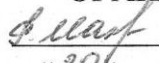


Министерство образования Белгородской области  
Областное государственное автономное  
профессиональное образовательное учреждение  
«Шебекинский техникум промышленности и транспорта»

**СОГЛАСОВАНО**

От имени трудового коллектива  
ОГАПОУ «ШТПТ»  
работником, действующим на  
основании предоставленных ему  
полномочий общим собранием трудового  
коллектива

ОГАПОУ «ШТПТ»

 Р.П. Махонина  
«30» 08 2024г.

**УТВЕРЖДЕНО**

Приказом директора  
ОГАПОУ «ШТПТ»

30.08.2024 г. №320/05-02

# ПОЛОЖЕНИЕ

по использованию средств криптографической  
защиты информации в ОГАПОУ «ШТПТ»

## 1. ОПРЕДЕЛЕНИЯ

1.1. **Администратор безопасности** - пользователь, уполномоченный выполнять действия (имеющий полномочия) по администрированию (управлению) системы защиты информации информационной системы персональных данных в соответствии с установленной ролью.

1.2. **Криптосредство** - шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

1.3. **Пользователь СКЗИ** - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

1.4. **Ответственный за организацию обработки персональных данных** - должностное лицо организации, эксплуатирующей информационную систему персональных данных, отвечающее за организацию обработки персональных данных.

1.5. **Криптоключ** - секретная информация, используемая криптографическим алгоритмом при шифровании/расшифровке сообщений.

## 2. СОКРАЩЕНИЯ

2.1. **ИС** - информационная система персональных данных.

2.2. **ОРД** - организационно - распорядительная документация по управлению обработкой ПДн в ИС и управлению системой защиты ИС.

2.3. **ПДн** - персональные данные.

2.4. **СКЗИ** - средства криптографической защиты информации.

2.5. **СЗИ** - средства защиты информации.

2.6. **ТС** - технические средства.

## 3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Положение по использованию средств криптографической защиты информации (далее по тексту - Положение) Областного государственного автономного профессионального образовательного учреждения «Шебекинский техникум промышленности и транспорта» (далее по тексту - Техникум) является локальным нормативным актом, устанавливающим правила управления, учета, хранения, выдачи и уничтожения шифровальных (криптографических) средств защиты информации (далее - СКЗИ); правила установки, хранения, размещения и монтаж СКЗИ; порядок утверждения, введения в действие и внесения изменений в настоящее Положение.

3.2. Настоящее Положение утверждается и вводится в действие приказом директора Техникума.

3.3. Настоящее Положение по использованию средств криптографической защиты информации (далее СКЗИ) в ИС разработано в соответствии со следующими нормативными правовыми актами и документацией на ИС и их системы защиты информации:

3.3.1. Приказом ФСБ Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации

требований к защите персональных данных для каждого из уровней защищенности».

3.3.2. Приказом ФСБ России от 9.02.2005 года №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (в ред. Приказа ФСБ РФ от 12.04.2010 N 173).

3.3.3. Приказом ФАПСИ 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».

3.3.4. Федеральным законом от 27.07.2006 года № 149 - ФЗ «Об информации, информационных технологиях и защите информации».

3.3.5. Федеральным законом от 27.07.2006 года № 152 - ФЗ «О персональных данных».

3.3.6. Приказом ФСТЭК России от 18.02.2013 года №21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных».

3.3.7. Приказом ФСТЭК России от 11.02.2013 года №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

3.3.8. Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационной системе персональных данных».

3.3.9. Нормативно - техническим документом «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР -К) (Утвержден приказом Гостехкомиссии России №282 от 30.08.2002).

3.3.10. ГОСТ Р 53114 - 2008 «Обеспечение информационной безопасности организации. Основные термины и определения».

3.4. Настоящее Положение предназначено для организации защиты ПДн с помощью СКЗИ.

3.5. Настоящее Положение при использовании в ИС СКЗИ и на основании Приказа ФСБ Российской Федерации №378 Часть 1, п.4 используется в Техникуме совместно с организационно - распорядительными документами по управлению обработкой и защитой ПДн в ИС.

3.6. При использовании СКЗИ требования настоящего Положения имеют преимущество перед требованиями организационно - распорядительной документации по управлению обработкой и защитой ПДн в ИС в отношении аналогичных объектов или процессов защиты.

3.7. Настоящее Положение вступает в силу после его утверждения директором Техникума и действует бессрочно, до момента его замены новым.

3.8. Для обеспечения функционирования и безопасности СКЗИ, на основании Приказа ФАПСИ при Президенте Российской Федерации от 13.06.2001 № 152, Приказа ФСБ Российской Федерации №378, директор Техникума приказом:

3.8.1. Либо назначает из числа сотрудников Техникума ответственного пользователя криптосредств.

3.8.2. Либо возлагает на ответственного за обеспечение безопасности персональных данных (администратора безопасности) Техникума (при наличии такой должности) обязанности ответственного пользователя криптосредств.

3.9. Обязанности ответственного пользователя криптосредств изложены в «Руководстве ответственного пользователя криптосредств».

3.10. Все пользователи СКЗИ участвуют в защите ПДн, обрабатываемых в ИС, и обязаны знать и выполнять требования:

3.10.1. Нормативно - правовых документов по защите ПДн.

3.10.2. Организационно - распорядительных документов по управлению системой защиты информации.

3.10.3. Настоящего Положения и перечисленных в нем инструкций, в части их касающейся.

3.10.4. «Руководства пользователя криптосредств».

## 4. УПРАВЛЕНИЕ СКЗИ

4.1. Управление СКЗИ осуществляется Техникумом с целью обеспечения безопасности обработки ПДн, с использованием криптосредств (Приказ ФСБ Российской Федерации №378 Часть 1, п.3).

4.2. Настоящее Положение регламентирует порядок управления СКЗИ на стадии эксплуатации СКЗИ в составе системы защиты информации ИС.

4.3. К управлению СКЗИ на этапе эксплуатации отнесены процедуры:

- учет СКЗИ;
- учет пользователей СКЗИ;
- контроль соблюдения условий использования СКЗИ;
- хранение, выдача, замена и уничтожение СКЗИ;
- действия при утере и компрометации СКЗИ;
- защита СКЗИ.

4.4. УЧЕТ СКЗИ

4.4.1. Учет СКЗИ осуществляет ответственный пользователь криптосредств в журнале учета СКЗИ, эксплуатационной и технической документации к ним.

4.5. Учет пользователей СКЗИ

4.5.1. Учет пользователей СКЗИ осуществляет ответственный пользователь криптосредств с помощью лицевых счетов пользователей СКЗИ.

4.6. Контроль соблюдения условий использования СКЗИ

4.6.1. Условия использования СКЗИ в ИС должны периодически, не реже 1 раза в год, проверяться на соответствие требованиям эксплуатации СКЗИ.

4.6.2. Проверки осуществляются комиссионно. Состав комиссии, сроки и порядок ее работы назначает ответственный за организацию обработки персональных данных.

4.6.3. Результаты проверок оформляются Актом результатов проверки условий использования СКЗИ по форме ПРИЛОЖЕНИЯ №1 к настоящему Положению.

4.6.4. В Акте результатов проверки условий использования СКЗИ должны быть отражены результаты проверки по следующим пунктам:

- состояние и актуальность Журнала учета СКЗИ;
- состояние и актуальность Лицевых счетов пользователей СКЗИ;
- соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИС и систему защиты информации;
- знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ.
- знание и выполнение пользователями правил защиты СКЗИ.

4.6.5. Если произошла потеря или компрометация СКЗИ, то ответственный за организацию обработки персональных данных назначает внеплановую проверку условий использования СКЗИ.

4.7. Действия при утере и компрометации СКЗИ

4.7.1. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи ответственный пользователь криптосредств должен немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

4.7.2. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя криптосредств, согласованного с ответственным за организацию обработки персональных, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

4.7.3. При обнаружении недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения ответственный пользователь криптосредств организует срочные меры к их розыску.

4.7.4. Организация, при утере и (или) компрометации СКЗИ, проводит мероприятия по устранению причин и последствий инцидента информационной безопасности в отношении СКЗИ. Порядок действий в этом случае регламентирован в организационно-распорядительной документации.

## **5. ПРАВИЛА УЧЕТА СКЗИ**

5.1. СКЗИ, используемые для обеспечения безопасности ПДн при их обработке в ИС, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

5.2. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярому учету в Журнале учета СКЗИ. Заполнение, хранение и ведение журнала учета СКЗИ осуществляет ответственный пользователь криптосредств.

5.3. Программные криптосредства учитываются в журнале учета СКЗИ совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

5.4. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств ИС, то такие криптосредства учитываются совместно с соответствующими аппаратными средствами, о чем вносится соответствующая запись в журнале учета СКЗИ.

5.5. Единицей поэкземплярного учета ключевых документов является ключевой блокнот.

5.6. Если один и тот же ключевой блокнот многократно используют для записи криптоключей, то его каждый раз регистрируют отдельно.

## **6. ПРАВИЛА ХРАНЕНИЯ СКЗИ**

6.1. Пользователи криптосредств должны хранить устанавливающие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального

пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

6.2. Пользователи криптосредств должны обеспечить отдельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

6.3. Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. Опечатывание (опломбирование) осуществляет ответственный пользователь криптосредств.

6.4. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища. Отключение и уборку криптосредств в опечатываемые хранилища производит пользователь этих криптосредств.

## **7. ПРАВИЛА ВЫДАЧИ СКЗИ**

7.1. Все экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов ответственный пользователь криптосредств выдает пользователям криптосредств под расписку в журнале поэкземплярного учета.

7.2. Ответственный пользователь криптосредств заводит и ведет на каждого пользователя криптосредств лицевой счет по форме ПРИЛОЖЕНИЯ №2, в котором регистрирует числящиеся за ним криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

7.3. Передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов пользователю криптосредств может производить только ответственный пользователь криптосредств под расписку в журнале поэкземплярного учета. Передача криптосредств между пользователями криптосредств запрещена.

## **8. ПРАВИЛА УНИЧТОЖЕНИЯ СКЗИ**

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

8.2. 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 криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

8.3. Ключевые носители уничтожаются путем 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 криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

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

8.5. Криптосредства уничтожаются (утилизируют) по приказу директора Техникума.

8.6. Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятими из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам процедура удаления программного обеспечения криптосредств, и они полностью отсоединены от аппаратных средств.

8.7. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

8.8. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документации не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения в журнал поэкземплярного учета заносит ответственный пользователь криптосредств.

8.9. Ключевые документы уничтожаются ответственным пользователем криптосредств.

8.10. Уничтожение большого объема ключевых документов может быть оформлено актом по установленной форме. Уничтожение по акту (ПРИЛОЖЕНИЕ №3) производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. 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, устанавливающих криптосредства носителей, эксплуатационной и технической документации.

## **9. УСТАНОВКА И ХРАНЕНИЕ СКЗИ**

9.1. Размер помещений для установки и хранения СКЗИ должен быть выбран с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией на СКЗИ.

9.2. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

9.3. Окна помещений, расположенных на первых и последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению в помещения.

9.4. Размещение и специальное оборудование в помещениях должны исключить возможность неконтролируемого просмотра посторонними лицами ведущихся там работ.

9.5. Для предотвращения просмотра извне помещений, в которых установлены или хранятся СКЗИ, их окна должны быть защищены.

9.6. Помещения должны быть оснащены охранной сигнализацией, связанной со

9.7. Охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц.

9.8. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается приказом директора Техникума.

9.9. Двери помещений, где установлены или хранятся СКЗИ, должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

9.10. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в помещения.

9.11. Дубликаты ключей от входных дверей помещений с установленными СКЗИ хранятся в сейфе ответственного пользователя криптосредствами.

9.12. Исправность сигнализации в помещениях, в которых установлены или хранятся СКЗИ, периодически, не реже раза в неделю, проверяет ответственный пользователь криптосредств совместно с представителем службы охраны или дежурным по организации.

9.13. По окончании рабочего дня помещение и установленные в нем хранилища СКЗИ должны быть закрыты и опечатаны. Закрывают и опечатывают помещения и хранилища СКЗИ назначенные приказом директора Техникума ответственные за хранилища или ответственный пользователь СКЗИ.

## **10. РАЗМЕЩЕНИЕ И МОНТАЖ СКЗИ**

10.1. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с криптосредствами, в соответствующих помещениях должны сводить к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

10.2. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

## **11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

11.1. Все пользователи криптосредств должны быть предупреждены об ответственности за действия с СКЗИ, нарушающие требования настоящего Положения и других организационных и правовых документов, определяющих меры по защите ПДн с помощью криптосредств.

11.2. Пользователи криптосредств, в том числе ответственный пользователь криптосредств должны быть ознакомлены в части их касающейся, с настоящим Положением до начала работы с криптосредствами под роспись. Обязанность ознакомления пользователей с настоящим Положением лежит на ответственном за организацию обработки персональных данных .

11.3. Настоящее утверждается и вводится в действие приказом директора Техникума.

11.4. Изменения и дополнения к настоящему Положению утверждаются в форме проекта изменений к настоящему Положению и вводятся в действие приказом директора Техникума.

АКТ № \_\_\_\_\_  
проверки соблюдения условий использования средств  
криптографической защиты информации

Дата составления: «\_\_\_» \_\_\_\_\_ 202\_\_ г.

Место проведение проверки: \_\_\_\_\_

Комиссия, назначенная приказом руководителя  
от «\_\_» 20 \_\_\_\_\_ № \_\_\_\_\_ в составе:

Председатель: \_\_\_\_\_

Члены комиссии: \_\_\_\_\_

---

Руководствуясь требованиями «Положения по использованию средств криптографической защиты информации» проведена проверка соблюдения условий использования средств криптографической защиты информации в информационной системе персональных данных ОГАПОУ «ШТПТ».

В ходе проведения проверки определялись:

1. Состояние и актуальность журнала учета СКЗИ;
2. Соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИС и систему защиты информации;
3. Знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ;
4. Знание и выполнение пользователями правил защиты СКЗИ;
5. Случаи компрометации СКЗИ и действия по устранению причин и последствий компрометации СКЗИ;
6. Состояние помещений с установленными или хранящимися в них СКЗИ и состояние режима доступа в эти помещения;
7. Наличие и состояние хранилищ СКЗИ и режим доступа к ним.

Выявленные нарушения: \_\_\_\_\_

ЗАКЛЮЧЕНИЕ комиссии:

Соблюдений условий использования средств криптографической защиты информации соответствует / не соответствует *(нужное подчеркнуть)* требованиям к условиям использования СКЗИ в ФАУ ДПО ИПКЛХ.

Председатель комиссии \_\_\_\_\_

Члены комиссии: \_\_\_\_\_

ЖУРНАЛ  
учета пользователей средств криптографической защиты информации

№ п.п.	ФИО пользователя СКЗИ	Наименование СКЗИ	Номер помещения, где размещено СКЗИ	Подпись пользователя СКЗИ, прошедшего инструктаж документов	ФИО и подпись ответственного пользователя СКЗИ	Дата получения

АКТ № \_\_\_\_\_  
уничтожения криптографических средств защиты информации

Проведен отбор СКЗИ, применяемых ранее в информационной системе ОГАПОУ «ШТПТ» и установлено, что в соответствии с действующими требованиями отобранные СКЗИ подлежат уничтожению:

№	Дата	Наименование СКЗИ	Регистрационный номер СКЗИ	Примечание

Всего экземпляров СКЗИ \_\_\_\_\_  
(цифрами и прописью количество)

На указанных экземплярах СКЗИ информация уничтожена путем \_\_\_\_\_  
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные экземпляры СКЗИ уничтожены путем \_\_\_\_\_  
(механического уничтожения, сжигания и т.п.)

Пользователь СКЗИ: \_\_\_\_\_  
(подпись)

\_\_\_\_\_ (расшифровка)