Что проверить в системе защиты персданных. Комплект документов для ответственного

Проведите аудит работы системы защиты персданных с инструкцией от экспертов. Штрафы за нарушения работы с персональными данными возросли до 18 млн руб. Памятки и чек-лист прилагаются.

Любовь КРИВОВА, юрист в области медицинского права, директор ООО «Медицина и право»

Мария КОРОБЕНКОВА, юрист, управляющий партнер ООО «Специализированная юридическая компания в области медицинского права "РМК"»

Татьяна ДЕГАЕВА, заместитель главного врача по поликлинической работе ГБУЗ РМ «Зубово-Полянская районная больница», к. м. н.

Персональные данные – любая информация, которая прямо или косвенно относится к определенному или определяемому физическому лицу – субъекту персональных данных (ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ).

Внутренний контроль или аудит необходимо проводить, чтобы проверить организацию обработки персональных данных на соответствие Закону № 152-ФЗ и нормативным правовым актам, требованиям к защите персданных, политике оператора в отношении обработки персданных, локальным актам оператора.

Контролеры могут проверить медорганизации на основании индикаторов риска нарушения обязательных требований. Что проконтролировать, чтобы не нарваться на внушительный штраф или привлечение к уголовной ответственности, читайте в статье.

Кого назначить ответственным за аудит

Медорганизации обязаны осуществлять регулярный внутренний контроль и аудит обработки персональных данных (порядок закрепите локальным актом).

Закон не устанавливает специальных требований к работнику, который будет заниматься обработкой.

Ответственным вы можете назначить, к примеру, сотрудника отдела кадров или специалиста информационно-технического отдела (приложение 1). Осуществлять внутренний контроль поручите сотруднику, который отвечает за организацию обработки персональных данных (ч. 2 ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ).

Утвердите приказом правила осуществления внутреннего контроля соответствия обработки персданных требованиям к защите персданных в вашей медорганизации.

Поручите ответственному выполнять периодические проверки условий обработки персональных данных.

Пропишите график плановых проверок условий обработки персональных данных в ежегодном плане внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных (плановые проверки).

Инициируйте проведение внеплановой проверки, если стало известно о нарушениях правил обработки персональных данных. Ответственный за организацию обработки персональных данных обязан организовать проверку в течение трех рабочих дней со дня поступления информации о нарушениях.

Что проверить в системе защиты персданных

Медорганизации должны разработать систему защиты персональных данных (приказ Минздрава от 24.12.2018 № 911н, приказ ФСТЭК от 11.02.2013 № 17, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

При утечке информации о персональных данных или несанкционированном доступе к материальным носите-

лям персональных данных (при неавтоматизированной обработке) посторонних лиц медорганизацию могут оштрафовать до 100 тыс. руб.

Поручите ответственному за аудит проверить, соответствуют ли меры защиты персональных данных требованиям нормативных актов, в частности постановления Правительства от 15.09.2008 № 687. В помощь выдайте памятки (приложения 2, 3). Для контроля системы используйте чек-лист (приложение 4).

Как оформить результаты контроля

Поручите ответственному за аудит составить отчет о результатах внутреннего контроля в произвольной форме или используйте образец (приложение 5).