УТВЕРЖДАЮ
Главный врач
БУ Лянторская городская больница
_____ / _____
«23» 12 2016 года

Политика
информационной безопасности бюджетного учреждения Ханты-Мансийского автономного округа - Югры «Лянторская городская больница»

Определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система АРМ – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система – представляющая собой совокупность данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких данных с использованием средств автоматизации или без использования таких средств.

Нарушитель безопасности – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности данных при их обработке техническими средствами в информационных системах данных.

Несанкционированный доступ (несанкционированные действия, НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Общие положения

Настоящая Политика информационной безопасности (далее – Политика) бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Лянторская городская больница» (далее – МО), определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих положений, правил, инструкций.

Политика учитывает текущее состояние и перспективы развития информационных технологий в МО, правовые основы их эксплуатации, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений МО.

В Политике определены требования к работникам МО, степень их ответственности, за обеспечение безопасности информации в информационных системах МО.

Требования настоящей Политики распространяются на всех работников МО (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

Цели и задачи политики информационной безопасности

Целью настоящей Политики является выработка единых требований и правил, обеспечивающих непрерывность основных бизнес-процессов, минимизацию возможных потерь и ущерба от нарушений в области информационной безопасности.

Основными задачами системы информационной безопасности являются:

- Отнесение информации к категории общедоступной, ограниченного распространения, персональным данным, коммерческой и другим видам тайн, иной конфиденциальной информации, подлежащей защите;
- Прогнозирование и своевременное выявление угроз безопасности информационным ресурсам МО, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- Создание условий функционирования МО с наименьшей вероятностью реализации угроз безопасности в информационных ресурсах и нанесения ущерба;
- Создание механизма и условий оперативного реагирования на угрозы

информационной безопасности и проявление негативных тенденций в функционировании МО, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;

- Создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц.

Объекты защиты информационной безопасности

Объектами защиты являются информация, обрабатываемая в информационных системах МО, и технические средства ее обработки и защиты.

Перечень защищаемой информации утверждается Главным врачом МО и включает в себя персональные данные, конфиденциальную, служебную тайну и другую защищаемую информацию.

Объекты защиты включают в себя:

- Обрабатываемую информацию;
- Технологическую информацию;
- Программно-технические средства обработки;
- Средства защиты информации;
- Каналы информационного обмена и телекоммуникации;
- Объекты и помещения, в которых размещены компоненты информационных систем.

Угрозы безопасности защищаемой информации

Основные угрозы безопасности защищаемой информации:

- Угрозы от утечки по техническим каналам;
- Угрозы несанкционированного доступа к информации;
- Угрозы уничтожения, хищения аппаратных средств носителей информации путем физического доступа к элементам информационных систем.
- Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования информационных систем, сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

- Угрозы преднамеренных действий внутренних нарушителей.
- Угрозы несанкционированного доступа по каналам связи.

Меры безопасности

Для обеспечения физической защиты информационных ресурсов МО в границах контролируемой зоны (здание стационара МО, расположенное по адресу: г. Лянтор, ул. С. Юлаева 7, кабинет на втором этаже) устанавливаются зоны безопасности и принимаются меры для предотвращения неавторизованного (несанкционированного) доступа в помещения, где происходит обработка защищаемой информации.

Двери кабинетов должны быть прочными, окна кабинетов оборудуются жалюзи. Окна кабинетов расположенные на первом, последнем этажах, и расположенные рядом с пожарными лестницами, где обрабатывается защищаемая информация, оборудуются дополнительно защищающим ограждением (внешним, внутренним), с соблюдением норм противопожарной охраны.

Двери кабинетов должны быть постоянно закрыты и открываться только для прохода работников и посетителей МО.

Уборка в кабинетах, где происходит, обработка защищаемой информации должна производиться в присутствии ответственного лица, за которым закреплено данное рабочее место, с соблюдением мер исключающим доступ к защищаемой информации.

Обработка защищаемой информации должна производиться без присутствия посторонних лиц в помещении, если требование этой меры безопасности невозможно выполнить, то необходимо минимизировать возможность видовой утечки защищаемой информации путем соответствующего расположения рабочего места.

Для уничтожения черновиков документов кабинеты должны быть оборудованы уничтожителями бумаг, CD, DVD дисков.

Помещение серверной должно быть оборудовано прочной металлической дверью с замком и опечатывающим устройством, пожарно-охранной сигнализацией, кондиционером, системой контроля доступа.

Охранно-пожарная сигнализация кабинетов должная быть с выводом на пульт дежурного охранника или на пульт вневедомственной охраны.

По окончании работы работники МО должны закрывать дверь на ключ.

Допуск работников к ресурсам информационной системы должен быть регламентирован. Уровень полномочий каждого пользователя информационной системы должен соответствовать его должностным обязанностям. Расширение прав должно

согласовываться с отделом ответственным за данный информационный ресурс с разрешения Главного врача МО.

Обработка информации в информационных системах должна происходить в соответствии с инструкциями по эксплуатации этих информационных ресурсов.

Все неиспользуемые в работе устройства ввода-вывода информации (WiFi, COM, LPT, USB, IR порты, дисководы ГМД, CD, DVD и т.п.) на рабочих местах работников, работающих с защищаемой информацией, должны быть по возможности отключены, не нужные для работы программные средства и данные с дисков также должны быть удалены.

Дополнительные устройства обмена информацией могут использоваться только в исключительных случаях и только в качестве временного средства. Установка подобных устройств должна согласовываться с отделом информационных технологий. Порядок их использования определяется отдельным документом.

На АРМ всех пользователей локальной сети МО устанавливается антивирусная программа. Антивирусная программа должна автоматически обновлять базу не реже одного раза в день. Полная проверка АРМ на вирусы должна быть настроена не реже одного раза в неделю. Быстрая проверка АРМ на вирусы должна быть настроена не реже одного раза в день. Права на антивирус должны быть, настроены так, чтобы пользователь имел минимальные права по управлению настройками Антивирусной программы.

Доступ к ресурсам информационной системы (вход в операционную систему, в прикладное программное обеспечение) должен быть организован с применением аутентификации (введение логина, пароля). При возможности программно-аппаратными средствами аутентификации с использованием Ru-Token, или E-Token.

Пароли пользователя и администраторов информационных систем должны соответствовать Парольной политике МО и меняться раз в три месяца.

Права пользователя в операционной системе должны быть минимальными, в прикладных программных продуктах в соответствии со своими должностными обязанностями.

На учетную запись администратора BIOS установить пароль, загрузка операционной системы должна быть установлена с жесткого диска.

На границе локальной сети должен быть установлен маршрутизатор. Сеть для разных информационных систем должна быть сегментирована.

Средства защиты информации применяемые на АРМ пользователей и в информационных системах устанавливаются и настраиваются специалистом отдела информационных технологий. Доступ пользователей к публичным ресурсам сети

Интернет регулироваться Инструкцией по работе с сетью Интернет.

При передаче защищаемых данных использовать криптографические средства защиты информации.

Для восстановления информационных систем от сбоев должен быть разработан План восстановления работоспособности информационных систем.

Требования к работникам

Все пользователи информационной системы должны быть ознакомлены с организационно - распорядительными документами по обеспечению информационной безопасности, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

При вступлении в должность нового работника начальник отдела информационных технологий, обязан организовать его ознакомление с инструкцией и документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных ресурсов.

Работники МО, использующие технические средства аутентификации, обеспечивают сохранность идентификаторов (электронных ключей) не должны допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники МО должны соблюдать установленные процедуры поддержания режима безопасности при выборе и использовании паролей (если не используются технические средства аутентификации).

Работникам МО категорически запрещено оставлять без присмотра АРМ, содержащие защищаемую информацию. Все пользователи должны знать требования по безопасности и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

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

Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами и бумажными носителями МО, третьим лицам.

При работе с защищаемой информацией работники МО обязаны обеспечить защиту от просмотра информации третьими лицами с мониторов АРМ.

При завершении работы работники обязаны защитить АРМ с помощью блокировки ключом (Ru-Token, E-Token) или, например, доступом по паролю (), если не используются более сильные средства защиты.

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

Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационной системы, которые могут повлечь за собой угрозы безопасности защищаемой информации, а также о выявленных ими событиях, затрагивающих безопасность информации, начальнику отдела и лицу, отвечающему за безопасность в МО.

Ответственность работников МО

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

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

Специалисты отдела информационных технологий несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях работниками МО - пользователями информационных систем правил, связанных с информационной безопасностью, они несут ответственность, установленную действующим законодательством Российской Федерации.

В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность конфиденциальной информации, ставшей известной в силу выполнения своих обязанностей.

Порядок внесения изменений и дополнений

Настоящая Политика вступает в законную силу с даты подписания Главным врачом МО. Изменения и дополнения в настоящую Политику вносятся по инициативе Главного врача, Начальника отдела информационных технологий и утверждаются Главным врачом МО в связи с изменением условий обработки информации других условий приведших к появлению новых угроз безопасности.

В случае вступления отдельных пунктов в противоречие с новыми законодательными актами, эти пункты утрачивают юридическую силу до момента внесения изменений в настоящую Политику.

Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 28.12.2013) «Об информации, информационных технологиях и о защите информации.
2. Федеральный закон об основах охраны здоровья граждан в Российской федерации № 323-ФЗ от 21.11.2011 г.
3. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»
4. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
5. «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.