Казенное учреждение Ханты-Мансийского автономного округа-Югры
«Детский противотуберкулёзный санаторий имени Е.М. Сагандуковой»

ПРИКАЗ

Дата 26.02.2016 г. № 23 -о

г. Ханты-Мансийск

«Об утверждении политики информационной безопасности»

В соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности казенного учреждения Ханты-Мансийского автономного округа – Югры «Детский противотуберкулезный санаторий имени Е.М. Сагандуковой» (Приложение).

2. Секретарю руководителя Мавлютовой Е.А. довести настоящий приказ до руководителей структурных подразделений Учреждения.

3. Руководителям структурных подразделений Учреждения:

3.1. ознакомить работников подразделения с Политикой информационной безопасности под роспись;

3.2. осуществлять внутренний контроль над исполнением требований Политики в подразделении.

4.Инженеру программисту Круглову А.В. разместить настоящий приказ на официальном сайте учреждения в течение одного рабочего дня с момента его подписания.

5. Контроль исполнения настоящего приказа возложить на начальника отдела материально-технического снабжения А.А. Нугманова.

Главный врач А.А. Таберт

Приложение
к приказу от 26.02. 2016 года № 23-о

Политика информационной безопасности
казенного учреждения Ханты-Мансийского автономного округа – Югры
«Детский противотуберкулезный санаторий имени Е.М. Сагандуковой»

Определения

Используемые в настоящем документе термины и их определения.

Защищаемая информация – информация, подлежащая защите в соответствии с требованиями нормативных документов в области безопасности информации или требованиями, устанавливаемыми собственником информации.

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

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

Угроза безопасности информации – некая совокупность факторов и условий, которая создает опасность в отношении защищаемой информации.

Правила разграничения доступа – совокупность правил, регламентирующих порядок и условия доступа субъектов доступа (сотрудников, программ) к объектам доступа (информации, её носителям, процессам и другим ресурсам).

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

Персональные данные – любая информация, относящаяся к прямо или косвенно 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.

Контролируемая зона – это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Дополнительные устройства обмена информацией – портативные жесткие диски, съемные флэш-носители, CD, DVD – диски.

Общие положения

Настоящая политика информационной безопасности (далее – Политика) казенного учреждения Ханты-Мансийского автономного округа – Югры «Детский

противотуберкулезный санаторий имени Е.М. Сагандуковой» (далее – Учреждение) разработана на основе требований действующих в Российской Федерации законодательных и нормативных документов, регламентирующих вопросы защиты информации, с учетом современного состояния, целей, задач и правовых основ создания, эксплуатации и функционирования информационных систем Учреждения, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений Учреждения.

Политика определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих положений, правил, инструкций.

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

Требования настоящей Политики распространяются на всех работников Учреждения (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 настоящей Политики являются:

– отнесение информации к категории общедоступной, ограниченного распространения, персональным данным, коммерческой и другим видам тайн, иной конфиденциальной информации, подлежащей защите;

– предотвращение несанкционированного доступа к защищаемой информации и (или) передачи её лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов несанкционированного доступа к защищаемой информации;

– недопущение воздействия на технические средства автоматизированной обработки защищаемой информации, в результате которого может быть нарушена её конфиденциальность, доступность, целостность;

– возможность незамедлительного восстановления защищаемой информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ним;

– постоянный контроль над обеспечением уровня защищённости информации;

– прогнозирование и своевременное выявление угроз безопасности информации, обрабатываемой в информационных системах Учреждения, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

– создание условий функционирования Учреждения 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 Учреждения, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности.

Объекты защиты информационной безопасности

Объектами защиты являются защищаемая информация, обрабатываемая в информационных системах Учреждения, технические и программные средства ее обработки, передачи и защиты.

Перечень защищаемой информации утверждается главным врачом Учреждения 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;
- программные и аппаратные 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 непреднамеренных 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 приказом главного врача Учреждения должны быть установлены границы контролируемой зоны, приняты меры для предотвращения неавторизованного (несанкционированного) доступа в помещения где происходит обработка защищаемой информации.

Входы на этажи должны быть оборудованы системой контроля доступа, двери кабинетов должны быть оборудованы опечатывающим устройством. В кабинетах

должны быть приняты меры для затруднения видимости посторонним лицам в виде штор/жалюзи. Кабинеты в нерабочее время должны опечатываться.

Двери кабинетов должны быть закрыты и должны открываться только для прохода работников и посетителей Учреждения согласно утвержденным правилам доступа в границы контролируемой зоны.

Уборка в кабинетах должна производиться только в присутствии работников Учреждения, с соблюдением мер, исключающих доступ к защищаемой информации и оборудованию.

Обработка защищаемой информации в помещениях Учреждения должна производиться таким образом, чтобы исключать ознакомление с защищаемой информацией лицами, не имеющими прав доступа к данной информации.

Для хранения документов, содержащих защищаемую информацию, кабинеты Учреждения должны быть оборудованы сейфами, металлическими шкафами с замками и опечатывающими устройствами.

Для уничтожения черновиков документов, содержащих защищаемую информацию, кабинеты должны быть оборудованы уничтожителями бумаг.

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

Охранно-пожарная сигнализация кабинетов должна реализоваться с выводом на пульт дежурного охранника или на пульт вневедомственной охраны.

По окончании рабочего дня работники Учреждения должны закрывать двери кабинетов на ключ и опечатывать её.

Печати, предназначенные для опечатывания кабинетов, сейфов, металлических шкафов должны храниться у уполномоченных работников.

Допуск работников к ресурсам информационных систем 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 и отделом по защите информации с разрешения главного врача Учреждения.

Обработка информации в информационных системах должна происходить в соответствии с документами, регламентирующими порядок работы в данной информационной системе.

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 жестких дисков удалены.

Дополнительные устройства обмена информацией могут использоваться только в целях переноса информации. Использование подобных устройств должно согласовываться с уполномоченным сотрудником Учреждения. Порядок использования дополнительных устройства обмена информацией определяется соответствующим регламентом.

На АРМ всех пользователей локальной сети Учреждения должна быть установлена антивирусная программа. Порядок управления антивирусной защитой в Учреждении определяется соответствующим регламентом.

Доступ к ресурсам информационной системы (вход в операционную систему, в прикладное программное обеспечение) должен быть организован с применением

аутентификации (введение логина, пароля). Возможно использование дополнительных программно-аппаратных средств аутентификации (в том числе двух- и трехфакторной).

Требования паролей пользователей и администраторов информационных систем устанавливаются соответствующим регламентом.

Установкой и настройкой средств защиты информации, применяемых для защиты информации в информационных системах, должен руководить уполномоченный сотрудник отдела по защите информации.

Доступ пользователей к публичным ресурсам сети Интернет определяется соответствующим регламентом.

Передача защищаемой информации по каналам, выходящим за границы контролируемой зоны, должна осуществляться только с использованием сертифицированных ФСБ России средств криптографической защиты информации.

Правила резервного копирования и восстановления информации, обрабатываемой в информационных системах, устанавливаются соответствующим регламентом.

Требования к работникам

Все пользователи информационных систем должны быть ознакомлены с организационно – распорядительными документами по обеспечению информационной безопасности в части их касающейся, знать и неукоснительно выполнять инструкции, положения, регламенты 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 обязан организовать его ознакомление с должностной инструкцией и документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных ресурсов.

Работники Учреждения, использующие технические средства аутентификации, обеспечивают сохранность идентификаторов (электронных ключей), не допускают НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность персональных идентификаторов.

Работники Учреждения должны соблюдать установленные процедуры поддержания режима безопасности при выборе и использовании паролей.

Работники Учреждения должны знать требования по безопасности информации и неукоснительно их выполнять.

Ответственность работников Учреждения

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.

Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Политика являются:

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