ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
КРАСНОДАРСКОГО КРАЯ
«ЦЕНТРАЛИЗОВАННАЯ БУХГАЛТЕРИЯ МИНИСТЕРСТВА
ЗДРАВООХРАНЕНИЯ КРАСНОДАРСКОГО КРАЯ»
(ГКУ КК «ЦБ МЗ КК»)

УТВЕРЖДЕНА
приказом ГКУ КК «ЦБ МЗ КК»
от «20» апреля 2023 г. № 52

# ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

г. Краснодар, 2023 г.

## 1. Общие положения

1.1. Инструкция пользователя системы защиты информации в системах ГКУ КК «ЦБ МЗ КК» определяет функциональные обязанности, права и ответственность пользователей ГКУ КК «ЦБ МЗ КК» по обеспечению безопасности обрабатываемой информации.

1.2. Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите информации, обрабатываемой с использованием средств автоматизации.

## 2. Обязанности пользователя

2.1. Пользователь ГКУ КК «ЦБ МЗ КК»:

2.1.1. Хранить в тайне защищаемую информацию, ставшую ему известной во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки защищаемой информации немедленно информировать ответственного за организацию обработки информации и персональных данных и Ответственного за ИБ.

2.1.2. При определении информации, подлежащей защите, использовать документ «Перечень сведений конфиденциального характера подлежащих защите, включая персональные данные».

2.1.3. Знать и выполнять правила работы со средствами защиты информации (далее – СрЗИ), используемыми на АРМ в соответствии с Инструкциями, требованиями, регламентирующими функционирование установленных СрЗИ.

2.1.4. Хранить в тайне свой пароль доступа в системы ГКУ КК «ЦБ МЗ КК», а также информацию о системе защиты, установленной в ГИС.

2.1.5. Использовать для работы, только учтенные съемные накопители информации (компакт диски, флешки и т.д.).

2.1.6. Сообщать о необходимости обновления антивирусных баз администратору ИБ или про другие проблемы в антивирусной программе.

2.1.7. Немедленно ставить в известность администратора ИБ в случае:

− утери носителя с конфиденциальной информацией и/или при подозрении компрометации личных ключей и паролей;

− нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа (далее - НСД);

− несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств.

2.1.8. В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения,

некорректного функционирования установленных СрЗИ ставить в известность Ответственного за ИБ.

2.1.9. В случае увольнения пользователь обязан вернуть все документы и материалы, относящиеся к деятельности организации. В том числе: отчеты, инструкции, служебную переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности ГКУ КК «ЦБ МЗ КК», полученные в течение срока работы.

2.1.10. Принимать меры по реагированию в случае возникновения нештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах, возложенных на него функций.

2.1.11. Оперативно докладывать администратору ИБ о случаях возникновения нештатных ситуаций и аварийных ситуаций.

2.1.12. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов систем ГКУ КК «ЦБ МЗ КК». Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

2.2. Пользователю категорически запрещается:

- передавать кому бы то ни было, устно или письменно, защищаемую информацию;
- использовать защищаемую информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами, содержащими защищаемую информацию, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения ответственного за организацию обработки информации и персональных данных;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие защищаемую информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими защищаемую информацию;
- использовать компоненты программного и аппаратного обеспечения ГКУ КК «ЦБ МЗ КК» в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию технических средств систем в части установки программных и аппаратных средств;
- осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность Ответственного за ИБ.

2.3. Уборка помещений должна производиться под контролем пользователя, имеющего доступ в помещение и постоянно в нем работающего.

2.4. Вынос технических средств, на которых проводилась обработка защищаемой информации, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с ответственным за организацию обработки информации и персональных данных запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.5. АРМ, используемые для работы с защищаемой информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора.

## 3. Права пользователя

3.1. Пользователь имеет право:

3.1.1. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.2. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

## 4. Ответственность пользователя

4.1. Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации.

4.2. За разглашение защищаемой информации, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.