Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение
«Политехнический колледж городского хозяйства»

Организационно-правовая документация

УТВЕРЖДЕНО
приказом директора
от 01.06 2023
№ 544 - ОД

ПОЛОЖЕНИЕ

ПО ИСПОЛЬЗОВАНИЮ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ В САНКТ-ПЕТЕРБУРГСКОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ «ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ ГОРОДСКОГО ХОЗЯЙСТВА»

Санкт-Петербург - 2023

	Должность	Фамилия И.О.	Подпись	Дата
Разработал	Специалист по защите информаций	Бабин С.А.		01.06.2023
Согласовано	Зам. директора по ПО	Бурдин Е.В.		01.06.2023.
Согласовано	Начальник отдела ИО и ПП	Ваганов С.Н..		01.06.2023
Согласовано	Начальник отдела ДОУ	Шорина А.В.		01.06.2023

Приложение № 5

УТВЕРЖДЕНО
приказом директора
от _____2023
№ _____-ОД

ПОЛОЖЕНИЕ

по использованию средств криптографической защиты информации организации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства»

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. **ИСПДн** – информационная система персональных данных.

2.2. **ОРД** – организационно – распорядительная документация по управлению обработкой ПДн в ИСПДн и управлению системой защиты ИСПДн.

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. Настоящее «Положение по использованию средств криптографической защиты информации организации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства» (далее – Положение) в информационных системах (в том числе - в ИСПДн) организации Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Политехнический колледж городского хозяйства» (далее – Организация) разработано в соответствии со следующими нормативными правовыми актами и документацией на системы и их системы защиты информации:

3.1.1. Федеральным законом от 27 июля 2006 года № 149 – ФЗ «Об информации, информационных технологиях и защите информации».

3.1.2. Федеральным законом от 27 июля 2006 года № 152 – ФЗ «О персональных данных».

3.1.3. Постановлением Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.1.4. Приказом ФСБ Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах 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».

3.1.5. Приказом ФСБ России от 09 февраля 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 апреля 2010 года № 173).

3.1.6. Нормативно – техническим документом «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) (Утвержден приказом Гостехкомиссии России от 30 августа 2002 года
№ 282).

3.1.7. ГОСТ Р 53114 – 2008 «Обеспечение информационной безопасности в организации. Основные термины и определения».

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

3.3. Настоящее Положение при использовании в ИСПДн СКЗИ используется в Организации совместно с организационно - распорядительными документами по управлению обработкой и защитой ПДн в ИСПДн.

3.4. При использовании СКЗИ требования настоящего Положения имеют преимущество перед требованиями организационно – распорядительной

документации по управлению обработкой и защитой ПДн в ИСПДн в отношении аналогичных объектов или процессов защиты.

3.5. Настоящее Положение вступает в силу после его утверждения руководителем Организации и действует бессрочно, до момента его замены новым.

3.6. Для обеспечения функционирования и безопасности СКЗИ руководитель Организации приказом:

3.6.1. либо назначает из числа сотрудников Организации ответственного пользователя криптосредств;

3.6.2. либо возлагает на ответственного за обеспечение безопасности персональных данных (администратора безопасности) Организации (при наличии такой должности) обязанности ответственного пользователя криптосредств.

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

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

3.8.1. нормативно – правовых документов по защите ПДн;

3.8.2. организационно – распорядительных документов по управлению системой защиты информации.

3.8.3. настоящего Положения в части их касающейся;

3.8.4. «Руководства пользователя криптосредств».

4. Управление СКЗИ

4.1. Управление СКЗИ осуществляется Организацией с целью обеспечения безопасности обработки ПДн, с использованием криптосредств (пункт 3 части I Приказа ФСБ Российской Федерации № 378).

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

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.

Учет пользователей СКЗИ достигается учетом Приказов о назначении пользователей СКЗИ в принятом порядке обеспечения делопроизводства в Организации.

4.6. Контроль соблюдения условий использования СКЗИ.

4.6.1. Условия использования СКЗИ в ИСПДн должны периодически, не реже 1 раза в год, проверяться на соответствие требованиям эксплуатации СКЗИ.
4.6.2. Проверки осуществляются комиссией. Состав комиссии, сроки и порядок ее работы, форма оформления результатов определены в действующей редакции «Инструкции контроля защищенности персональных данных» и «Правил осуществления внутреннего контроля обработки персональных данных на соответствие требованиям к их защите».
4.6.3. В Акте результатов проверки условий использования СКЗИ должны быть отражены результаты проверки по следующим пунктам:
– состояние и актуальность журнала учета СКЗИ;
– состояние и актуальность журнала учета пользователей СКЗИ;
– соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИСПДн и систему защиты информации;
– знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ;
– знание и выполнение пользователями правил защиты СКЗИ.
4.6.4. 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 данных, 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.

5. Правила учета СКЗИ

5.1. СКЗИ, используемые для обеспечения безопасности ПДн при их обработке в ИСПДн, 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 поэкземплярному учету в журнале учета СКЗИ по форме Приложения № 1. 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 ИСПДн, 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 инсталлирующие 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 раздельное 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. 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) производиться 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 уничтожают 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 уничтожают путем сжигания или с помощью любых бумагорезательных машин.

8.5. Криптосредства уничтожают (утилизируют) по приказу руководителя Организации.

8.6. Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми 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 документацией 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 № 2) 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, инсталлирующих криптосредства носителей, эксплуатационной и технической документации.

9. Требования к помещениям для установки и хранения 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 службой охраны здания или дежурным по Организации.

10. Режим работы помещений для установки и хранения СКЗИ

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

10.2. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается приказом руководителя Организации.
10.3. Двери помещений, где установлены или хранятся СКЗИ, должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.
10.4. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в помещения.
10.5. Дубликаты ключей от входных дверей помещений с установленными СКЗИ хранятся в сейфе ответственного пользователя криптосредствами.
10.6. 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.
10.7. По окончании рабочего дня помещение и установленные в нем хранилища СКЗИ должны быть закрыты и опечатаны. Закрывают и опечатывают помещения и хранилища СКЗИ ответственный пользователь СКЗИ.

11. Требования к размещению и монтажу СКЗИ

11.1. 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.
11.2. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

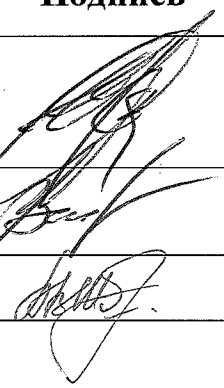
12. Заключительные помещения

12.1. 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.
12.2. 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.

Разработчик:
Специалист по защите информации
отдела ИО и ПП С.А.Бабин

ЛИСТ СОГЛАСОВАНИЯ

к «Положению по использованию средств криптографической защиты информации организации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства»

Ф.И.О.	Должность	Подпись	Дата
Бурдин Е.В	Заместитель директора по ПО		01.06.23
Ваганов С.В.	Начальник отдела ИО и ПП		01.06.2023
Шорина А.В	Начальник отдела ДОУ		01.06.2023

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

к «Положению по использованию средств криптографической защиты информации организации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства»

Информация о внесенных изменениях					
№ изменения	№ листа	№ и дата приказа	Дата внесения изменения	Дата введения изменения в действие	Подпись лица, внесшего изменения
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

Информация о проведении актуализации		
Дата ежегодной актуализации	Результаты актуализации	Подпись разработчика

Приложение № 1
к Положению по использованию
средств криптографической
защиты информации

ЖУРНАЛ

учета средств криптографической защиты информации

Учетный № _____

202____ год. Листов (_____)

№	Наименование СКЗИ	Регистрационные номера СКЗИ	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя СКЗИ, производившего подключение (установку	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

ПРАВИЛА

по формированию и ведению журнала поэкземплярного учета СКЗИ

В соответствии с требованиями Положения ПКЗ-2005 все используемые или хранимые СКЗИ подлежат поэкземплярному учету по установленным формам.

Настоящая инструкция определяет порядок ведения журнала поэкземплярного учета СКЗИ при осуществлении распространения СКЗИ в соответствии с условиями действия лицензии ФСБ России.

1. Формирование журнала.

1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации.
1.2. Обложка журнала изготавливается из листов плотностью 100-120 г/м2.
1.3. Все листы журнала, за исключением листов обложки, нумеруются.
1.4. Все листы журнала сшиваются и опечатываются, при этом на наклейке, фиксирующей прошивку, указывается количество пронумерованных и прошитых листов, ставится подпись заместителя руководителя ОКЗ и оттиск печати организации.

2. Ведение журнала.

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

2.1. Графы журнала заполняются следующим образом:
2.2. Графа 1 – номер записи по порядку.
2.3. Графа 2 – наименование СКЗИ.
2.4. Возможные варианты:
2.5. ViPNet CSP, версия 4.2.
2.6. ViPNet Клиент КС2, версия 4.2.
2.7. ViPNet Координатор КС2, версия 4.2.
2.8. ViPNet Координатор КС2 Linux.
2.9. Домен-КС2 [ViPNet КриптоСервис].

2.10.Графа 3 – серийный (регистрационный) номер СКЗИ.
2.11.Графа 4 – 1 (если лицензия на одну установку) или по порядку.
2.12.Графа 5 – наименование организации, передавшей СКЗИ.
2.13.Графа 6 – указывается дата установки.
2.14.Графа 7 – ФИО лица, на чьем компьютере произведена установка.
2.15.Графа 8 – Расписка лица по п. 7.
2.16.Графа 9 – ФИО лица, производившего установку СКЗИ при передаче через агента, или наименование организации, установившей СКЗИ.
2.17.Графа 10 – дата установки.
2.18.Графа 11 – серийный или инвентарный номер компьютера.
2.19.Графа 12 – не заполняется.
2.20.Графа 13 – не заполняется.
2.21.Графа 14 – не заполняется.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.

Приложение № 2
к Положению по использованию средств криптографической защиты информации

Акт № _____

уничтожения криптографических средств защиты информации

Проведен отбор СКЗИ, применяемых ранее в информационной системе персональных данных _____ (название) установлено, что в соответствии с действующими требованиями отобранные СКЗИ подлежат уничтожению:

№	Дата	Наименование СКЗИ	Регистрационный номер СКЗИ	Номер экземпляра ключевых документов	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)*

ЛИСТ ОЗНАКОМЛЕНИЯ

с «Положением по использованию средств криптографической защиты информации организации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства»

(утверждено приказом от «01» 06 2023 №544-од)

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата