

**ПОЛИТИКА ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ  
ГБУЗ МО «КЦРБ»**

2016 г.

## 1. Термины и определения

*Автоматизированная система(АС)* - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

*Администратор информационной безопасности (администратор ИБ)* - специалист или группа специалистов учреждения, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

*Анализ риска* - систематическое использование информации для определения источников и оценки риска.

*Аудит информационной безопасности (аудит ИБ)* - процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самой организацией (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

*Аутентификация* - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

*Доступ к информации* - возможность получения информации и ее использования.

*Защищенный канал передачи данных* - логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

*Идентификатор доступа* - уникальный признак субъекта или объекта доступа.

*Идентификация* - присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

*Информация* - это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

*Информационная безопасность (ИБ)* - механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

*Информационная система (ИС)* - совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений ГБУЗ МО «КЦРБ». В ГБУЗ МО «КЦРБ» используются различные типы информационных систем для решения управленческих, учетных, обучающих и других задач.

*Информационные технологии* - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

*Информационные активы* - информационные системы, информационные средства, информационные ресурсы.

*Информационные средства* - программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

*Информационные ресурсы* - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

*Инцидент информационной безопасности* - действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов учреждения.

*Источник угрозы* - намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

*Конфиденциальная информация* - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

*Конфиденциальность* - доступ к информации только авторизованных пользователей.

*Критичная информация* - информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений ГБУЗ МО «ГБУЗ МО «КЦРБ»», привести к причинению ГБУЗ МО «ГБУЗ МО «КЦРБ»» материального или иного вида ущерба.

*Локальная вычислительная сеть (ЛВС)* - группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

*Межсетевой экран (МЭ)* - программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью ГБУЗ МО «КЦРБ» и внешними сетями (сетью Интернет).

*Мониторинг информационной безопасности* - постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы учреждения, информационные услуги учреждения и пр.

*Несанкционированный доступ к информации (НСД)* - доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

*Обработка риска* - процесс выбора и осуществления мер по модификации риска.

*Остаточный риск* - риск, остающийся после обработки риска.

*Политика информационной безопасности (ПБ)* - комплекс взаимосвязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

*Пользователь ЛВС* - сотрудник ГБУЗ МО «КЦРБ» (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

*Принятие риска* - решение принять риск.

*Программное обеспечение (ПО)* - совокупность прикладных программ, установленных на сервере или ЭВМ.

*Рабочая станция АРМ* - персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

*Регистрационная (учетная) запись пользователя* - включает в себя имя пользователя и его уникальный идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

*Роль* - совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

*Система менеджмента информационной безопасности (СМИБ)* - та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности.

*Системный администратор (СА)* - сотрудник учреждения, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети учреждения и ПК.

*Список контроля доступа (ACL)* - правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии фильтрации и действия, производимые над пакетами.

*Собственник* - лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

*Средства криптографической защиты информации (СКЗИ)* - средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

*Угрозы информационным данным* - потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

*Управление информационной безопасностью* - совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

*Уязвимость* - недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

*Целостность информации* - состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

*ЭВМ* - электронная вычислительная машина, персональный компьютер.

*Электронная цифровая подпись (ЭЦП)* - реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

*VPN (VIRTUAL PRIVATE NETWORK)* - «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

БД -	База данных.
ЗИ -	Защита информации.
ИТС -	Информационно-телекоммуникационная система.
КЗ -	Контролируемая зона.
ОС -	Операционная система.
СВТ -	Средства вычислительной техники.
СЗИ -	Средство защиты информации.
СПД -	Система передачи данных.
СУБД -	Система управления базами данных.
СУИБ -	Система управления информационной безопасностью.
СЭД -	Система электронного документооборота.

## **2. Общие положения**

Политика информационной безопасности государственного бюджетного учреждения здравоохранения Московской области «Коломенская центральная районная больница» (ГБУЗ МО «КЦРБ», учреждение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется ГБУЗ МО «КЦРБ» в своей деятельности.

Общее руководство обеспечением ИБ осуществляет руководитель учреждения. Ответственность за организацию обработки персональных данных несет один из заместителей руководителя учреждения, назначенный приказом по учреждению. Ответственность за обеспечение и контроль за соблюдением требований ИБ несет сотрудник, назначенный приказом по учреждению. Ответственность за функционирование автоматизированной системы учреждения несет сотрудник, выполняющий функции (ведущий программист) (далее СА). Должностные обязанности администратора ИБ и СА закрепляются в соответствующих инструкциях.

Руководители структурных подразделений учреждения ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

### **3. Цели и назначение**

Основными целями политики ИБ являются защита информации и обеспечение эффективной работы всего информационно-вычислительного комплекса ГБУЗ МО «КЦРБ» при осуществлении деятельности, указанной в Уставе. Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба ГБУЗ МО «КЦРБ» обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне общества), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Для противодействия угрозам ИБ в ГБУЗ МО «КЦРБ» на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для ГБУЗ МО «КЦРБ». Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

- описание организации системы управления ИБ в ГБУЗ МО «КЦРБ»;
- определение Политик информационной безопасности, а именно:
  - политика реализации антивирусной защиты;
  - политика учетных записей;
  - политика предоставления доступа к информационному ресурсу;
  - политика использования паролей;
  - политика защиты АРМ;

- политика конфиденциального делопроизводства;
- определение порядка сопровождения ИС ГБУЗ МО «КЦРБ».

### **Область применения**

Настоящая Политика распространяется на все структурные подразделения ГБУЗ МО «КЦРБ» и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

### **Период действия и порядок внесения изменений**

Настоящая политика вводится в действие со дня утверждения руководителем ГБУЗ МО «КЦРБ».

Политика признается утратившей силу на основании приказа руководителя ГБУЗ МО «КЦРБ».

Изменения в политику вносятся приказом руководителя ГБУЗ МО «КЦРБ». Инициаторами внесения изменений в политику информационной безопасности являются:

- главный врач ГБУЗ МО «КЦРБ»;
- специалист по защите информации;
- начальник отдела ИТ;
- администратор ИБ.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

- при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;
- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности ГБУЗ МО «КЦРБ».
- при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб ГБУЗ МО «КЦРБ»

Ответственными за актуализацию политики информационной безопасности (плановую и внеплановую) несет специалист по защите информации.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на ответственного за организацию обработки персональных данных в ГБУЗ МО «КЦРБ».

## **4. Политика информационной безопасности ГБУЗ МО «КЦРБ»**

### **4.1. Назначение политики информационной безопасности**

Политики информационной безопасности ГБУЗ МО «КЦРБ» - это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в ГБУЗ МО «КЦРБ».

Под политиками безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию ГБУЗ МО «КЦРБ» в области ИБ.

Политики информационной безопасности регламентируют эффективную работу средств защиты информации. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики информационной безопасности реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены руководителем учреждения ГБУЗ МО «КЦРБ».

#### **4.2. Основные принципы обеспечения ИБ**

Основными принципами обеспечения ИБ являются следующие:

- Постоянный и всесторонний анализ информационного пространства общества с целью выявления уязвимостей информационных активов.
- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ ГБУЗ МО «КЦРБ», корректировка моделей угроз и нарушителя.
- Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей ГБУЗ МО «КЦРБ», а также повышать трудоемкость технологических процессов обработки информации.
- Контроль эффективности принимаемых защитных мер.
- Персонафикация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

#### **4.3. Соответствие политики информационной безопасности действующему законодательству**

Правовую основу политик составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

#### **4.4. Ответственность за реализацию политики информационной безопасности**

Ответственность за разработку мер и контроль обеспечения защиты информации несёт специалист по защите информации.

Ответственность за реализацию политик возлагается:

- в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты - на администратора ИБ;
- в части, касающейся доведения правил политик до сотрудников ГБУЗ МО «КЦРБ», а также иных лиц (см. область действия настоящей политики) - на ответственного за организацию обработки персональных данных в ГБУЗ МО «КЦРБ» и руководителей подразделений;
- в части, касающейся исполнения правил политики, - на каждого сотрудника ГБУЗ МО «КЦРБ», согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

#### **4.5. Порядок подготовки персонала по вопросам ИБ и допуска его к работе**

Организация просвещения сотрудников ГБУЗ МО «КЦРБ» в области ИБ возлагается на специалиста по защите ИБ. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по ИБ». Обучение сотрудников ГБУЗ МО «КЦРБ» правилам обращения с конфиденциальной информацией, проводится путем:

- проведения специалистом по защите ИБ инструктивных занятий с сотрудниками, принимаемыми на работу в ГБУЗ МО «КЦРБ»;
- самостоятельного изучения сотрудниками внутренних нормативных документов ГБУЗ МО «КЦРБ».

Допуск персонала к работе с защищаемыми информационными ресурсами ГБУЗ МО «КЦРБ» осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Инструкцией по работе пользователей в АС ГБУЗ МО «КЦРБ»», а также иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по ИБ».

Допуск персонала к работе с конфиденциальной информацией ГБУЗ МО «КЦРБ» осуществляется после ознакомления с «Инструкцией по обращению с носителями

конфиденциальной информации». Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками ГБУЗ МО «КЦРБ», определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

#### 4.6. Защищаемые информационные ресурсы ГБУЗ МО «КЦРБ»

№ п/п	Наименование ИС
1.	ИС внутренняя- кадры
2.	ПО "Парус"
3.	Единая Медицинская Информационная Автоматизированная Система
4.	ТАСУ ОМС

#### 4.7. Различаются следующие категории информационных ресурсов, подлежащих защите в ГБУЗ МО «КЦРБ»:

*Конфиденциальная* - информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 27.07.2006 г. №152-ФЗ «О персональных данных», указом президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера» пункт 4, постановлением правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

*Публичная* - информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

*Открытая* - информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности ГБУЗ МО «КЦРБ», которую запрещено относить конфиденциальной на основании законодательства Российской Федерации. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности ГБУЗ МО «КЦРБ».

*Ограниченного доступа* - информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Конфиденциальная информация представляет собой сведения ограниченного доступа, включая **персональные данные**, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Правила отнесения информации к конфиденциальной и порядок работы с конфиденциальными документами, определяются "Инструкцией по обращению с носителями конфиденциальной информации", а также «Перечнем сведений конфиденциального характера».

Подходы к решению проблемы защиты информации в ГБУЗ МО «КЦРБ», в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов ГБУЗ МО «КЦРБ».

**Для этого в ГБУЗ МО «КЦРБ» выполняются следующие мероприятия:**

- определяется порядок работы с документами, образцами изделиями и др., содержащими конфиденциальные сведения;
- устанавливается круг лиц и порядок доступа к подобной информации;
- вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;



- включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

**Форма подписки о неразглашении сведений конфиденциального характера подписывается при заключении трудового договора, который подписывается всеми сотрудниками учреждения при приеме на работу в ГБУЗ МО «КЦРБ».**

Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых ГБУЗ МО «КЦРБ» с другими организациями. Персональные данные сотрудника учреждения - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно Ст.86 п.7 Трудового кодекса РФ защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно Ст.88 Трудового кодекса РФ при передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

- осуществлять передачу персональных данных сотрудника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым сотрудник должен быть ознакомлен под расписку;
- разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно Ст.90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

## **4.8. Организация системы управления информационной безопасностью ГБУЗ МО «КЦРБ»**

### **4.8.1. Организация системы управления ИБ**

Система управления информационной безопасности ГБУЗ МО «КЦРБ» (СУИБ) - предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности ГБУЗ МО «КЦРБ».

Для успешного функционирования СУИБ ГБУЗ МО «КЦРБ» должны быть реализованы следующие процессы:

- определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ;
- определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью ГБУЗ МО «КЦРБ», а также оценки правовых рисков деятельности ГБУЗ МО «КЦРБ»;
- анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов;
- выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ;
- принятие руководством ГБУЗ МО «КЦРБ» остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности ГБУЗ МО «КЦРБ», и оценено их влияние на достижение целей деятельности ГБУЗ МО «КЦРБ»;
- реализация системы управления ИБ.

В системе управления ИБ должны быть реализованы следующие процессы:

- разработка плана обработки рисков ИБ;
- реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;
- реализация программ по обучению и осведомленности ИБ;

- обнаружение и реагирование на инциденты безопасности;
- обеспечение непрерывности деятельности и восстановления после прерываний. На этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. ГБУЗ МО «КЦРБ» принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

#### **4.8.2. Методы оценивания информационных рисков**

Оценка информационных рисков ГБУЗ МО «КЦРБ» выполняется по следующим основным этапам:

- идентификация и количественная оценка информационных ресурсов, значимых для работы ГБУЗ МО «КЦРБ» оценивание возможных угроз;
- оценивание существующих уязвимостей;
- оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые уязвимые информационные ресурсы ГБУЗ МО «КЦРБ» подвергаются риску, если по отношению к ним существуют какие-либо угрозы. При этом информационные риски зависят от:

- показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности организации.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса ГБУЗ МО «КЦРБ».

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

- привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
- возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
- техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;
- степенью легкости, с которой уязвимость может быть использована.

## 4.9. Политики информационной безопасности

### 4.9.1. Политика предоставления доступа к информационному ресурсу

#### Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам ГБУЗ МО «КЦРБ»

#### Положение политики

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику ГБУЗ МО «КЦРБ», допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в ГБУЗ МО «КЦРБ» одного и того же имени пользователя («группового имени») **ЗАПРЕЩЕНО**.

### 4.9.2. Порядок создания (продления) учетной записи пользователя

Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника ГБУЗ МО «КЦРБ» инициируется заявкой (Приложение № 1). В заявке указывается:

- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- основание для регистрации учетной записи (номер приказа о принятии на работу в ГБУЗ МО «КЦРБ» или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к информационным ресурсам ГБУЗ МО «КЦРБ».

Заявку подписывает инспектор кадровой службы подтверждающий, что указанный сотрудник действительно принят в штат ГБУЗ МО «КЦРБ».

Заявка согласуется с администратором ИБ и передается САу.

СА рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам ГБУЗ МО «КЦРБ».

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

### 4.9.3. Порядок предоставления (изменения) полномочий пользователя

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам ГБУЗ МО «КЦРБ» инициируется заявкой сотрудника (Приложение № 2). В заявке указывается:

- должность, фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- наименование информационного актива (системы, ресурса), к которому необходим допуск (или изменение полномочий пользователя);
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных информационных ресурсах ИС) с указанием разрешенных видов доступа к ресурсу (ролей).

Заявка согласуется с администратором ИБ и передается СА у на исполнение.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

#### **4.9.4. Порядок удаления учетной записи пользователя**

При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно **блокироваться**.

Предпочтительно использовать механизмы автоматического блокирования учетных записей уволенных сотрудников, используя соответствующие ИС. При невозможности автоматического блокирования учетных записей, сотрудникам сопоставляются временные учетные записи (с фиксированным сроком действия), о чем делается отметка в заявке при ее исполнении и в обязательном порядке доводится до инициатора заявки.

Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. В этом случае **начальник кадровой службы** обязан своевременно подавать заявки на блокирование учетной записи сотрудника (Приложение №3) не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.

В заявке указывается:

- должность сотрудника, фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- дата прекращения полномочий пользователя.

Заявку подписывает **начальник кадровой службы**, утверждая тем самым факт прекращения срока действия полномочий пользователя.

Администратор ИБ рассматривает представленную заявку и передает заявку на исполнение САу.

По окончании внесения изменений в заявку делается отметка о выполнении задания за подписями исполнителей.

В случае необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации. Заявка должна подаваться даже в случае применения механизмов автоматической блокировки учетных записей уволенных сотрудников.

Такая заявка должна быть предварительно согласована с администратором ИБ, и после выполнения действий по блокированию учетной записи передается САу для исполнения требования по сохранению данных.

#### **4.9.5. Порядок хранения исполненных заявок**

Исполненные заявки передаются САу и хранятся в архиве в течение 5 лет с момента окончания предоставления доступа к информационному ресурсу ГБУЗ МО «КЦРБ».

Копии исполненных заявок хранятся у администратора ИБ.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий в ИС ГБУЗ МО «КЦРБ»;
- для контроля правомерности наличия у конкретного пользователя прав доступа к информационному ресурсу
- тем или иным ресурсам системы при разборе конфликтных ситуаций;
- для проверки САом правильности настройки средств разграничения доступа к ресурсам системы.

В случае невозможности исполнения, инициатору заявки направляется мотивированный отказ с приложением заявки.

## 4.10. Политика учетных записей

### Назначение

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов ГБУЗ МО «КЦРБ». Положение политики учетных записей подразделяются на:

- пользовательские - предназначенные для идентификации/аутентификации пользователей информационных активов ГБУЗ МО «КЦРБ»
- системные - используемые для нужд операционной системы;
- служебные - предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов ГБУЗ МО «КЦРБ» назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе **категорически запрещено**.

## 4.11. Политика использования паролей

### 4.11.1. Назначение

Настоящая политика определяет основные правила обращения с паролями, используемыми для доступа к защищаемым информационным активам ГБУЗ МО «КЦРБ».

### 4.11.2. Положения политики

Положения политики закрепляются в «Инструкции по парольной защите».

## 4.12. Политика реализации антивирусной защиты

### 4.12.1. Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в ГБУЗ МО «КЦРБ».

### 4.12.2. Положения политики

Положения политики закрепляются в «Инструкции по проведению антивирусного контроля».

## 4.13. Политика защиты АРМ

### 4.13.1. Назначение

Настоящая Политика определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации ГБУЗ МО «КЦРБ» от неавторизованного доступа, утраты или модификации.

### 4.13.2. Положения политики

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами ГБУЗ МО «КЦРБ», (согласно занимаемой должности), а именно с инструкциями по обращению с носителями конфиденциальной информации, «Перечень сведений конфиденциального характера».

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратор информационной безопасности.

Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

**Пользователям запрещается** устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к САу.

**Локальное** техническое обслуживание должно осуществляться только в личном присутствии пользователя.

**Дистанционное** техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками ГБУЗ МО «КЦРБ».

Запрещается использование указанных АРМ другими пользователями без согласования с администратором ИБ ГБУЗ МО «КЦРБ»

При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).

*СА вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.*

#### **4.14. Порядок сопровождения ИС ГБУЗ МО «КЦРБ»**

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации).

Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии администратора ИБ и САа. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34.xxx «Стандарты информационной технологии».

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии администратора ИБ.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

- неверной формулировки требований к ИС;
- выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;
- принятия неверных проектных решений;
- внесения разработчиком дефектов на уровне архитектурных решений;
- внесения разработчиком недокументированных возможностей в ИС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;
- разработки некачественной документации;
- сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;
- неверного конфигурирования ИС;
- приемки ИС, не отвечающей требованиям заказчика;
- внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, принятых разработчиком в отношении угроз ИБ.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, принятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть

представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство ГБУЗ МО «КЦРБ», должно обеспечить анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности работы.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

- умышленное несанкционированное раскрытие, модификация или уничтожение информации;
- неумышленная модификация или уничтожение информации;
- недоставка или ошибочная доставка информации;
- отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз:

- внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;
- невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб ГБУЗ МО «КЦРБ», и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

#### **4.15. Профилактика нарушений политик информационной безопасности**

Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в ГБУЗ МО «КЦРБ» и проведение разъяснительной работы по информационной безопасности среди пользователей.

Проведение в ИС ГБУЗ МО «КЦРБ» регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС ГБУЗ МО «КЦРБ» степенью периодичности.

Задача предупреждения в ИС ГБУЗ МО «КЦРБ» возможных нарушений информационной безопасности решается по мере наступления следующих событий:

- включение в состав ИС ГБУЗ МО «КЦРБ» новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС ГБУЗ МО «КЦРБ»
- изменение конфигурации программных и технических средств ИС (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС ГБУЗ МО «КЦРБ» при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС ГБУЗ МО «КЦРБ»
- Администратор ИБ (возможно, при помощи сторонней организации специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС ГБУЗ МО «КЦРБ»;



- Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Администратор ИБ (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организывает периодическую проверку СЗИ ИС ГБУЗ МО «КЦРБ» путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС ГБУЗ МО «КЦРБ» средств и функций защиты. По результатам профилактических работ, проводимых в ИС, необходимо сделать соответствующие записи в специальном журнале (Журнале проверки исправности и технического обслуживания).

Плановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников ГБУЗ МО «КЦРБ» по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в ГБУЗ МО «КЦРБ», проводится администратором ИБ ежеквартально.

Внеплановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников ГБУЗ МО «КЦРБ» по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в ГБУЗ МО «КЦРБ», проводится при пересмотре настоящих политик, при возникновении инцидента нарушения правил настоящих политик.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящих политик.

#### **4.16. Ликвидация последствий нарушения политик информационной безопасности**

Администратор ИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления НСД к защищаемым информационным ресурсам ИС рекомендуется уведомить администратора ИБ и начальника информационного отдела, и далее следовать их указаниям.

Действия администратора ИБ и САа при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

- Инструкцией пользователя автоматизированной системы;
- Политикой информационной безопасности;
- Должностными обязанностями администратора ИБ;
- Должностными обязанностями САа.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

#### **4.17. Ответственность нарушителей Политик информационной безопасности**

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник ГБУЗ МО «КЦРБ» в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности ГБУЗ МО «КЦРБ», могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный ГБУЗ МО «КЦРБ» в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники ГБУЗ МО «КЦРБ» несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации (приложение №4).

## **5. Регулирующие законодательные нормативные документы**

При организации и обеспечении работ по информационной безопасности сотрудники ГБУЗ МО «КЦРБ» должны руководствоваться следующими законодательными нормативными документами:

### **5.1. основополагающие нормативные документы**

К основополагающим нормативным документам относятся:

- Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895).

-

### **5.2. Законы Российской Федерации**

- Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности»;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 10 января 2002 г. № 1 –ФЗ «Об электронной цифровой подписи» (с изменениями от 8 ноября 2007 г.);
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Уголовный кодекс РФ;
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 9 мая 2005 г., 1 мая, 1 декабря 2007 г.);
- Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями от 13, 21 марта, 9 декабря 2002 г., 10 января, 27 февраля, 11, 26 марта, 23 декабря 2003 г., 2 ноября 2004 г., 21 марта, 2 июля, 31 декабря 2005 г., 27 июля, 4, 29 декабря 2006 г., 5 февраля, 19 июля, 4, 8 ноября, 1, 6 декабря 2007 г.).

### **5.3. Указы и распоряжения президента Российской Федерации**

- Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (с изменениями от 26 июля 1995 г., 17 января, 9 июля 1997 г.);

- Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (с изменениями от 25 июля 2000 г.);

- Указ Президента Российской Федерации от 3 июля 1995 г. № 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации» (с изменениями от 16 августа 1995 г., 4 января 1996 г., 28 мая 1997 г., 29 ноября 2004 г.);

- Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» (с изменениями от 30 декабря 2000 г.);

- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 г.).

#### **5.4. Постановления и распоряжения правительства Российской Федерации**

- Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;
- Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» (с изменениями от 23 апреля 1996 г., 29 марта 1999 г., 17 декабря 2004 г.).

#### **5.5. Нормативные и руководящие документы Федеральных служб РФ**

- Решение Гостехкомиссии России от 21 октября 1997 г. № 61 «О защите информации при вхождении России в международную информационную систему «Интернет»;
- Постановление Госстандарта Российской Федерации от 21 сентября 1994 г. № 15 «Об утверждении «Порядка проведения сертификации продукции в Российской Федерации» (с изменениями от 25 июля 1996 г., 11 июля 2002 г.);
- Постановление Госстандарта Российской Федерации от 10 мая 2000 г. № 26 «Об утверждении Правил по проведению сертификации в Российской Федерации» (с изменениями от 5 июля 2002 г.);
- Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. №199);
- Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.);
- Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 5 января 1996 г. № 3);
- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);
- Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114);

- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187).

## **5.6. Государственные стандарты**

- ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение» (утвержден постановлением Госстандарта СССР от 28 июня 1984 г. № 2206, с изменениями от июня 1987 г., ноября 1988 г., декабря 1990 г.);

- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (утвержден постановлением Госстандарта СССР от 24 марта 1989 г. № 661);

- ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта России от 9 февраля 1995 г. № 49);

- ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний», Госстандарт России, 1995 г.;

- ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Госстандарта России от 14 июля 1998 г. № 295);

- ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (введен в действие постановлением Госстандарта России от 12 мая 1999 г. № 160);

- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения», Госстандарт России, 2000 г.;

- ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования», Госстандарт России, 2000 г.;

ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (принят постановлением Госстандарта России от 29 декабря 2005 г. № 447-ст).

## Приложения:

НОМЕР ПРИЛОЖЕНИЯ	НАИМЕНОВАНИЕ ПРИЛОЖЕНИЯ	КРАТКОЕ ОПИСАНИЕ СОДЕРЖАНИЯ	ПРИМЕЧАНИЕ
1.	Форма заявления на создание учетной записи пользователя	Содержит форму заявления, которое должен написать руководитель пользователя для создания пользовательской учетной записи в ИС ГБУЗ МО «КЦРБ»	Включено в настоящий документ
2.	Форма заявления на создание и изменение полномочий пользователю	Содержит форму заявления, оформляемого руководителем пользователя для наделения пользователя новыми полномочиями для работы с информационными ресурсами ИС ГБУЗ МО «КЦРБ»	Включено в настоящий документ
3.	Форма заявления на блокировку учетной записи пользователя	Содержит форму заявления, оформляемого руководителем пользователя для блокирования учетной записи пользователя	Включено в настоящий документ
4.	статьи 272, 273 и 274 Уголовного кодекса Российской Федерации	Ответственность за нарушения ИБ	Включено в настоящий документ

**Начальник отдела по безопасности**

**В.Е. Лавута**

**«СОГЛАСОВАНО»**

**Начальник отдела информационных технологий**

**О.В. Трипутень**

**«20» июня 2016 г.**

**Приложение 1  
к Положению  
Политика информационной  
безопасности**

**Форма заявления на создание учетной записи пользователя.**

**СОГЛАСОВАНО**

инспектор по кадрам  
(для штатных сотрудников)

«\_\_» \_\_\_\_\_ 20\_\_ г.

Специалист информационной безопасности

«\_\_» \_\_\_\_\_ 20\_\_ г.

**ЗАЯВЛЕНИЕ № \_\_\_\_\_**

На создание (продление) учетной записи пользователя

Прошу создать (продлить) учетную запись пользователя:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Ф.И.О. непосредственного руководителя, должность, телефон	

Сотрудник приступает к работе с: «\_\_» \_\_\_\_\_ 20\_\_ г. по «\_\_» \_\_\_\_\_ 20\_\_ г.  
(указывается при необходимости)

Обоснование служебной необходимости: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.  
(Фамилия И.О. начальник подразделения) (подпись) (дата)

С правилами работы в информационной системе ГБУЗ МО «КЦРБ» ознакомлен(а)

\_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.  
(Фамилия И.О. сотрудника) (подпись) (дата)

Выполнено: \_\_\_\_\_  
(назначенное имя пользователя) (адрес почты)

Системный администратор \_\_\_\_\_ Системное Время: чч \_\_\_\_\_ мм  
(Подпись) (Фамилия И.О.)

Дата: «\_\_» \_\_\_\_\_ 20\_\_ г.

**Приложение 2  
к Положению  
Политика информационной  
безопасности**

**Форма заявления на изменение полномочий.**

**СОГЛАСОВАНО**

Специалист информационной безопасности

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**ЗАЯВЛЕНИЕ № \_\_\_\_\_**

На изменение полномочий пользователю

Прошу изменить полномочия по работе с информационным ресурсом:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Имя в системе (указывается если есть)	
Ф.И.О. непосредственного руководителя, должность, телефон	
Наименование информационного ресурса	
Старые полномочия (если были)	
Новые полномочия	

Изменения вступают в силу с: « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. по « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
(указывается при необходимости)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

(Фамилия И.О. начальник подразделения) (подпись) (дата)

С правилами работы в информационной системе ГБУЗ МО «КЦРБ» ознакомлен(на)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

(Фамилия И.О. сотрудника) (подпись) (дата)

Выполнено: \_\_\_\_\_  
(назначенное имя пользователя, описание выполненных действий)

Системный администратор \_\_\_\_\_ Системное Время: чч \_\_\_\_\_ мм  
(Подпись) (Фамилия И.О.)

Дата: « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**Приложение 3  
к Положению  
Политика информационной  
безопасности**

**Форма заявления на блокировку учетной записи.**

Инспектор по кадрам  
(для штатных сотрудников)

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

Специалист информационной безопасности

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

**ЗАЯВЛЕНИЕ №**  
На блокировку учетной записи пользователя

Прошу заблокировать учетную запись пользователя:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Имя в системе	
Ф.И.О. непосредственного руководителя, должность, телефон	

Срок действия полномочий прекратить с: «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Обоснование блокировки: \_\_\_\_\_

\_\_\_\_\_ « \_\_\_ » \_\_\_\_\_ 20\_\_ г.  
(Фамилия И.О. начальник подразделения) (подпись) (дата)

С гарантированным хранением данных в течении \_\_\_\_\_  
(указывается срок хранения данных пользователя)

Пользователь заблокирован

Системный администратор \_\_\_\_\_ Системное Время: чч \_\_\_\_\_ мм  
(Подпись) (Фамилия И.О.)

Дата: «\_\_\_» \_\_\_\_\_ 20\_\_ г.



## **Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

### **Статья 272. Неправомерный доступ к компьютерной информации**

(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

(в ред. Федерального закона от 28.06.2014 N 195-ФЗ)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

**Статья 273. Создание, использование и распространение вредоносных компьютерных программ**

(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до

двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

**Статья 274.** Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, -

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

**Главный специалист по ИБ ГБУЗ МО «ГБУЗ МО «КЦРБ»  
Пашков**

**Ю.Н.**

« \_\_\_\_ » \_\_\_\_\_ 201 \_\_\_\_ г.