УТВЕРЖДАЮ

Главный врач
ГАУЗ РКОД Минздрава РБ

_____ **А.А. Измайлов**

«25» мая **2022 г.**

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГАУЗ Республиканский клинический онкологический диспансер

Минздрава РБ

Общие положения

Политика информационной безопасности ГАУЗ РКОД Минздрава РБ (далее – Политика) предполагает создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, определяющих порядок обеспечения безопасности информации в информационных системах, управления и контроля информационной безопасности, а также выдвигающих требования по поддержанию подобного порядка.

Политика отражает позицию руководства по вопросу обеспечения информационной безопасности диспансера.

Политика направлена на:

- нормативное регулирование процесса обмена защищаемой информацией диспансера с вышестоящими органами, соответствующими Министерствами, с взаимодействующими структурами, юридическими и физическими лицами;
- установление определенного организационно-правового режима использования информационных ресурсов диспансера;
- разработку системы нормативных документов диспансера, действующих на правах стандартов и определяющих степень конфиденциальности информации, требуемый уровень защищенности объектов информатизации диспансера, 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 диспансера;
- организацию постоянного контроля эффективности принятых мер защиты и функционирования системы обеспечения информационной безопасности диспансера;
- создание в исполнительном комитете резервов и возможностей по ликвидации последствий нарушения режима защиты информации и восстановления системы обеспечения информационной безопасности.

Цель обеспечения информационной безопасности

Основной целью является обеспечение информационной безопасности диспансера, 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 ГАУЗ РКОД Минздрава РБ 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) ГАУЗ РКОД Минздрава РБ, независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности диспансера, не жертвуя при этом основными принципами информационной безопасности, описанными в данной Политике.

Ответственность за организацию и проведение работ по обеспечению информационной безопасности ГАУЗ РКОД Минздрава РБ несет руководитель ГАУЗ РКОД Минздрава РБ. Методическое руководство и контроль за эффективностью предусмотренных мер защиты осуществляет назначенный руководителем ответственный за информационную безопасность ГАУЗ РКОД Минздрава РБ.

Объекты информационной безопасности

Объектом защиты в контексте данной Политики являются информационные ресурсы ГАУЗ РКОД Минздрава РБ, 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 ГАУЗ РКОД Минздрава РБ.

Основными объектами защиты ГАУЗ РКОД Минздрава РБ являются:

– информационные ресурсы ГАУЗ РКОД Минздрава РБ ограниченного распространения, в том числе содержащие конфиденциальные сведения;

– программные информационные ресурсы ГАУЗ РКОД Минздрава РБ, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

– физические информационные ресурсы ГАУЗ РКОД Минздрава РБ:

- компьютерное аппаратное обеспечение всех видов;
- носители информации всех видов (электронные, бумажные и прочие);
- все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением;
- технические сервисы ГАУЗ РКОД Минздрава РБ (отопление, освещение, энергоснабжение, 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. И доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения имиджа ГАУЗ РКОД Минздрава РБ, 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.

Задачи обеспечения информационной безопасности

Основными задачами обеспечения информационной безопасности ГАУЗ РКОД Минздрава РБ являются:

– инвентаризация и систематизация всех информационных ресурсов ГАУЗ РКОД Минздрава РБ;

– обеспечение безопасности информационных ресурсов диспансера, 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 реагирования по случаям инцидентов;

– обеспечение безопасной, четкой и эффективной работы сотрудников ГАУЗ РКОД Минздрава РБ 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 прочее);

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

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 диспансера.

Оценка рисков

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

- ущерб, который может нанести деятельности ГАУЗ РКОД Минздрава РБ 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.

Требования в отношении обучения вопросам информационной безопасности

Основной целью обучения является:

– обеспечение уверенности в осведомленности сотрудников ГАУЗ РКОД Минздрава РБ об угрозах и проблемах, связанных с информационной безопасностью, об ответственности в соответствии с законодательством;

– знание работниками правильного использования средств обработки информации прежде чем им будет предоставлен доступ к информации или услугам;

– оснащение работников диспансера всем необходимым для соблюдения требований политики безопасности больницы при выполнении служебных обязанностей.

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

Работники диспансера, для исполнения своих служебных обязанностей с применением компьютерной техники, должны уметь работать на уровне пользователя с операционными системами, антивирусным программным обеспечением, офисным программным обеспечением, средством архивации.

Сотрудники отдела УИТ должны обучать работников диспансера правильному использованию средств обработки защиты информации, чтобы свести к минимуму возможные риски безопасности.

Правила физической защиты

Перед внедрением и использованием нового аппаратного, программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо разработать для него правила обеспечения безопасности 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 и (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 его безопасного функционирования, соответствующего положениям, изложенным в прилагаемой к нему документации. В период простоя устройства необходимо обеспечить сохранность его работоспособности и внешнего вида.

Всю документацию на компьютерное оборудование и программное обеспечение (гарантийные обязательства производителей (продавцов), руководства пользователей (User's Manual), регистрационные карточки, кассовые и товарные чеки и прочее) должны обязательно сохраняться после покупки и храниться в надежном, 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 регулярно 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 ненадежных носителях информации и носителях, поддерживающих операции перезаписи;

– любые другие данные согласно решению уполномоченных работников

больницы.

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 др.) с конфиденциальной информацией и резервными копиями этой и другой информации сотрудника диспансера 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 энергосбережению 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 аппаратной (программной) документации и должны соответствующим образом обслуживаться.

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

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 руководителя отдела УИТ.

Отделу УИТ в кратчайшие сроки организовать мероприятия по его ремонту или замене.

Следует составить подробные технологические схемы для проведения различного рода мероприятий, связанных с аппаратным 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, на 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.

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 работники больницы 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 прочее) 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 работники больницы обязаны: приостановить работу на компьютере, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя отдела, владельца зараженных файлов, смежные отделы, 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).

Правила доступа в Интернет

Программное обеспечение, обеспечивающее защиту системы от проникновения, должно быть задействовано в полном объеме на протяжении всего сеанса связи с Интернетом.

Допускается временное отключение части программного обеспечения, обеспечивающего защиту системы, в тех случаях, когда без этого невозможно выполнить какой-либо вид работы. После выполнения данного вида работ отключенные части системы защиты должны быть вновь задействованы.

Работники диспансера допускаются к использованию Интернета только после прохождения инструктажа, в котором разъяснялась бы Политика безопасности данной системы в отношении глобальной сети, и с письменного подтверждения руководителя подразделения, сотрудникам которого необходим допуск к сети Интернета, о производственной необходимости допуска к сети Интернет и с перечнем сайтов, к которым будет открыт доступ.

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

Все файлы, полученные из Интернета, перед их использованием должны пройти дополнительную антивирусную проверку.

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.

Правила безопасности электронной почты

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 работники больницы (особенно от неизвестного адресата) должны немедленно и безвозвратно удаляться без оценки их полезности. При этом каждый подобный факт должен быть зарегистрирован. Если нет полной уверенности в 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.

Работники диспансера 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.

Правила управления доступом

В отношении всех основных и не основных (гости и прочее) работников диспансера необходимо осуществлять комплекс мер по обеспечению их работы в автоматизированной системе диспансера, 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 удачные и неудачные попытки входа в систему, а также вести аудит доступа работников диспансера 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 осуществляется на основании Политики парольной защиты ГАУЗ РКОД Минздрава РБ.

Управление непрерывностью работы диспансера

Основной целью управления непрерывностью работы диспансера является противодействие прерывания 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, по результатам анализа разрабатывать и внедрять планы обеспечения непрерывности работы с целью восстановления рабочих процессов в течение 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 руководством диспансера. 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.

Ответственность за нарушение политики безопасности

Все работники диспансера несут ответственность за нарушение требований настоящей Политики согласно действующему законодательству в области защиты информации.

Сопровождение правил

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

Политика 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, 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.

Все работники диспансера должны быть ознакомлены с Политикой.

Копия настоящей Политики должна находиться в доступном для работников и пациентов ГАУЗ РКОД Минздрава РБ месте – официальном сайте диспансера: www.onkorb.ru