# Политика информационной безопасности

# 1. Общие положения

Политика информационной безопасности ГАУЗ «Центральная городская клиническая больница №18» (далее – ЦГКБ №18) предполагает создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, определяющих порядок обеспечения безопасности информации в информационных системах соответствующего, управления и контроля информационной безопасности, а также выдвигающих требования по поддержанию подобного порядка.

Политика информационной безопасности отражает позицию руководства по вопросу обеспечения информационной безопасности учреждения.

Политика информационной безопасности направлена на:

-нормативное регулирование процесса обмена защищаемой информацией с взаимодействующими структурами, юридическими и физическими лицами;

-установление определенного организационно-правового режима использования информационных ресурсов;

-разработку системы нормативных документов, действующих на правах стандартов и определяющих степень конфиденциальности информации, требуемый уровень защищенности объектов информатизации, ответственность должностных лиц и сотрудников за соблюдение этих требований;

-реализацию комплекса организационных, инженерно-технических, технических и аппаратно-программных мероприятий по предупреждению несанкционированных действий с информацией и защиту ее от утечки по техническим каналам;

-предоставление пользователям необходимых сведений для сознательного поддержания установленного уровня защищенности объектов информатизации;

-организацию постоянного контроля эффективности принятых мер защиты и функционирования системы обеспечения информационной безопасности;

-создание резервов и возможностей по ликвидации последствий нарушения режима защиты информации и восстановления системы обеспечения информационной безопасности.

# 2. Цель обеспечения информационной безопасности

Основной целью является обеспечение информационной безопасности, что предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности, подчиненное единому замыслу.

Главная цель принимаемых мер защиты информации состоит в том, чтобы гарантировать целостность, достоверность, доступность и конфиденциальность информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационно-вычислительных и телекоммуникационных системах (далее - информационные системы), независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности учреждения, не жертвуя при этом основными принципами информационной безопасности, описанными в данной Политике.

Ответственность за организацию и проведение работ по обеспечению информационной безопасности несет главный врач ЦГКБ №18.

Методическое руководство и контроль за эффективностью предусмотренных мер защиты осуществляет соответствующий специалист по информационной безопасности ЦГКБ №18.

# 3. Объекты информационной безопасности

Объектом защиты в контексте данной Политики являются информационные ресурсы ЦГКБ №18, обрабатываемые в информационных системах и ее функциональных подсистемах, содержащие сведения доступ к которым ограничен, и используемые в процессах сбора, обработки, накопления, хранения и распространения в границах информационных систем ЦГКБ №18.

Основными объектами защиты являются:

-информационные ресурсы, содержащие сведения, отнесенные к государственной тайне;

-информационные ресурсы, представляющие коммерческую ценность;

-программные информационные ресурсы, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальное средства и утилиты;

-физические информационные ресурсы: компьютерное обеспечение всех видов; носители информации всех видов (электронные, бумажные и проч.);

-все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением;

-технические серверы (отопление, освещение, электроснабжение, кондиционирование воздуха и т.п.).

Следует также отметить, что указанные выше основные объекты защиты являются наиболее ценными ресурсами, и следовательно, по отношению к ним должны применяться самые эффективные правила и методы защиты. Их доступность, целостность и конфиденциальность могут иметь значение для обеспечения имиджа ЦГКБ №18, эффективности его функционирования и т.д. Доступность, целостность и конфиденциальность в обязательном порядке должны учитываться при разработке организационно-распорядительной документации по обеспечению информационной безопасности для системы в целом и для каждого ее ресурса в отдельности.

# 

# 4. Задачи обеспечения информационной безопасности

Основными задачами обеспечения информационной безопасности являются:

-инвентаризация и систематизация всех информационных ресурсов;

-обеспечение безопасности информационных ресурсов: уменьшение риска их случайной или намеренной порчи, уничтожения или хищения;

-сведение к минимуму финансовых, временных и прочих потерь, связанных с нарушением информационной безопасности и физическими неисправностями аппаратного и программного обеспечения, а также осуществление мониторинга и реагирование по случаям инцидентов;

-обеспечение безопасной, четкой и эффективной работы сотрудников с его информационными ресурсами;

-сведение к разумному минимуму финансовых затрат на поддержание функционирования аппаратного и программного обеспечения и автоматизированной системы в целом на должном уровне (сюда относятся крупные и мелкие обновления программного и аппаратного обеспечения, бесперебойное обеспечение системы расходными материалами и проч.);

-сведение пользования информационными ресурсами к единой системе организационно-распорядительной документации.

# 5. Принципы обеспечения информационной безопасности

При построении системы защиты необходимо придерживаться следующих принципов:

-применение разнородных систем обеспечения информационной безопасности;

-достоинства одних частей системы обеспечения информационной безопасности должны перекрывать недостатки других;

-система обеспечения информационной безопасности должна строиться многоуровневой;

-в зоне максимальной безопасности должны располагаться особо важные информационные ресурсы;

-непрерывность и целенаправленность процесса обеспечения информационной безопасности;

-усиление защиты информации во время нештатных ситуаций;

-обеспечение возможности регулирования уровня информационной безопасности без изменения функциональной базы системы информационной безопасности;

-обеспечение простоты в применении механизмов защиты для рядовых сотрудников ЦГКБ №18.

# 6. Оценка рисков

Для оценки рисков при составлении и последующем пересмотре организационно-распорядительных документов необходимо систематически рассматривать следующие аспекты:

-ущерб, который может нанести деятельности ЦГКБ №18 серьезное нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;

-реальную вероятность такого нарушения защиты в свете превалирующих угроз и средств контроля.

# 7. Требования в отношении обучения вопросам информационной безопасности

Основной целью обучения является:

-Обеспечение уверенности в осведомленности сотрудников ЦГКБ №18 об угрозах и проблемах, связанных с информационной безопасностью, об ответственности в соответствии с законодательством;

-знание сотрудниками правильного использования средств обработки информации прежде, чем им будет предоставлен доступ к информации или услугам;

-оснащение сотрудников всем необходимым для соблюдения требований политики безопасности при выполнении служебных обязанностей.

Сотрудники должны знать и выполнять требования организационно-распорядительных документов (в части касающейся) в области информационной безопасности, требования обеспечения безопасности обработки информации на средствах вычислительной техники, правила работы в сети Интернет.

Сотрудники должны уметь работать с системой электронного документооборота; операционными средствами MS Windows на уровне пользователя, антивирусным программным обеспечением, офисным программным обеспечением (MS Word, MS Excel, MS Power Point), должны уметь пользоваться встроенной справкой.

Соответствующий специалист по информационной безопасности должен обучать сотрудников правильному пользованию средств обработки защиты информации, чтобы свести к минимуму возможные риски безопасности.

Все сотрудники, и при необходимости, пользователи третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик информационной безопасности, принятых в ЦГКБ №18.

# 8. Правила физической защиты

Перед внедрением и использованием нового аппаратного, программного обеспечения или иного ранее использовавшегося информационного ресурса необходимо разработать и использовать их наряду с правилами, изложенными в данном разделе.

Перед установкой и использованием какого-либо компьютерного аппаратного обеспечения в обязательном порядке следует ознакомиться с информацией, предоставленной разработчиком (продавцом), и строго ей следовать.

Перед проведением крупной модернизации или ремонта, перед выполнением манипуляций непосредственно с носителями информации необходимо выполнить резервное копирование данных.

После выполнения процесса модернизации аппаратного или программного обеспечения необходимо обязательно провести внеплановое техническое обслуживание всей системы.

При размещении компьютерного оборудования в помещении, а также в процессе его эксплуатации приоритетным является обеспечение для него безопасного функционирования, соответствующего положениям, изложенным в прилагаемой к нему документации. В период простоя устройства необходимо обеспечить сохранность его работоспособности и внешнего вида.

Все приобретенное компьютерное аппаратное и программное обеспечение должно регистрироваться в специальном журнале с указанием подробной информации о его покупке. Также следует тщательно регистрировать все действия по модернизации компьютерного аппарата и программного обеспечения.

Всю документацию на компьютерное оборудование и программное обеспечение (гарантийные обязательства производителей/продавцов, руководства пользователей (User's Manual) регистрированные карточки, кассовые и товарные чеки и проч.) должны обязательно сохранятся после покупки и храниться в надежном месте, защищенном от света и других вредоносных воздействий месте в упаковке.

Следует в полном объеме и неукоснительно соблюдать правила эксплуатации тех или иных аппаратных компьютерных компонентов.

Техническое обслуживание компьютерного оборудования и программного обеспечения (физическая чистка оборудования, поддержание программного обеспечения в работоспособном состоянии и т.д.), следует производить регулярно, желательно в соответствии с заранее составленным расписанием и с учетом рекомендаций разработчиков данного оборудования и программ (с данными рекомендациями следует внимательно ознакомиться до выполнения каких-либо действий по обслуживанию).

Техническим обслуживанием считаются также и мероприятия по резервному копированию данных, которые должны неукоснительно исполняться. Они должны выполняться строго и не реже, чем раз в неделю. Если это возможно, стоит сделать повторную копию данных и разместить ее на хранение отдельно от первой. Сразу же после проведения резервного копирования данных необходимо каким-либо способом убедиться в работоспособности и корректности полученной копии.

Резервному копированию в обязательном порядке подлежат:

-все конфиденциальные данные сотрудников в автоматизированной системе;

-все исходные материалы для разработки собственного программного обеспечения и прочих проектов;

-такие данные системы, без которых невозможна ее нормальная работа;

-все прочие важные данные, которые записаны на физически надежных носителях информации и носителях, поддерживающих операции перезаписи;

-любые другие данные согласно решению уполномоченных сотрудников соответствующего органа местного самоуправления.

Во время резервного копирования данных, а также во время записи любой информации на носители информации однократной записи, нельзя производить другие виды работ на той компьютерной системе, при помощи которой осуществляется эта запись.

Все носители (электронные, бумажные и все другие) с конфиденциальной информацией и резервными копиями этой и другой информации должны храниться в недоступном для посторонних, защищенном от света и других вредоносных воздействий месте, с соблюдением правил безопасного хранения для данного вида носителя информации. Носителям с особо ценной информацией следует уделять повышенное внимание.

Все расходные материалы следует использовать максимально эффективно, не допуская нерационального их использования. Все расходные материалы (используемые в данный момент и неиспользуемые) необходимо хранить в строгом соответствии с правилами их хранения.

Желательно предпринять ряд мер по энергоснабжению для тех устройств, которые временно не используются или находятся в состоянии ожидания.

Запрещается курить, употреблять пищу и напитки непосредственно вблизи компьютера. Необходимо предпринять меры, чтобы обезопасить компьютерное оборудование от повреждения в данном случае.

В течение внедрения и использования нового аппаратного, программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо приложить все усилия к тому, чтобы научиться эффективно его применять.

Необходимо в обязательном порядке записать все наиболее важные установки и настройки системы в состоянии ее нормального (штатного) функционирования. Подобные записи приравниваются к аппаратно-программной документации, и должны соответствующим образом обслуживаться.

Необходимо размещать системы вывода информации (мониторы, дисплеи и т.д.) компьютеров так, чтоб они не были видны со стороны двери, окон и тех мест в помещениях, которые не контролируется.

Необходимо предпринять ряд мер, благодаря которым компьютерные системы пользователя будут обеспечены стабильным электропитанием. Обязательным является использование хотя бы самых простых средств по обеспечению надежности электропитания системы (сетевые фильтры, заземление и т.д.).

При возникновении какой-либо аварийной ситуации необходимо немедленно прекратить эксплуатацию аварийного устройства. Немедленно поставить в известность главного врача. Соответствующему специалисту в кратчайшие сроки организовать мероприятия по его ремонту или замене.

Следует составить подробные технологические системы для проведения различного рода мероприятий, связанных с аппаратом и программным обеспечением (техническое обслуживание, правила техники безопасности, резервное копирование данных и т.п.).

Необходимо рассмотреть возможность применения различных систем автоматизированного мониторинга текущего состояния аппаратных информационных ресурсов, и при первой же возможности внедрить их, по крайней мере, наиболее важных и ответственных участках.

В течение процесса списания компьютерной техники, носителей информации и др. необходимо позаботиться о том, чтобы после выполнения процедуры переноса основных информационных ресурсов со списываемой техники, было произведено полное и безвозвратное уничтожение содержащейся на ней конфиденциальной и любой другой информации.

Необходимо обязательно разработать план действий по продолжению работы и обеспечению безопасности данных на случай, если выйдут из строя какие-либо аппаратные и (или) программные части компьютерной системы. Данный план должен систематически проверяться на актуальность и при необходимости пересматриваться.

# 9. Правила внешнего доступа

После установки системы и перед первым выходом в сеть необходимо в обязательном порядке принять комплекс мер по установлению защиты от вредоносного воздействия сети.

В системе должны быть предприняты все возможные меры для предотвращения распространения в ней компьютерных вирусов, "червей" и прочей потенциально опасной для ее безопасности информации. Все сотрудники обязаны принимать участие в реализации этих мер и никакими своими действиями не должны препятствовать их проведению.

Необходимо строго контролировать с помощью соответствующего программного обеспечения (антивирус, брандмауэр и проч.) всю входящую и исходящую информацию на наличие вирусов и прочей потенциально опасной информации. Необходимо также тщательно настроить параметры безопасности того программного и аппаратного обеспечения, которое непосредственно будет иметь доступ в сеть.

Система должна подвергаться периодической проверке антивирусными средствами (не реже чем раз в месяц) и другими средствами обеспечивающими безопасность в системе (если таковые имеются). В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники соответствующего органа местного самоуправления обязаны: приостановить работу на компьютере, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения, владельца зараженных файлов, смежные структурные подразделения, использующие эти файлы в работе, а также соответствующего специалиста по информационной безопасности.

Все внешние носители информации, полученные из сомнительных или неизвестных источников должны подвергаться полному антивирусному сканированию перед использованием.

Необходимо регулярно обновлять версии программного обеспечения, связанного с обеспечением безопасности системы; устанавливать официальные обновления программ, которые имеют прямое или косвенное отношение к работе с сетью. Сюда же относятся и обновления, связанные с управлением аппаратным обеспечением системы (драйверы устройств и т.п.).

При обнаружении зараженных вирусами данных, эти данные должны немедленно и безвозвратно удаляться. Исключение составляют лишь важные данные, для которых имеет смысл попробовать применить процедуры восстановления.

Следует с большой осторожностью относится к программам, в которых присутствуют определенного рода уязвимости для несанкционированного проникновения, или же в которых включены особые привилегии для их разработчиков.

Необходимо внимательно проанализировать систему данных сотрудника и обеспечить ее структурированное хранение на носителях информации. Все данные должны классифицироваться согласно их применению или же по другому, четко установленному сотрудником критерию (например, критериями могут служить соображения конфиденциальности данных, место из размещения и способ пересылки).

# 10. Правила доступа в Internet

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. ЦГКБ №18 оставляет за собой право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

При работе с ресурсами сети Интернет недопустимо:

-разглашение коммерческой и служебной информации ЦГКБ №18, ставшей известной сотруднику ЦГКБ №18 по служебной необходимости либо иным путем;

-распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

-публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию;

-сотрудники должны стараться предоставлять о себе как можно меньше информации в сеть, а тем более не должны разглашать любую конфиденциальную информацию.

При работе с ресурсами Интернет запрещается:

-загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.

-использовать анонимные прокси серверы.

-использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой компании.

После каждого сеанса связи с Интернетом необходимо проводить очистку системы от ненужных служебных данных, которые появились в результате соединения с сетью.

Все данные, полученные из Интернета должны систематизироваться и сохраняться.

Вся информация о ресурсах, посещаемых сотрудниками ЦГКБ №18, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а так же руководству ЦГКБ №18 для детального изучения.

ЦГКБ №18 несет финансовую ответственность за действия своих сотрудников.

# 11. Правила безопасности электронной почты

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности и неотделима от нее.

Электронная почта является собственностью ЦГКБ №18 и может быть использована **ТОЛЬКО** в служебных целях. Использование электронной почты в других целях категорически запрещено.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

Все наиболее важные сообщения электронной почты должны архивироваться, особенно те сообщения, которые присланы официальными группами технической поддержки каких-либо информационных ресурсов. Также регулярной архивации должна подвергаться информация, касающаяся данных о тех сотрудниках, с которыми осуществляется связь средствами электронной почты (адресные книги и т.д.).

Все ранее сохраненные почтовые сообщения, потерявшие свою актуальность, должны быть тщательным образом безвозвратно уничтожены со всех носителей информации.

Необходимо в обязательном порядке сканировать каждое исходящее и получаемое сообщение электронной почты на наличие потенциально опасного содержимого (вирусы, "черви" и т.д.). Почтовые сообщения, не удовлетворяющие установленным требованиям, должны немедленно и безвозвратно удаляться.

Необходимо на всех используемых почтовых ящиках установить, при необходимости, ограничения на содержимое и размер принимаемых сообщений и отсеивать те сообщения, которые не удовлетворяют установленным критериям.

После отправки письма по электронной почте необходимо хранить его до тех пор, пока не будет уверенности (подтверждения) в том, что оно достигло получателя. Это же касается и любых других способов передачи информации. Все файлы (особенно исполнимые и файлы больших размеров), полученные вместе с сообщением электронной почты без какого-либо запроса со стороны сотрудника соответствующего органа местного самоуправления (особенно от неизвестного адресата) должны немедленно и безвозвратно удаляться без оценки их полезности. При этом каждый подобный факт должен быть зарегистрирован. Если полной уверенности и необходимости удаления данного сообщения, необходимо, в случае если адресат известен и только в этом случае, дополнительно связаться с ним (не по электронной почте) и попросить у него подтверждения в посылке сообщения.

Сотрудники ЦГКБ №18 не должны участвовать в рассылке посланий, передаваемых по цепочке, не должны отвечать на оскорбительные и провокационные сообщения. Такие послания должны быть сначала переданы службам технической поддержки используемых почтовых сервисов для анализа, а после этого - безвозвратно удалены из системы. Также необходимо принять все возможные меры по обеспечению прекращения получения из данного источника подобной информации в будущем.

**При работе** с **корпоративной системой электронной почты сотрудникам организации запрещается:**

-использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с сотрудником, назначенным приказом за обеспечение информационной безопасности ЦГКБ №18;

-публиковать свой адрес, либо адреса других сотрудников ЦГКБ №18 на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

-отправлять сообщения с вложенными файлами общий объем которых превышает 10 Мегабайт.

-открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

-осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными.

-осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с сотрудником, назначенным приказом за обеспечение информационной безопасности ЦГКБ №18;

-рассылка через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

-распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны.

-распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

-распространять информацию ограниченного доступа, представляющую коммерческую тайну;

-предоставлять, кому бы-то ни было пароль доступа к своему почтовому ящику;

# 12. Правила управления доступом

В отношении всех основных и не основных (гости и проч.) сотрудников необходимо осуществлять комплекс мер по обеспечению их работы в автоматизированной системе, в частности регистрацию, выделение определенных информационных ресурсов и установление четких, не избыточных, а только необходимых, прав доступа к ним.

Служба регистрации должна обеспечить положительную аутентификацию. Это даст гарантию того, что законный пользователь получит доступ к системе.

Необходимо в обязательном порядке регистрировать все неудачные попытки входа в систему, а также вести аудит доступа сотрудников к ее объектам и периодически просматривать результаты его работы.

При первой же необходимости работы с системой при помощи удаленного доступа или же с локальной сетью необходимо разработать правила безопасности, регламентирующие данные виды работ.

Использование имен и паролей для доступа к информационным ресурсам:

-необходимо использовать пароли везде, где это целесообразно;

-следует придерживаться следующих правил составления и использования паролей - пароль должен состоять не менее чем из шести символов, состоять из произвольных комбинаций букв, цифр и других символов или же представлять собой бессмысленную комбинацию слов, включающую буквы верхнего регистра;

-необходимо менять все пароли не реже, чем раз в два месяца (желательно делать это не по графику), при этом использовать пароли повторно не разрешается;

-запрещено использовать одинаковые пароли к разным информационным ресурсам;

-пароли необходимо хранить в надежном, недоступном для посторонних месте или использовать специальные аппаратные средства для их хранения;

-хранения паролей осуществляется операционной системой, и установленный ею уровень защиты не может быть ослаблен;

-запрещено сообщать свои пароли третьим лицам в какой-бы то ни было форме;

-пароли запрещается писать на компьютерных терминалах, помещать в общедоступные места;

-необходимо заменить все пароли, назначенные системой по умолчанию, на собственные, а потом, если это возможно, отключить возможность доступа к данному ресурсу по стандартному паролю;

-все имена и пароли для доступа к каким-либо информационным ресурсам, которые не используются, подлежат надежной блокировке;

-система должна предотвращать попытки регистрации и перерегистрации тех сотрудников, чьи имена и пароли для входа в систему не соответствуют установленным правилам;

-при получении доступа к какому-либо информационному ресурсу при помощи процесса авторизации по имени (паролю), сотрудник не должен произносить эти данные вслух при вводе их в систему;

-изменять пароли необходимо всякий раз, когда есть указания на возможную компрометацию систем или паролей.

# 13. Управление непрерывностью работы

Основной целью управления непрерывностью работы является противодействие прерыванию работы и защита рабочих процессов от последствий при значительных сбоях или бедствиях.

Необходимо обеспечивать управление непрерывностью работы с целью минимизации отрицательных последствий, вызванных нарушениями безопасности. Последствия от нарушений безопасности и отказов в обслуживании необходимо анализировать и внедрять планы обеспечения непрерывности с целью восстановления рабочих процессов в течении требуемого времени при их нарушении. Такие планы следует поддерживать и применять на практике. Должна быть выработана стратегия непрерывности рабочего процесса в соответствии с согласованными целями и приоритетами.

Необходимо чтобы планирование непрерывности работы начиналось с идентификации событий, которые могут быть причиной прерывания работы, например отказ оборудования, наводнение или пожар. Планирование должно сопровождаться оценкой рисков с целью определения последствий этих прерываний (как с точки зрения масштаба повреждения, так и периода восстановления). Оценка риска должна распространяться на все рабочие процессы и не ограничиваться только средствами обработки информации. В зависимости от результатов оценки рисков необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности работы.

Разработанный план должен быть утвержден главным врачом ЦГКБ №18.

Необходимо, чтобы план обеспечения непрерывности работы предусматривал следующие мероприятия по обеспечению информационной безопасности:

-определение и согласование всех обязанностей должностных лиц и процедур на случай чрезвычайных ситуаций;

-внедрение в случае чрезвычайных ситуаций процедур, обеспечивающих возможность восстановления рабочего процесса в течение требуемого времени;

-особое влияние следует уделять оценке зависимости работы от внешних факторов и существующих контрактов;

-документирование согласованных процедур и процессов;

-соответствующее обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление.

Необходимо, чтобы план обеспечения непрерывности работы соответствовал требуемым целям работы.

# 14. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных.

-типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

-типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

-необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

-в персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

# 15. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

# 16. Ответственность за нарушение политики безопасности

Все сотрудники ЦГКБ №18 несут ответственность за нарушение требований настоящей Политики информационной безопасности согласно действующему [законодательству](garantF1://12048555.0)в области защиты информации.

# 17. Сопровождение правил

Все без исключения положения данного документа имеют одинаково равную силу и должны неукоснительно соблюдаться.

Политика информационной безопасности должна в обязательном порядке периодически перечитываться и пересматриваться (не реже чем один раз в год).

Ежемесячно должна проводиться оценка текущего состояния имеющихся у сотрудников информационных ресурсов. В результате этой оценки в соответствующие документы по безопасности должны вноситься необходимые изменения (если они есть).

При проведении каких-либо изменений в данных правилах, соответствующие изменения, при необходимости, должны производиться и в других документах, касающихся обеспечения безопасности.

Если возникли непредвиденные обстоятельства, требующие срочного пересмотра Политики информационной безопасности, то такой пересмотр может быть осуществлен до планового пересмотра.

При возникновении серьезных проблем с безопасностью системы (например, при успешном взломе системы безопасности) возникшая проблема должна быть немедленно проанализирована, а организационно-распорядительные документы по информационной безопасности - пересмотрены в соответствии с проведенным анализом. При этом нужно рассматривать проблему в целом и излишне не фокусировать внимание на отдельных деталях.

Копия настоящей Политики должна находиться в доступном для сотрудников месте.