Полиграф – это комплексная компьютерная аппаратная методика измерения уровня психологического стресса у человека, позволяющая выявить скрываемую информацию. Слово «полиграф» дословно означает «много писаний» (греч. «poly» – много, «graphos» – писание), указывая на его способность одновременно записывать несколько физиологических функций организма, таких как дыхание, проводимость кожи, частота пульса, кровяное давление и др. Записанные показания являются специфическими физиологическими изменениями, происходящими в организме обследуемого, когда ему задают вопросы, касающиеся области расследования. Данные изменения носят характер кратковременного импульса, однако полиграф, снабженный рядом чувствительных датчиков, улавливает и фиксирует каждый из них. Эти записи (полиграммы), зафиксированные в виде нескольких кривых на экране компьютера, затем обрабатываются полиграфологом, который делает вывод о правдивости ответов обследуемого лица.

Процедура проведения опроса с использованием полиграфа документируется. Документами, сопровождающими обследование, являются заявление обследуемого о согласии на проведение опроса с использованием полиграфа; вопросы, заданные опрашиваемому лицу в ходе тестирования на полиграфе; полиграмма, отражающая зарегистрированные в ходе опроса физиологические реакции; аудио- и (или) видеозаписи, полученные при проведении предтестовой беседы, тестирования на полиграфе и (или) послетестовой беседы. Результатом проведения обследования является письменное заключение полиграфолога, которое представляется инициатору обследования.

Документы, фиксирующие ход и результат проведенного обследования, как электронные, так и бумажные, аудио- и видеозаписи являются конфиденциальными и подлежат соответствующему обращению с ними.

Каменко С. Н., КГЭУ

## ДОКУМЕНТИРОВАНИЕ ПРОЦЕДУРЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

Сегодня нельзя представить деятельность организации без обработки информации о человеке. Организация хранит и обрабатывает данные о сотрудниках, клиентах, партнерах, поставщиках и других физических лицах, с которыми ей приходится сталкиваться. Утечка, потеря или несанкционированное изменение персональных данных приводит к очень серьезному ущербу, а иногда и к полной остановке деятельности организации.

В соответствии с Федеральным законом от 27 июля 2006 г. № 152–ФЗ «О персональных данных» под информационной системой персональных данных

понимается «информационная система, представляющая собой совокупность персональных данных, содержащихся в автоматизированной базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных».

Обеспечения безопасности персональных данных в наше время является всеобщей необходимостью. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Информация в руках мошенника превращается в орудие преступления, в руках уволенного сотрудника – в средство мщения, в руках инсайдера – товар для продажи конкуренту. Именно поэтому персональные данные нуждаются в самой серьезной защите.

Необходимость принятия мер по защите персональных данных (далее – ПДн) вызвана также возросшими техническими возможностями по копированию и распространению информации. Уровень информационных технологий достиг того предела, когда самозащита информационных прав уже не является эффективным средством против посягательств на частную жизнь. Современный человек уже физически не способен скрыться от всего многообразия различных применяемых в отношении него технических устройств сбора и технологий обработки данных.

С развитием средств массовых коммуникаций возросли также и злоупотребления, связанные с использованием собранной и накопленной информации о человеке. Появились и эффективно используются злоумышленниками средства внедрения и быстрой обработки персональных данных, которые создают угрозу правам и интересам человека. Без контроля персональных данных во времени и пространстве, можно нанести значительный ущерб человеку.

В каждой организации накапливаются, формируются, обрабатываются, хранятся и используются большие объемы данных обо всех категориях сотрудников. Эти сведения относятся к так называемым персональным данным, которые отражают личную или семейную тайну граждан, их частную жизнь и входят в круг информации, подлежащей защите от несанкционированного доступа.

Понимая важность и ценность информации о человеке, а также заботясь о соблюдении прав своих граждан, государство требует от организаций и физических лиц обеспечить надежную защиту персональных данных. Законодательство Российской Федерации в области ПДн основывается на Конституции РФ и международных договорах Российской Федерации и состоит из Федерального закона РФ от 27 июля 2006 г. № 152–ФЗ «О персональных данных» и других федеральных законов, определяющих случаи и особенности обработки персональных данных, нормативных актов, инструкций и требований.

Актуальность выбранной темы заключается в том, что все сведения, использующиеся в организации при неправильном использовании, могут стать

орудием в руках правонарушителя и поэтому их необходимо защищать. Для этого проводиться определенный комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному на основании такой информации физическому лицу.

Разработка пакета внутренних документов, регламентирующих вопросы защиты персональных данных, является основной и первоочередной организационной мерой при внедрении комплексной системы защиты персональных данных. В ходе работ создаются общие организационно-распорядительные документы (положения, приказы, инструкции, планы, перечни, формы уведомлений) и индивидуальные для каждой информационной системы персональных данных документы (модели угроз, описания, акты, технические задания и т. п.).

Для обеспечения безопасности ПДн в ИС ПДн в организации могут использоваться следующие методы и способы защиты:

– реализуется система допуска пользователей к информационным ресурсам;

– ограничен доступ пользователей в помещения, где размещены технические средства, а также, хранятся носители информации;

– осуществляется разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– осуществляется учет и хранение съемных носителей информации, и контроль за их обращением;

– регулярно проводится резервное копирование и восстановление работоспособности технических средств, программного обеспечения, базы данных и носителей информации;

– организуется защита помещений и технических средств;

– осуществляется предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов).

Тухватуллина Р. М., КГЭУ

## ДОКУМЕНТИРОВАНИЕ ПРОЦЕДУРЫ ЗАЧИСЛЕНИЯ ДЕТЕЙ В ЛОГОПЕДИЧЕСКУЮ ГРУППУ (НА ПРИМЕРЕ ДОШКОЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ РЕСПУБЛИКИ ТАТАРСТАН)

Изучение состава документов, сопровождающих коррекционный процесс речевых нарушений у детей в рамках интенсивного развития и совершенствования дифференцированной системы специальных дошкольных учреждений, является актуальным и малоизученным. Современные дошкольные образовательные учрежде-