Политика информационной безопасности

Информационные системы персональных данных в ООО «Стоматология Здоровье»

Обозначения и сокращения

ИС – информационная система
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
ПДн – персональные данные
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
УБПДн – угрозы безопасности персональных данных

Введение

Политика информационной безопасности в ООО «Стоматология Здоровье» (Политика) основана на официальных документах Министерства здравоохранения и социального развития РФ. Строится 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», с использованием «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России от 15.02.2008 г.

Политика учитывает требования к персоналу и степень их ответственности, структуру и необходимый уровень защищенности ПДн.

Политика закрепляет статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности.

Общие положения

Безопасность объектов информатизации достигается противодействием всем видам угроз, внешним и внутренним, умышленным и непреднамеренным, минимизацией ущерба от возможной реализации УБПДн, исключением несанкционированного, в том числе случайного, доступа к объектам защиты. ПДн подлежат защите в контролируемой зоне и при передаче по каналам связи за ее границы.

Область действия

Требования Политики распространяются на всех сотрудников, а также прочих лиц, привлекаемых к исполнению работ связанных с обработкой ПДн.

Система защиты персональных данных

СЗПДн строится на основании регулярных внутренних проверок состава ПДн, соответствия уровня защиты составу ПДн, выявления угроз безопасности. Для достижения необходимого уровня безопасности выполняются плановые обучающие, административные и технические

мероприятия. В составе СЗПДн действуют следующие стандартные подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Функционал подсистем СЗПДн учитывает класс ИСПДн.

Пользователи ИСПДн

На основании проводимой Политики произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности по обработке. Каждая группа пользователей, получает доступ и информированность в соответствие с компетентностью.

Требования к персоналу по обеспечению защиты ПДн

Все сотрудники, являющиеся пользователями ИСПДн, знают и выполняют установленные правила доступа к защищаемым объектам, соблюдают режим безопасности.

При вступлении в должность нового сотрудника организовано его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн. Проводится обучение навыкам санкционированного использования ИСПДн.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами, третьим лицам. При работе с ПДн обеспечивается перекрывание просмотра ПДн третьими лицами.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн. По выявленным событиям организуется немедленное реагирование на угрозы безопасности ПДн.

Ответственность пользователей ИСПДн

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. Требования нормативных документов по защите информации отражены в должностных инструкциях сотрудников.