



Российская Федерация
Тюменская область
Ханты-Мансийский автономный округ – Югра
г. Мегион

**Муниципальное бюджетное учреждение
«Централизованная библиотечная система»**

628684 ХМАО – Югра
г. Мегион, ул. Заречная 16а
тел./ факс: (34663) 3-21-36; 3-45-00

E-mail: megalib@mail.ru
Адрес сайта: <http://megionlib.ru/>

ПРИКАЗ

04.03.2022

№33-О

о назначении ответственного за эксплуатацию и
хранение средств криптографической защиты информации

Во исполнение "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", утвержденной приказом ФАПСИ от 13 июня 2001 г. N 152,

приказываю:

1. Назначить заведующего отделом автоматизации, сетевых технологий и электронных ресурсов Булыгина Андрея Владимировича ответственным за эксплуатацию и хранение средств криптографической защиты информации в муниципальном бюджетном учреждении «Централизованная библиотечная система».

2. Утвердить Инструкцию по эксплуатации криптосредств и криптографических ключей к ним в муниципальном бюджетном учреждении «Централизованная библиотечная система» (Приложение 1).

3. Ответственному должностному лицу при организации и обеспечении работы со средствами криптографической защиты информации и криптографическими ключами, а также при осуществлении хранения средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов руководствоваться "Инструкцией по эксплуатации криптосредств и криптографических ключей к ним в муниципальном бюджетном учреждении «Централизованная библиотечная система»".

4. Возложить на назначенное должностное лицо персональную ответственность за сохранность всех экземпляров средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

5. Утвердить Список работников муниципального бюджетного учреждения «Централизованная библиотечная система», наделенных правом электронной подписи электронных документов (Приложение 2).

6. Утвердить следующие журналы:

- Журнал учета антивирусных проверок (Приложение 3);

- Журнал учета паролей по информационной системе персональных данных (ИСПДн) (Приложение 4);

- Журнал учета инцидентов информационной безопасности (Приложение 5);

- Журнал учета передачи персональных данных (Приложение 6);

7. Контроль за исполнением приказа оставляю за собой.

Директор

Т.В.Котлярова

ИНСТРУКЦИЯ

по эксплуатации криптосредств и криптографических ключей к ним в муниципальном бюджетном учреждении «Централизованная библиотечная система»

1. Общие положения

1.1. Настоящие Инструкция по эксплуатации криптосредств и криптографических ключей к ним в муниципальном бюджетном учреждении «Централизованная библиотечная система» (далее - Инструкция) определяют порядок учета, хранения и использования криптосредств и криптографических ключей, а также порядок изготовления, смены и уничтожения криптографических ключей в целях обеспечения безопасности эксплуатации криптосредств.

1.2. Настоящие Инструкция разработаны на основе следующих документов:

- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом Федеральной службы безопасности России от 09.02.2005 N 66;

- Инструкция 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", утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 N 152;

- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 №1119.

1.3. В настоящей Инструкции используются следующие термины и определения:

- **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- **персональные данные** - любая информация, относящаяся прямо или косвенно к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

- **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;

- **криптографическая защита** - защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования;

- **открытый ключ** - уникальная последовательность данных, связанная с закрытым ключом с помощью особого математического соотношения. Открытый ключ пользователя известен всем другим пользователям, но это не позволяет вычислить закрытый ключ;

- **закрытый ключ** - уникальная последовательность данных, которая известна только владельцу ключа и сохраняется им в тайне;

- **криптографические ключи** - открытый и закрытый ключи;

- **ключевой документ** - контейнер с криптографическими ключами на ключевом носителе;

- **компрометация ключа** - хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых теряется доверие к тому, что используемые ключи обеспечивают безопасность информации;

- **ПЭВМ** - персональная электронно-вычислительная машина (персональный компьютер);

- остальные термины и определения, используемые в настоящих правилах, должны пониматься в соответствии с законодательством Российской Федерации.

1.4. Настоящая Инструкция является обязательной для всех пользователей криптосредств.

2. Организация деятельности по эксплуатации криптосредств

2.1. При осуществлении деятельности с криптосредствами следует производить:

- установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к ним;

- проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;

- обучение сотрудников, использующих криптосредства (пользователей криптосредств), работе с ними;

- поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним;

- учет пользователей криптосредств;

- контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

- разбирательство и составление заключений по фактам нарушения условий использования криптосредств.

2.2. Пользователи криптосредств допускаются к работе с криптосредствами приказом оператора и несут персональную ответственность за сохранность криптосредств, ключевой, эксплуатационной и технической документации, эксплуатируемых пользователем.

2.3. Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее - ответственный пользователь криптосредств). Функции ответственного пользователя криптосредств возлагаются на одного из пользователей криптосредств. На время отсутствия ответственного пользователя криптосредств должен быть назначен сотрудник, его замещающий.

2.4. Пользователи криптосредств обязаны соблюдать требования настоящих правил и других документов, принятых у оператора, регламентирующих эксплуатацию криптосредств, и несут ответственность за несоблюдение ими данных требований в соответствии с законодательством Российской Федерации.

2.5. Перед началом работы с криптосредствами пользователи криптосредств должны пройти советующий инструктаж.

2.6. Ознакомление пользователей криптосредств с документами по эксплуатации криптосредств осуществляет ответственный пользователь криптосредств .

3. Учет, хранение, передача криптосредств и криптографических ключей к ним

3.1. Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземпляруному учету ответственным пользователем криптосредств в журнале поэкземпляруного учета криптосредств, эксплуатационной и технической документации к ним (далее - журнал поэкземпляруного учета).

3.2. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к одному из внутренних интерфейсов аппаратных средств, такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

3.3. Единицей поэкземпляруного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.4. Крипсредства подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

3.5. Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземпляруного учета пользователям криптосредств и несущим персональную ответственность за их сохранность.

3.6. Инсталлирующие криптосредства носители, эксплуатационная и техническая документация к криптосредствам, ключевые документы, в том числе резервные ключевые документы пользователей криптосредств, предназначенные для применения в случае компрометации действующих ключевых документов, хранятся у ответственного пользователя криптосредств.

3.7. Ключевые носители с криптографическими ключами хранятся у пользователей криптосредств.

3.8. Хранение осуществляется в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.9. Если у пользователя криптосредств отсутствует шкаф (ящик, хранилище) индивидуального пользования, ключевые носители с криптографическими ключами по окончании рабочего дня в опечатанном пенале сдаются ответственному пользователю криптосредств.

3.10. Ключевые носители с неработоспособными криптографическими ключами ответственный пользователь криптосредств принимает от пользователя криптосредств и делает соответствующие пометки журнале поэкземпляруного учета. Неработоспособные криптографические ключи подлежат уничтожению.

3.11. 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) должно быть таким, чтобы его можно было визуальнo контролировать.

3.12. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища. В противном случае по согласованию с ответственным пользователем криптосредств необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

3.13. Вскрытие системного блока ПЭВМ, на которой установлено криптосредство, для проведения ремонта или технического обслуживания должно осуществляться в

присутствии ответственного пользователя криптосредств, который осуществляет контроль за криптосредствами во время проведения работ и производит опечатывание после окончания работ.

3.14 При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств.

3.15. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3.16. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

3.17. Криптосредства и ключевые документы могут доставляться курьерской, фельдъегерской (в том числе ведомственной) связью или со специально выделенными руководителем сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки. Эксплуатационную и техническую документацию к криптосредствам можно пересылать заказными или ценными почтовыми отправлениями.

3.18. Для пересылки криптосредств и ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптосредства пересылают отдельно от ключевых документов к ним. На упаковках указывают организацию или ответственного сотрудника, для которых эти упаковки предназначены. На таких упаковках делают пометку "Лично". Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

3.19. Для пересылки криптосредств, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также при необходимости - назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

3.20. Полученные упаковки вскрывает только ответственный пользователь криптосредств или ответственный сотрудник, для которого они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю. Полученные с такими отправлениями криптосредства и ключевые документы до получения указаний от отправителя применять не разрешается.

3.21. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует вернуть изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

3.22. Получение криптосредств, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать

доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

4. Изготовление и перевыпуск криптографических ключей

4.1. Криптографические ключи изготавливаются в соответствии с эксплуатационно-технической документацией на используемые криптосредства.

4.2. Криптографический ключ невозможно использовать если истек срок его действия.

4.3. Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно.

4.4. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи по заявлению пользователя криптосредств.

4.5. При замене криптографических ключей используют программное обеспечение в соответствии с эксплуатационной документацией на криптосредства.

5. Мероприятия при компрометации криптографических ключей

5.1. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей относится, включая, но не ограничиваясь, следующее:

- потеря ключевых носителей с криптографическими ключами;
- потеря ключевых носителей с криптографическими ключами с их последующим обнаружением;
- увольнение сотрудника, имевшего доступ к ключевым носителям с криптографическими ключами;
- исключение сотрудника из перечня лиц, допущенных к работе со средствами криптографической защиты информации;
- возникновение подозрений на утечку информации;
- нарушение печати (пломбы) шкафов (ящиков, хранилищ), аппаратных средств, с которыми осуществляется штатное функционирование криптосредств, а также аппаратных и аппаратно-программных криптосредств, где производилось опечатывание (опломбирование);
- неподконтрольный доступ посторонних лиц к ключевым носителям с криптографическими ключами (осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения);
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями с криптографическими ключами (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

5.2. В случае возникновения вышеуказанных обстоятельств пользователь криптосредств обязан незамедлительно прекратить работу с криптосредствами, в том числе обмен электронными документами, и уведомить ответственного пользователя криптосредств о возможной компрометации криптографических ключей.

5.3. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается по решению ответственного

пользователя криптосредств использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

5.4. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием конфиденциальных данных, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств.

5.5. Мероприятия по локализации последствий компрометации ключевых документов организует ответственный пользователь криптосредств.

6. Уничтожение криптографических ключей

6.1. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю криптосредств или по его указанию должны быть уничтожены на месте.

6.2. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:

- установить наличие оригинала и количество копий криптографических ключей;
- проверить внешним осмотром целостность каждого ключевого носителя;
- установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в журнале поэкземплярного учета;
- убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат удалению;
- произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

6.3. В журнале поэкземплярного учета ответственным пользователем криптосредств производится отметка об уничтожении соответствующих криптографических ключей.

6.4. Уничтожение криптоключей (исходной ключевой информации) может 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).

6.5. 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.

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

6.7. 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.

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 тому подобное), 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).

6.8. 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 оформляется в соответствующих журналах поэкземплярного учета. Хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

6.9. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в криптосредствах или иных дополнительных устройствах уничтожаются пользователями криптосредств самостоятельно под расписку в техническом (аппаратном) журнале.

6.10. Ключевые документы уничтожаются либо пользователями криптосредств, либо ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и тому подобное) ответственного пользователя криптосредств.

Уничтожение большого объема ключевых документов производит комиссия с оформлением акта. 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. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

7. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

7.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность конфиденциальных данных, криптосредств и ключевых документов к ним.

7.2. Режимные помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

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

7.4. Размещение, специальное оборудование, охрана и организация режима в режимных помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.5. Двери режимных помещений должны быть закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе.

7.6. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

7.7. Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Исправность сигнализации периодически необходимо проверять представителям службы охраны с отметкой в соответствующих журналах.

7.8. Для хранения ключевых документов, эксплуатационной и технической документации, устанавливающих криптосредства носителей, должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя криптосредств.

7.9. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале.

7.10. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный пользователь криптосредств.

7.11. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только сотрудниками, имеющими доступ в данные помещения, или руководителем.

7.12. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю криптосредств или руководителю. Прибывший ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять при необходимости меры к локализации последствий компрометации конфиденциальных данных и к замене скомпрометированных криптоключей.

7.13. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

Список работников муниципального бюджетного учреждения
«Централизованная библиотечная система», наделенных правом электронной
подписи электронных документов

№ п/п	Ф.И.О. сотрудника	Должность	Телефон
1	Котлярова Татьяна Владимировна	Директор	+7 (34643) 3-21-36
2	Рахимова Алсу Фадитовна	Главный бухгалтер	+7 (34643) 3-38-03
3	Коваль Оксана Владимировна	Специалист по договорам	+7 (34643) 3-45-00
4	Мериора Дмитрий Иванович	Заведующий отделом обеспечения деятельности учреждения	+7 (34643) 3-45-00
5	Булыгин Андрей Владимирович	Заведующий отделом автоматизации, сетевых технологий и электронных ресурсов	+7 (34643) 3-45-00
6	Плаксына Галина Петровна	Бухгалтер	+7 (34643) 3-38-03