ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
«ЦЕНТРАЛИЗОВАННАЯ БУХГАЛТЕРИЯ МОСКОВСКОЙ ОБЛАСТИ»

ПРИКАЗ

04.03.2026 № 34

г. Москва

Об утверждении порядка организации
и проведения работ по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных

Во исполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Политики в отношении обработки персональных данных Государственного казенного учреждения Московской области «Централизованная бухгалтерия Московской области» (далее — ГКУ МО ЦБ МО), утвержденной приказом ГКУ МО ЦБ МО от 26.09.2024 № 158 «Об утверждении документации, регламентирующей защиту персональных данных, обрабатываемых в информационной системе «Бухгалтерия, кадровый учет и документооборот», П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые:

Инструкцию пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГКУ МО ЦБ МО (далее – Инструкция);

Форму перечня должностных лиц структурного подразделения, допущенных к работе с персональными данными.

2. Начальникам управлений ГКУ МО ЦБ МО:

2.1. В двухнедельный срок организовать ознакомление с Инструкцией работников вверенных подразделений, осуществляющих обработку персональных

данных в информационных системах персональных данных (далее – ИСПДн) под подпись.

2.2. Перед допуском к работе в ИСПДн обеспечить ознакомление с Инструкцией вновь принимаемых работников под подпись.

2.3. Обеспечить ведение и актуализацию перечней должностных лиц, допущенных к работе с персональными данными, по форме, утвержденной настоящим приказом.

3. Признать утратившим силу приказ ГКУ МО ЦБ МО от 14.03.2019 № 26 «Об утверждении Инструкции пользователю по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4. Контроль за исполнением настоящего приказа возложить на заместителя директора Юфина Е.А.

Подлинник электронного документа, подписанного ЭП, хранится в Межведомственной системе электронного документооборота Правительства Московской области

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 6126365669CE376DF88907AEE80CE92E
Владелец: Осотов Алексей Алексеевич
Действителен с 08-04-2025 до 02-07-2026

Директор А.А. Осотов

УТВЕРЖДЕНА
приказом ГКУ МО ЦБ МО
от 04.03.2026 № 34

ИНСТРУКЦИЯ

пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Государственного казенного учреждения Московской области «Централизованная бухгалтерия Московской области»

I. Обозначения и сокращения

АРМ	автоматизированное рабочее место
ИБ	информационная безопасность
ИС	информационная система
ИСПДн	информационная система персональных данных
ИТКС	информационно-телекоммуникационная сеть
НСД	несанкционированный доступ
ОИБ	отдел информационной безопасности
ОСТиАБП	отдел сетевых технологий и автоматизации бюджетного процесса
ОС	операционная система
ПДн	персональные данные
ПО	программное обеспечение
УИКТ	Управление информационно-коммуникационных технологий

II. Термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть (ИТКС) – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Несанкционированный доступ (НСД) – доступ к информации или к средствам вычислительной техники, ИТКС, информационным системам (в том числе ИСПДн), осуществляемый с нарушением установленных прав и (или) правил доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или информационными системами.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Пользователь ИСПДн (пользователь) – работник ГКУ МО ЦБ МО, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных при помощи ИСПДн.

III. Общие положения

1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных» и постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Инструкция устанавливает единый порядок автоматизированной обработки ПДн в ИСПДн Государственного казенного учреждения Московской

области «Централизованная бухгалтерия Московской области» (далее — Учреждение), а также права и обязанности пользователей.

3. Инструкция обязательна к соблюдению всеми пользователями ИСПДн.

4. Обработка ПДн в ИСПДн разрешается только работникам, включенным в Перечень должностных лиц структурного подразделения, допущенных к работе с ПДн, по форме утвержденной приказом Учреждения (далее – Перечень).

4.1. Включение работника в Перечень осуществляется на основании служебной записки начальника структурного подразделения на имя начальника УИКТ, путем направления проекта Перечня для согласования. Срок согласования проекта Перечня не должен превышать одного рабочего дня с момента регистрации служебной записки в УИКТ. После согласования Перечень утверждается начальником структурного подразделения.

4.2. При наступлении обстоятельств, влекущих необходимость исключения работника из Перечня (изменение должностных обязанностей, увольнение, иные обстоятельства, влекущие прекращение необходимости доступа к ПДн), длительное отсутствие работника (отпуск по беременности и родам, отпуск по уходу за ребенком, приостановление трудового договора) либо изменения данных работника (фамилии, имени, отчества, должности), начальник структурного подразделения в течение одного рабочего дня с момента возникновения таких обстоятельств обязан направить начальнику УИКТ служебную записку с информацией об исключении или изменении данных работника в Перечне, приложив к ней проект актуализированного Перечня (с внесенными изменениями).

4.3. Актуальная версия Перечня подлежит хранению в ОИБ для целей учета, контроля и использования в работе.

5. Пользователь несет ответственность за свои действия при работе с ПДн в ИСПДн.

6. Пользователь в своей работе руководствуется должностными инструкциями и организационно-распорядительными документами по ИБ, утвержденными в Учреждении.

7. Настоящая Инструкция распространяется на обработку ПДн в следующих ИСПДн Учреждения:

государственная информационная система «Централизованная система ведения бухгалтерского учета Московской области» (ГИС ЕИСБУ);

информационная система «Бухгалтерия, кадровый учет и документооборот» (ИС БКУиД).

IV. Обязанности пользователя

8. Пользователь обязан знать и выполнять требования законодательных актов Российской Федерации, внутренних нормативных и руководящих документов в области защиты ПДн, инструкций и распоряжений по защите информации.

9. Пользователю разрешается обрабатывать только те ПДн, к которым ему предоставлен доступ.

10. Пользователь обязан придерживаться правил парольной и антивирусной защиты, принятых в Учреждении.

11. Передача ПДн третьим лицам должна осуществляться только с письменного согласия субъекта персональных данных или в иных случаях, предусмотренных законодательством Российской Федерации, и только при помощи защищенного канала связи с использованием сертифицированных средств криптографической защиты информации.

12. Обо всех выявленных нарушениях, связанных с защитой ПДн, обрабатываемых в ИСПДн, пользователь обязан незамедлительно сообщить своему непосредственному руководителю, который не позднее одного рабочего дня с момента получения информации о нарушении информирует лицо, ответственное за организацию обработки ПДн в Учреждении – начальника УИКТ посредством служебной записки.

13. При утрате носителей информации, ключевых носителей электронных подписей, а также удостоверений, пропусков, ключей от помещений, хранилищ и сейфов, где хранятся данные для доступа в ИСПДн и (или) сами ПДн, в день обнаружения утраты пользователь обязан предоставить письменное объяснение (с изложением обстоятельств утраты) своему непосредственному руководителю и начальнику ОИБ.

14. При прекращении трудовых отношений все материальные носители, содержащие ПДн (флеш-накопители, дискеты, диски, документы, черновики, распечатки, и пр.), пользователь обязан передать своему непосредственному руководителю или начальнику структурного подразделения. Ключевые носители электронных подписей должны быть переданы в ОИБ.

15. Пользователю запрещается:

передавать (в том числе устно) ПДн, которые доверены или стали известны в период исполнения должностных обязанностей, работникам сторонних организаций без согласия субъекта персональных данных, а также работникам Учреждения, не допущенным к работе с ПДн;

покидать свое АРМ, предварительно не заблокировав или не переведя ОС в «спящий режим» (для ОС Windows: [WIN] + [L] или [CTRL] + [ALT] + [DEL]

с дальнейшим нажатием кнопки «Блокировка» в появившемся меню, либо «Пуск» — «Выключение» — «Спящий режим»);

допускать к работе за своим АРМ других работников Учреждения или иных лиц, а также передавать кому-либо учетные данные для входа в ИСПДн;

передавать кому-либо свои учетные данные (логин и пароль) для входа в ИСПДн, а также записывать и хранить пароли в общедоступных местах (например, на бумажных носителях, на рабочем столе, на мониторе, под клавиатурой и т.п.);

записывать и хранить ПДн на мобильных носителях информации;

пересылать ПДн при помощи сетей общего пользования (например – сети «Интернет»), в том числе по личной электронной почте, системам мгновенного обмена сообщениями («мессенджеров»), социальных сетей и иным способам, за исключением пересылки по корпоративным почтовым сервисам Учреждения между работниками при условии применения шифрования или парольной защиты файлов, содержащих персональные данные;

открывать общий доступ к ресурсам на АРМ;

фотографировать ПДн;

распечатывать и копировать ПДн из ИСПДн без служебной необходимости или разрешения руководства;

отключать антивирусные и другие средства защиты информации АРМ;

самостоятельно устанавливать ПО на АРМ (для установки и модификации ПО необходимо обращаться в ОСТиАБП);

предпринимать попытки самостоятельного устранения неисправностей АРМ;

подключать незарегистрированные мобильные устройства к АРМ;

самостоятельно получать и настраивать доступ к ИТКС (в том числе «Интернет») на АРМ, кроме как по рекомендации работников УИКТ;

самостоятельно изменять файлы установленного на АРМ ПО для доступа к ИСПДн;

самостоятельно изменять конфигурацию АРМ;

умышленно использовать недокументированные свойства и ошибки ПО или средств защиты, которые могут привести к возникновению внештатной ситуации.

V. Права пользователя

16. Пользователь имеет право:

обращаться в ОИБ за методической помощью в обеспечении безопасности ПДн, а также за технической поддержкой в настройке средств защиты информации (антивирусного ПО, средств защиты от НСД и пр.);

обращаться в ОСТиАБП за технической поддержкой по вопросам работы ИСПДн, ИТКС Учреждения, удаленного доступа к информационным ресурсам Учреждения;

пользоваться всеми ИС, ИТКС и информационными ресурсами Учреждения, к которым допущен для исполнения должностных обязанностей.

VI. Ответственность

17. Пользователь несет ответственность в порядке, предусмотренном законодательством за:

ненадлежащее исполнение или неисполнение обязанностей и запретов, предусмотренных настоящей Инструкцией, должностной инструкцией, локальными нормативными актами Учреждения в области обработки и защиты ПДн;

правонарушения, совершенные в процессе осуществления своей деятельности;

несоблюдение требований политики ИБ Учреждения;

разглашение сведений, конфиденциального характера, ставших известными в результате исполнения должностных обязанностей;

действия или бездействие, которые могут повлечь за собой разглашение ПДН, а также за НСД к информации, доступ к которой ограничен в соответствии с законодательством.

УТВЕРЖДЕНА
приказом ГКУ МО ЦБ МО
от 04.03.2026 № 34

Форма
перечня должностных лиц структурного подразделения, допущенных к работе с персональными данными

Перечень
должностных лиц_____ , допущенных
(структурное подразделение)
к работе с персональными данными

№ п/п	Подразделение	Должность	Фамилия и инициалы
1			
2			
3			
4			
5			
6			
7			

Начальник структурного подразделения _____ Ф.И.О.
(подпись)

«___» _____ г.

СОГЛАСОВАНО:

Начальник Управления информационно-коммуникационных технологий

_____ /_____/
(подпись) (Ф.И.О.)
«___» _____ 20___ г.