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

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Краснодар, 2023 г.

1. Общие положения

1.1. Настоящая Политика в отношении обработки информации и персональных данных работе в ГКУ КК «ЦБ МЗ КК»(далее – ГКУ КК «ЦБ МЗ КК»)определяет основные цели, задачи, требования и базовые подходы,а также общую стратегию построения системы защиты информации (далее - СЗИ) для достижения требуемого уровня безопасности информации.

1.2. Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности, который предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку СЗИ, с позиции комплексного применения технических и организационных мер и средств защитыинформации (далее – СрЗИ).

1.3. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности в ГКУ КК «ЦБ МЗ КК»,а также нормативных и методических документов, обеспечивающих ее реализацию. Политика является методологической основой для:

– принятия управленческих решений и разработки практических мер по воплощению политики безопасности защищаемой информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз защищаемой информации;

– координации деятельности уполномоченных лицпри проведении работ по развитию и эксплуатации СЗИс соблюдением требований обеспечения безопасности защищаемой информации;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности защищаемой в Системеинформации и персональных данных.

1.4. Политика разработана на основании следующих документов:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 06 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации» (в редакции с дополнением Постановления Правительства Российской Федерации от 11.05.2017 г. № 555)

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных»;

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

– Приказ ФСТЭК России № 27 от 15 февраля 2017 года «О внесении изменений в требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17».

1.5. В документе определены требования к операторам обрабатывающим ПДн в ГКУ КК «ЦБ МЗ КК», ихстепень ответственности и должностные обязанности, а также должностные обязанности работников, ответственных за обеспечение безопасности защищаемыхв СЗИ.

2. Цель и область действия Политики

2.1. Целью настоящей Политики является обеспечение безопасности защищаемой информациии персональных данных в ГКУ КК «ЦБ МЗ КК»от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации.

2.2. Безопасность защищаемой информации достигается путем исключения несанкционированного, в том числе случайного доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий.

2.3. Защищаемая информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности защищаемой информации.

2.4. Требования настоящей Политики распространяются на всех работников(штатных, временных, работающих по контракту и т.п.), допущенных к работе в ГКУ КК «ЦБ МЗ КК», а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты информации

3.1. Система защиты информацииГКУ КК «ЦБ МЗ КК»строится с учетом:

- Перечня сведений конфиденциального характера подлежащих защите, включая персональные данные;
- Модели угроз и нарушителя безопасности информации(далее – Модель угроз);
- Требований Технического задания;
- Требований нормативных документов ФСТЭК России и ФСБ России.

3.2. Система защиты информации должна обеспечивать защиту от влияния как преднамеренно инициируемых, так и случайных событий, процессов или явлений,

которые могут привести к искажению, уничтожению и копированию информации, блокированию доступа к ней, а также предотвратить возможные воздействия на компоненты Системы, приводящие к сбою их функционирования.

3.3. Система защиты информации должна включать в себя формализованные процедуры, сертифицированные средства защиты информации,организационные и технические меры, обеспечивающие нейтрализацию актуальных угроз и выполнение мер по обеспечению безопасности информации и персональных данных для установленного для Системы класса защищенности информации и уровня защищенности персональных данных.

3.4. Система защиты информации должна обеспечивать выполнение следующих основных функций:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей персональных данных;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- управление конфигурацией информационной системы и системы защиты персональных данных.

3.5. Функции защиты информации должны обеспечиваться штатными средствами операционных систем и СУБД, прикладным программным обеспечением и используемыми средствами защиты информации.

4. Основные принципы построения СЗИ

4.1. Построение и функционирование СЗИв ГКУ КК «ЦБ МЗ КК»осуществляется в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- простота применения средств защиты;

- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

4.2.Законность.

Данный принцип предполагает осуществление защитных мероприятий и разработку СЗИв соответствии с действующим законодательством в области защиты информации и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Работники и обслуживающий персоналГКУ КК «ЦБ МЗ КК»должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

4.3. Системность.

Системный подход к построению СЗИпредполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации вГКУ КК «ЦБ МЗ КК». При создании СЗИ должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированный доступ (далее – НСД) к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.4. Комплексность.

Комплексное использование методов и средств защиты информации предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

4.5. Непрерывность защиты информации.

Защита информации– не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных СрЗИ, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла СЗИ ГКУ КК «ЦБ МЗ КК». СЗИ ГКУ КК «ЦБ МЗ КК»должна находиться в защищенном состоянии на протяжении всего времени своего функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода в незащищенное состояние. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного

хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

4.6. Своевременность.

Данный принцип предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите систем ГКУ КК «ЦБ МЗ КК»и реализацию мер обеспечения безопасности информации на ранних стадиях разработки в целом, и ее СЗИ, в частности. Разработка СЗИ должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

4.7. Преемственность и совершенствование.

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования СЗИГКУ КК «ЦБ МЗ КК» с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.8. Персональная ответственность.

Предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.9. Принцип минимизации полномочий.

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к защищаемой информации должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

4.10. Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в коллективеГКУ КК «ЦБ МЗ КК», для снижения вероятности возникновения негативных действий, связанных с человеческим фактором. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности ответственного за обработку персональных данных.

4.11. Гибкость системы защиты информации.

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств

защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

4.12. Простота применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

4.13. Научная обоснованность и техническая реализуемость.

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации. СЗИ должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

4.14. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация СрЗИ должна осуществляться профессионально подготовленными специалистами.

4.15. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

4.16. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

5. Требования к подсистемамСЗИ

5.1. СЗИдолжна обеспечивать выполнение организационных и технических меры защиты информации, соответствующих основным функциям, перечисленным в п. 3.4.

5.2. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им

идентификатора (подтверждение подлинности).

5.3. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

5.4. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

5.5. Меры по защите машинных носителей информации должны обеспечивать контроль доступа к машинным носителям информации и учет, контроль перемещения и использования.

5.6. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

5.7. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

5.8. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

5.9. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

5.10. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

5.11. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

5.12. Меры по защите среды виртуализации должны исключать

несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам.

5.13. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

5.14. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

5.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечить управление изменениями конфигурации информационной системы, анализировать потенциальное воздействие планируемых изменений в конфигурации информационной системы и системы защиты персональных данных, а также определению лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.

6. Пользователи ГКУ КК «ЦБ МЗ КК»

6.1. ВГКУ КК «ЦБ МЗ КК»присутствуют следующие группы пользователей, участвующих в обработке и хранении защищаемой информации:

- ответственный за организацию обработки информации и персональных данных;
- пользователь СЗИ.

6.2. Ответственный за организацию обработки информации и персональных данных

Ответственный за организацию обработки информации и персональных данных обладает следующим уровнем доступа и знаний:

- знает законодательные и нормативные правовые акты, методические и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности;
- знает порядок использования, обработки и хранения конфиденциальной информации, в том числе персональных данных.

- обладает полной информацией о системном и прикладном программном обеспечении СЗИ;
- обладает полной информацией о технических средствах и конфигурации СЗИ;
- имеет доступ ко всем техническим средствам обработки информации и даннымСЗИ;
- обладает полной информацией о ГКУ КК «ЦБ МЗ КК»;
- имеет полныйдоступ к СрЗИ, средствам протоколирования и к части ключевых элементов Системы;
- имеет полный доступ к СКЗИ.

Уполномочен:

- реализовывать политики безопасности в части настройки средств защиты информации, межсетевых экранов в соответствии с которыми пользователь получает возможность работать с элементами ГКУ КК «ЦБ МЗ КК»;
- осуществлять аудит СрЗИ;
- осуществлять внутренний контроль соблюдения законодательства Российской Федерации в части защиты информации, в том числе персональные данные ПДн;
- доводить до сведения работников положения законодательства Российской Федерации в части защиты информации, в том числе персональные данные ПДн;
- предоставлять необходимую информацию при проведении проверок регулирующими органами, а также проведении контрольных мероприятий по обеспечению информационной безопасности;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

6.3. ПользовательГКУ КК «ЦБ МЗ КК».

ПользовательГКУ КК «ЦБ МЗ КК»осуществляет обработку защищаемой информации. Обработка информации включает: возможность просмотра защищаемой информации, ручной ввод информации в Систему, формирование справок и отчетов по информации, полученной из Системы. Пользователь не имеет полномочий для управления подсистемами обработки данных иСЗИ.

ПользовательСистемы обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;
- располагает конфиденциальными данными, к которым имеет доступ.

7. Требования к персоналу по обеспечению защиты информации

7.1. Все работники, являющиеся пользователями ГКУ КК «ЦБ МЗ КК», должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемой информации и соблюдению режима безопасности информации.

7.2. При вступлении в должность нового работника,ответственный за обеспечение безопасности информации и персональных данныхобязан организовать его ознакомление с должностной инструкцией и необходимыми документами,

регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования систем ГКУ КК «ЦБ МЗ КК».

7.3. Работник должен быть ознакомлен со сведениями настоящейПолитики, принятых процедур работы с элементамиСЗИ.

7.4. Работники, имеющие доступ к системам ГКУ «КК ЦБ МЗ КК», должны следовать установленным процедурам поддержания режима безопасности информации при выборе и использовании паролей (если не используются технические средства аутентификации).

7.5. Работники, имеющие доступ к системам ГКУ «КК ЦБ МЗ КК»,должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности информации и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

7.6. Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

7.7. Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе в ГКУ КК «ЦБ МЗ КК», третьим лицам.

7.8. При работе с защищаемой информацией в ГКУ КК «ЦБ МЗ КК»по Краснодарскому краюработники обязаны обеспечить отсутствие возможности просмотра защищаемой информации третьими лицами с мониторов АРМ или терминалов.

7.9. При завершении работы в ГКУ КК «ЦБ МЗ КК»обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

7.10. Работники должны быть проинформированы об угрозах нарушения режима безопасности информации и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.

7.11. Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы систем ГКУ КК «ЦБ МЗ КК», могущих повлечь за собой угрозы безопасности информации, а также о выявленных ими событиях, затрагивающих безопасность информации, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности информации.

8. Должностные обязанности пользователейГКУ КК «ЦБ МЗ КК»

8.1. Должностные обязанности пользователей ГКУ КК «ЦБ МЗ КК» прописаны в следующих документах:

- инструкция ответственного за организацию обработки информации и персональных данных;

- инструкция пользователя системы защиты информации.

9. Ответственность пользователейГКУ КК «ЦБ МЗ КК»

9.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

9.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

9.3. При нарушениях работникамиГКУ КК «ЦБ МЗ КК»правил, связанных с безопасностью информации, они несут ответственность, установленную действующим законодательством Российской Федерации.