашение экрана, возобновление активности экрана производится с использованием пароля доступа.
18. При обнаружении фактов компрометации, пользователь обязан немедленно прекратить использование скомпрометированных ключей и сообщить о факте компрометации администратору безопасности.

3. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ ГИС ПРИ КОМПРОМЕТАЦИИ КРИПТОКЛЮЧЕЙ.

1. К событиям, относящимся к компрометации ключей, относятся следующие ситуации:
1) утрата ключевых документов;
2) утрата ключного документа с последующим обнаружением;
3) увольнение сотрудников, имевших доступ к ключевой информации;
4) возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
5) нарушение целостности печатей на сейфах (шкафах, хранилищах), предназначенных для их хранения;

6) утрата ключей от сейфов (шкафов, хранилищ) в случае нахождения в них ключевых документов;

7) утрата ключей от сейфов (шкафов, хранилищ в случае нахождения в них ключевых документов с последующим обнаружением;

8) доступ посторонних лиц к ключевой информации.

2. При наличии оснований полагать, что криптоключи скомпрометированы, пользователь ГИС должен немедленно поставить в известность администратора информационной безопасности и должен прекратить использование скомпрометированных криптоключей.

3. Для расследования инцидента, связанного с компрометацией криптоключей Абонентом создается комиссия, по результатам работы которой составляется письменный отчет об инциденте информационной безопасности, с ведения о котором направляются Оператору.

4. После компрометации криптоключей Абонент обращается в ГКУ ВО «ЦИТ ВО» для их аннулирования и для выпуска новых криптоключей.

5. Возобновление работы с СКЗИ возможно только после замены скомпрометированных криптоключей.

6. Не допускается:

1) Осуществлять несанкционированное копирование ключевых носителей.

2) Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами).

3) Вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя.

4) Подключать к АРМ ГИС дополнительные устройства и соединители, не предусмотренные штатной комплектацией.

5) Работать на компьютере, если во время его начальной загрузки не проходит встроенный тест оперативной памяти, предусмотренный базовой системой ввода-вывода АРМ ГИС.

6) Вносить какие-либо изменения в программное обеспечение СКЗИ.

7) Изменять настройки, установленные программой установки СКЗИ или администратором.

8) Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации.

9) Осуществлять несанкционированное вскрытие системных блоков АРМ ГИС.