4. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КОГНИТИВНЫЕ ТЕХНОЛОГИИ В ИНФОРМАТИЗАЦИИ

УДК 349; 004.8

ЗАЩИТА И ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

М. С. Абламейко[1], Р. П. Богуш[2]
[1]Белорусский государственный университет, Минск
[2]Полоцкий государственный университет, Новополоцк, Беларусь

Рассмотрены вопросы по защите персональных данных в системах искусственного интеллекта. Для обучения таких систем очень важен вопрос обезличивания персональных данных. Даны конкретные предложения по технической и правовой организации данных процессов в Беларуси.

Введение

В последние годы все больше расширяется использование систем искусственного интеллекта (ИИ) во многих сферах человеческой деятельности, таких как медицинская диагностика, обеспечение общественной безопасности и др. [1]. Успех ИИ обусловлен прорывами в аппаратных средствах и методах машинного обучения, в частности успехами в разработке глубокого обучения нейронных сетей. Для возможности их практического применения требуются чрезвычайно большие наборы данных на этапе тренировки нейросетевых структур, поэтому невозможно переоценить значимость создания размеченных данных для различных прикладных задач. Это обусловлено тем, что все системы ИИ имеют схожий принцип: первоначально используемая модель обучается на огромной выборке и только после этого систему можно использовать для полноценной работы. Отметим, что очень важно обучить систему именно на реальных данных.

Очевидно, что, работая с человеком, ИИ должен обучаться, используя данные о людях, и может владеть многими персональными данными (ПД) человека (личными, медицинскими и др.). Вместе с тем на правовом уровне многие государства принимают меры по защите ПД, в частности, в большинстве случаев применяется принцип согласия владельца. При использовании ПД для обучения систем ИИ такие данные должны быть обезличены.

Обезличивание ПД предполагает удаление части или полную их замену специальными идентификаторами. Цель таких действий заключается в обеспечении невозможности определения принадлежности данной информации конкретному человеку, что позволяет использовать ПД, не нарушая законодательства. Во многих странах применение обезличенных данных возможно без согласия субъектов.

Для развития и использования систем ИИ необходимо содействовать исследованию юридических и технических проблем, связанных с предоставлением ПД, и предложить сбалансированные решения, как способствующие распространению новых технологий, так и обеспечивающие их надежность и безопасность. Выгодное с экономической точки зрения вовлечение технологий ИИ в общественные процессы не должно привести к ущемлению интересов граждан и обрушению морально-нравственных норм, сформированных человечеством [2]. В докладе даны предложения с технической и правовой точек зрения по организации данных процессов в Республике Беларусь.

1. Защита персональных данных

Во многих странах мира в последнее время значительное внимание уделяется вопросам защиты ПД в связи с повсеместным использованием систем ИИ. Остро стоит вопрос защиты неприкосновенности частной жизни, так как частичная или полная идентификация может нанести ущерб человеку. При этом следует учитывать, что право человека на невмешательство в его личную и семейную жизнь отнесено к числу основополагающих.

Запрет на такое вмешательство, а также право на защиту от него были закреплены уже в ст. 12 Всемирной декларации прав человека в 1948 г. Международный пакт о гражданских и политических правах (1966 г.) закрепил принцип невмешательства в частную жизнь.

Первым международным договором, заложившим правовые основы регулирования ПД в общественном и частном секторе, а также принципы защиты физических лиц от незаконного обращения с их данными, имеющим обязательную силу, является Конвенция Совета Европы № 108 «О защите частных лиц в отношении автоматизированной обработки данных личного характера» (Конвенция № 108), подписанная 28 января 1981 г. На сегодняшний день она насчитывает 55 стран-участников на четырех континентах, еще 20 государств принимают участие в ее работе. Во многих государствах она стала базой соответствующего национального законодательства, в том числе послужила основой для первой директивы Европейского союза по защите данных, принятой в 1995 г. [3].

В ЕС вопросам защиты неприкосновенности частной жизни и ПД уделяется большое внимание. 27 апреля 2016 г. был принят Регламент Европейского Парламента и Совета ЕС 2016/679 о защите физических лиц при обработке ПД и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите ПД – General Data Protection Regulation, GDPR) [4]. Два года были даны государствам на осуществление необходимых мер по его реализации, 25 мая 2018 г. он вступил в силу.

Регламент GDPR содержит широкое определение ПД, в которое включены практически все данные о лице, в том числе генетические, биометрические, о состоянии здоровья и др. Установлено, что обработка данных является законной не только при получении на то прямого согласия субъекта данных, но и в ряде других случаев.

Анализ опыта зарубежных стран показывает, что защите персональных данных уделяется большое внимание со стороны как государства, так и частного сектора. Правовые рамки в данной сфере становятся все более жесткими в связи с тем, что развитие информационных технологий позволяет получать о человеке большое количество информации, а системы ИИ способны ее генерировать и использовать для полной идентификации человека, что может применяться в противоправных целях.

2. Обезличивание персональных данных

Обезличенные данные на сегодняшний день используются в широком спектре областей – от маркетингового анализа до медицинских исследований. Поскольку они не содержат личной информации, их можно безопасно использовать для анализа трендов, паттернов и других массовых явлений, не нарушая прав на конфиденциальность пользователей. Наконец, обезличенные ПД играют важную роль в обучении ИИ, например прогностических, которые предсказывают потребительское поведение пользователей.

Таким образом, использование данных является необходимостью как со стороны государственного, так и частного секторов. Необходимо искать баланс интересов государства в части развития технологий, в частности ИИ, и интересов личности с точки зрения недопущения злоупотребления вмешательства в свою жизнь.

В ст. 1 Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» обезличивание ПД определяется как действия, в результате которых становится невозможным определить принадлежность ПД конкретному субъекту без использования дополнительной информации. При обезличивании ПД можно использовать в научных и исследовательских целях без согласия субъекта на обработку [5].

На сегодняшний день Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» в Приложении 5 к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, определено пять методов обезличивания ПД:

1) Метод введения идентификаторов – замена ПД или их части, позволяющих идентифицировать субъекта, их идентификаторами и создание таблицы соответствия с последующим раздельным хранением. В результате создается таблица, где обозначены коды и их расшифровка. Такой метод при наличии соответствующего доступа позволяет восстановить изначальный объем и содержание ПД.

2) Метод изменения состава – обобщение, изменение или удаление части сведений, позволяющих идентифицировать субъект, с последующим раздельным хранением полученных данных и правил изменения. В этом случае производится удаление части информации, не имеющей пользы, ее замена на анонимизированные данные или обобщение.

3) Метод декомпозиции – разбиение множества записей ПД на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением подмножеств и таблиц. Суть метода заключается в том, что, имея доступ лишь к части информации, невозможно понять, какому именно субъекту она принадлежит.

4) Метод перестановки – взаимное перемешивание отдельных записей, а также групп записей между собой с последующим раздельным хранением полученных данных и правил изменения. Перемешивание осуществляется до того момента, когда становится невозможным определить, о чьих именно данных идет речь.

5) Метод зашифрования – применение средств криптографической защиты информации (предварительного шифрования), имеющих сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой ОАЦ.

Процедура обезличивания ПД также регулируется отдельными законодательными актами в различных сферах. Особое внимание уделяется автоматизированным государственным информационным системам, содержащим ПД физических лиц, так как в них накапливаются данные на протяжении жизни человека и защита их гарантируется государством.

В соответствии со ст. 30 Закона Республики Беларусь от 21.07.2008 № 418-З «О регистре населения» «обезличивание персональных данных, содержащихся в регистре, может производиться в научных или иных исследовательских целях путем исключения из ПД идентификационного номера, Ф.И.О., его родителей, опекунов, попечителей, супруга (супруги), ребенка (детей), цифрового фотопортрета». Кроме того,

могут быть исключены и другие ПД или их составляющие в порядке, установленном владельцем регистра. Процедура обезличивания определена постановлением Министерства внутренних дел Республики Беларусь от 27.09.2012 № 341 «Об установлении порядка обезличивания ПД, содержащихся в регистре населения» и осуществляется путем присвоения ПД конкретных физических лиц уникальных последовательных номеров за исключением ПД, указанных в ст. 30 Закона «О регистре населения», а также номера дома, корпуса и квартиры места жительства и (или) места пребывания; учетного номера плательщика; данных об исполнении воинской обязанности; данных о серии и номере документов, подтверждающих основные и дополнительные ПД.

Законом Республики Беларусь от 30.06.2022 № 183-З «О правах инвалидов и их социальной интеграции» наряду со сбором, хранением и использованием предусмотрено обезличивание ПД без согласия инвалидов и их представителей для целей ведения базы данных социальной поддержки и реабилитации инвалидов.

В медицинской сфере Законом Республики Беларусь от 18.06.1993 № 2435-XII «О здравоохранении» также предусмотрена процедура обезличивания ПД лиц, которым оказывается медицинская помощь в рамках эксплуатации централизованной информационной системы здравоохранения. В постановлении Министерства здравоохранения Республики Беларусь от 28.05.2021 № 64 «Об утверждении Инструкции о порядке обезличивания ПД лиц, которым оказывается медицинская помощь» обезличивание ПД определено как действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПД конкретному субъекту ПД.

Обезличиванию подлежат: Ф.И.О., данные о серии и номере документов, подтверждающих основные и дополнительные ПД; идентификационный номер; номера дома, корпуса и квартиры места жительства (места пребывания); фотоизображение (цифровой фотопортрет); данные о роде деятельности; информация о результатах патологоанатомического вскрытия для установления причины смерти. Инструкцией предусмотрено обезличивание данных путем введения идентификаторов, замены состава или декомпозиции, осуществляемых оператором. Следует отметить, что данное регулирование касается эксплуатации централизованной информационной системы здравоохранения.

Таким образом, в настоящее время процедура обезличивания ПД предусмотрена как на уровне основного закона, регулирующего оборот ПД, – Закона «О защите персональных данных», так и отраслевых законодательных актов. В связи с тем что развитие технологий ИИ и робототехники является приоритетным направлением научной, научно-технической и инновационной деятельности на 2021–2025 годы, в рамках Указа Президента Республики Беларусь от 07.05.2020 № 156 требуется совершенствование законодательства.

Одной из основных проблем развития технологий ИИ является проблема получения доступа к данным. В настоящее время процедура обезличивания ПД без согласия субъекта возможна только в научных или исследовательских целях. Вместе с тем разработчиками систем ИИ чаще являются коммерческие организации и ими преследуются иные цели. Безусловно, процедура обезличивания данных в первую очередь должна рассматриваться как механизм защиты прав граждан, а уже во вторую – как стимулирование развития технологий. С технической точки зрения большинство используемых методов не способны обезличить данные с сохранением их ценности. Применяемые методы нацелены на минимизацию рисков идентификации, однако при математической обработке данные могут быть персонализированы. Для эффективного регулирования

данной сферы следует принять стандарты, которые были бы доступны и понятны всем участникам рынка.

Считаем целесообразным дополнить действующий Закон ««О защите персональных данных» главой, посвященной теме обезличивания ПД, в которой необходимо предусмотреть следующие аспекты:

– согласие на обезличивание ПД субъекта ПД;

– определение перечня данных, подлежащих обезличиванию в обязательном порядке;

– определение методов, подлежащих применению;

– установление обязанностей оператора и др.

Очевидно, что должны быть разработаны программно-технические средства, позволяющие переводить ПД конкретного человека в разряд обезличенных.

Другим важным аспектом является организационное управление обезличенных ПД. В России, например, планируется создание Центра обезличивания данных для подготовки ИИ в составе Минцифры [5].

По мнению авторов, в Беларуси данный процесс может регулироваться Национальным центром защиты персональных данных, которым должны быть разработаны общие рекомендации по обезличиванию ПД. Затем каждое ведомство и организация, которая работает с ПД, должна разработать свои правила работы по выполнению данной процедуры. Процесс обезличивания должен завершаться распоряжением по организации. После того как ПД будут обезличены выбранным методом, нужно составить акт с перечислением типов обработанных данных.

Заключение

Для применения методов обезличивания ПД необходимо внести дополнения в действующее законодательство, дополнив Закон «О защите персональных данных» соответствующей главой. Особое внимание следует уделить созданию нормативно-технических документов, регламентирующих применение и требования к программно-аппаратным средствам при обезличивании ПД. Еще одним важным шагом является разработка методических документов Национальным центром защиты персональных данных, регламентирующих процессы обезличивания данных.

Комплексный и системный подход разработки и создания правовой базы в данной сфере позволит повысить уровень защиты ПД и будет способствовать более широкому использованию систем ИИ для развития личности и государства в целом.

Список литературы

1. Абламейко, М. С. Использование систем искусственного интеллекта при обеспечении общественной безопасности в «умном городе»: юридические аспекты / М. С. Абламейко, Н. В. Шакель, Р. П. Богуш // Вестник Полоцкого гос. ун-та. Серия D. Экономические и юридические науки. – 2021. – № 5. – С. 84–92.

2. Русакович, А. С. Визуальные персональные данные и их защита / А. С. Русакович, М. С. Абламейко // Право и цифровые технологии : сб. ст. Междунар. науч.-практ. конф., Новополоцк, 26 ноября 2021 г. ; редкол.: И. В. Шахновская, П. В. Соловьев. – Новополоцк : Полоцкий гос. ун-т им. Е. Полоцкой, 2022. – С. 125–132.

3. Овчинский, В. С. Под прицелом видеокамер и Big Data / В. С. Овчинский, Ю. Н. Жданов // Защита и безопасность. – 2021. – № 2(97). – С. 38–41.

4. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. COM/2021/206 final [Electronic resource]. – Mode of access: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206. – Date of access: 13.08.2023.

5. Булгаков, Д. Другим именем: в России создадут центр обезличивания данных для подготовки ИИ. Новое подразделение в составе Минцифры может появиться в 2024 г. [Электронный ресурс] / Д. Булгаков. – Режим доступа: https://iz.ru/1536931/dmitrii-bulgakov/drugim-imenem-v-rossii-sozdadut-tcentr-obezlichivaniia-dannykh-dlia-podgotovki-ii. – Дата доступа: 12.08.2023.