Приказ

О утверждении Политики информационной безопасности в ООО «Клиника Подологии»

Во исполнение требований Федерального закона "О персональных данных" от 27.07.2006 N 152-ФЗ приказываю:

1. Утвердить Политику информационной безопасности в ООО «Клиника Подологии» (приложение №1)
2. Контроль за исполнением приказа оставляю за собой

Генеральный директор Токарева Юлия Олеговна

Приложение №1

Политика информационной безопасности ООО «Клиника Подологии»

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

В Политике определены требования к персоналу Информационной системы обработки персональных данных (Далее – ИСПДН), степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн ООО «Клиника подологии».

1 Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты ООО «Клиника Подологии» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности сохранности персональных данных.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозу безопасности персональных данных.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2 Область действия

Требования настоящей Политики распространяются на всех сотрудников ООО «Клиника Подологии», подлежащих защите (штатных, временных и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3 Система защиты персональных данных

Система защиты персональных данных, строится на основании:

- Отчета о результатах проведения внутренней проверки;

- Перечня персональных данных, подлежащих защите;

- Акта классификации информационной системы персональных данных;

- Модели угроз безопасности персональных данных;

- Положения о разграничении прав доступа к обрабатываемым персональным данным;

На основании этих документов определяется необходимый уровень защищенности персональных данных.

В организации составлен список используемых технических средств защиты, а также программного обеспечения участвующего в обработке персональных данных.

Система защиты персональных данных включает в себя:

- антивирусные средства для рабочих станций пользователей и серверов.

Список функций защиты включает в себя:

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;

- обеспечение целостности данных;

- возможность производить обнаружений вторжений.

Список используемых средств поддерживается в актуальном состоянии. При изменении состава технических средств защиты, соответствующие изменения вносятся в Список и утверждаются руководителем ООО «Клиника Подологии» или лицом, ответственным за обеспечение защиты персональных данных.

Система антивирусной защиты предназначена для обеспечения антивирусной защиты серверов пользователей ООО «Клиника Подологии».

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;

- антивирусное сканирование;

- скрипт-блокирование;

- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

- автоматизированное обновление антивирусных баз;

- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

Система анализа защищенности обеспечивает выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения, которые могут быть использованы нарушителем для реализации атаки на систему. Функционал системы реализован программными и программно-аппаратными средствами.

Система обнаружения вторжений обеспечивает выявление сетевых атак на элементы информационной системы персональных данных, подключенные к сетям общего пользования и (или) международного обмена. Функционал системы реализован программными и программно-аппаратными средствами.

4 Пользователи ИСПДн

В ИСПДн в обработке и хранении ПДн участвуют:

- Администратор безопасности ИСПДн;

- Администратор ИСПДн;

- Пользователи сети;

Все сотрудники ООО, являющиеся пользователями ИСПДн, знают и строго выполняют установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.

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

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ООО «Клиника Подологии», третьим лицам.

При работе с персональными данными сотрудники ООО «Клиника Подологии» обязаны обеспечить отсутствие возможности просмотра данных третьими лицами с мониторов или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить мониторы или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники ООО «Клиника Подологии» проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение, ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности персональных данных.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

5 Обязанности оператора персональных данных

Оператор персональных данных обязан при сборе персональных данных по общему правилу использовать базы данных, находящиеся на территории РФ,

Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» (далее – Федеральный закон) и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам, в частности, относятся:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети "Интернет", с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПД, повлекшей нарушение прав субъектов ПД, оператор обязан уведомить Роскомнадзор о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПД, и предполагаемом вреде, нанесенном правам субъектов ПД, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о контактном лице - в течение суток с момента выявления такого инцидента оператором, самим Роскомнадзором или иным заинтересованным лицом, а о результатах внутреннего расследования выявленного инцидента и о лицах, действия которых стали причиной выявленного инцидента (при наличии) - в течение трех суток.

оператор обязан в порядке, определенном ФСБ, обеспечивать взаимодействие с ГосСОПКА, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПД. Поступившая от оператора информация передается органами ФСБ в Роскомнадзор в согласованном ими порядке.

6. Права субъекта персональных данных

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

Сроки и порядок ответа оператора на запрос субъекта ПД:

сведения должны быть предоставлены субъекту ПД в течение десяти рабочих дней с момента обращения (получения оператором соответствующего запроса).

Указанный срок может быть продлен не более чем на пять рабочих дней по мотивированному уведомлению, которое оператор должен направить в адрес субъекта ПД. Сведения предоставляются в той форме, в которой направлено соответствующее обращение, если в нем не указано иное.

В случае обращения субъекта ПД к оператору с требованием о прекращении обработки ПД оператор обязан по общему правилу прекратить их обработку или обеспечить прекращение такой

обработки (если за оператора действует обработчик) за исключением случаев, когда обработка возможна без согласия субъекта ПД, в течение десяти рабочих дней с даты получения требования.

Указанный срок может быть продлен не более чем на пять рабочих дней по мотивированному уведомлению, которое оператор должен направить в адрес субъекта ПД.