Приложение к приказу
ФГБУ «НИДОИ им. Г.И. Турнера»
Минздрава России
от « 22 » 02 2018 г. № 83

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
федерального государственного бюджетного учреждения «Научно-исследовательский детский ортопедический институт имени Г.И. Турнера» Министерства здравоохранения Российской Федерации

Общие положения

Политика информационной безопасности (далее – Политика) федерального государственного бюджетного учреждения «Научно-исследовательский детский ортопедический институт имени Г.И. Турнера» Министерства здравоохранения Российской Федерации 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 информационной безопасности отражает позицию руководства по вопросу обеспечения информационной безопасности федерального государственного бюджетного учреждения «Научно-исследовательский детский ортопедический институт имени Г.И. Турнера» Министерства здравоохранения Российской Федерации (далее – Институт).

Политика информационной безопасности Института направлена на:

нормативное регулирование процесса обмена защищаемой информацией Института с вышестоящими органами государственной и исполнительной власти, соответствующими министерствами, с взаимодействующими структурами, юридическими и физическими лицами;

установление определенного организационно-правового режима использования информационных ресурсов Института;

разработку системы нормативных документов Института, действующих на правах стандартов и определяющих степень конфиденциальности информации, требуемый уровень защищенности объектов информатизации Института, 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 Института;

организацию постоянного контроля эффективности принятых мер защиты и

функционирования системы обеспечения информационной безопасности Института;

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

Настоящий документ разработан в соответствии с требованиями Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ и национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

Цель обеспечения информационной безопасности

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

Ответственность за организацию и проведение работ по обеспечению информационной безопасности Института несет директор ФГБУ «НИДОИ им. Г.И. Турнера» Минздрава России. В Институте осуществляется разработка проектов объектов информатизации в защищенном исполнении и их эксплуатация с учетом требований по защите информации. Методическое руководство и контроль за эффективностью предусмотренных мер защиты осуществляет назначенный директором ФГБУ «НИДОИ им. Г.И. Турнера» Минздрава России ответственный за информационную безопасность Института.

Объекты информационной безопасности

Объектом защиты в контексте данной Политики являются информационные ресурсы ФГБУ «НИДОИ им. Г.И. Турнера» Минздрава России, 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 Института.

Основными объектами защиты Института являются:

1. информационные ресурсы ограниченного распространения, в том числе содержащие конфиденциальные сведения;
2. программные информационные ресурсы, а именно:

2.1. прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

2.2. физические информационные ресурсы Института:

- 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 Института (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 Института, 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 Института являются:

- Инвентаризация и систематизация всех информационных ресурсов Института;
- обеспечение безопасности информационных ресурсов Института, 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 Института 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

Института.

Оценка рисков

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

ущерб, который может нанести деятельности Института 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 Института об угрозах и проблемах, связанных с информационной безопасностью, об ответственности в соответствии с законодательством Российской Федерации;
- знание сотрудниками правильного использования средств обработки информации прежде чем им будет предоставлен доступ к информации или услугам;
- оснащение сотрудников Института всем необходимым для соблюдения требований политики безопасности Института при выполнении служебных обязанностей.

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

Сотрудники Института должны уметь работать с системой электронного документооборота, операционными системами на уровне пользователя, антивирусным программным обеспечением, офисным программным обеспечением, средством архивации, должны уметь пользоваться почтовыми программами.

Специалист по информационной безопасности должен инструктировать сотрудников Института правильному использованию средств обработки защиты информации, чтобы свести к минимуму возможные риски безопасности.

Все сотрудники Института при необходимости должны проходить соответствующее обучение и получать на регулярной основе обновленные варианты политики информационной безопасности, принятые администрацией Института.

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.

Всю документацию на компьютерное оборудование и программное обеспечение (гарантийные обязательства производителей (продавцов), 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 регулярно исполняться. 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 должностных лиц Института.

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 Института 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 с компьютерным оборудованием необходимо немедленно прекратить эксплуатацию аварийного устройства. Немедленно поставить в известность начальника отдела информационных технологий (системного администратора).

Отделу информационных технологий (системному администратору) в кратчайшие сроки организовать мероприятия по его ремонту или замене.

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 сотрудники Института 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 и другими средствами, обеспечивающими безопасность в системе (если таковые имеются). В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники Института 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 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.

Сотрудники Института допускаются к использованию Интернета только после прохождения инструктажа, в котором разъяснялась бы Политика безопасности данной системы в отношении глобальной сети.

Сотрудники Института 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 файлы), полученные вместе с сообщением электронной почты без какого-либо запроса со стороны сотрудника Института (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.

Сотрудники Института 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) сотрудников Института необходимо осуществлять комплекс мер по обеспечению их работы в автоматизированной системе Института, 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.

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 для доступа к разным информационным ресурсам;

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

- хранение 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 и 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.

Управление непрерывностью работы Института

Основной целью управления непрерывностью работы Института 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 директором Института. 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 контактов;
- 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 сотрудники Института несут персональную ответственность за нарушение требований настоящей Политики информационной безопасности согласно действующему законодательству Российской Федерации в области защиты информации.

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 и пациентов (их законных представителей) ФГБУ «НИДОИ им. Г.И. Турнера» Минздрава России месте.