ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, доцента Баранковой Инны Ильиничны на диссертационную работу Мищенко Евгения Юрьевича на тему «Моделирование процессов обезличивания персональных данных и оценка эффективности используемых методов на основе модели нарушителя», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Обезличивание персональных данных (ПД) является методом обработки, при котором без дополнительной информации невозможно определить принадлежность ПД физическому лицу при обработке и передаче ПД в незащищенной среде. Существующие методы обезличивания, основанные на искажении или на разделении данных, требуют разработки методик для выбора обезличиваемых атрибутов физического лица и оценки их эффективности.

Обоснование выбора обезличиваемых атрибутов и оценки эффективности процесса обезличивания является актуальной задачей. Для реализации методов обезличивания, основанных на разделении данных, актуальным также является обеспечение безопасной передачи информации по незащищенным каналам.

Научная новизна полученных результатов

В диссертационной работе автором получены и научно обоснованы следующие результаты, обладающие новизной:

1. Разработана математическая модель идентификации ФЛ, отличающаяся применением количественных оценок вероятности идентификации по атрибуту в целом, и сформулирован критерий необходимости обезличивания ПД по любым идентификаторам или их совокупности.

2. Разработана функциональная модель нарушителя, реализующая итерационный алгоритм деобезличивания ПД для методов обезличивания, основанных на искажении ПД, отличающаяся применением количественных оценок эффективности методов обезличивания.

3. Разработана функциональная схема передачи информации между базами ПД, разделенными методом введения идентификаторов, отличающаяся применением внешнего бумажного носителя идентификационной информации и

реализующая безопасную передачу информации между таблицей идентификаторов и обезличенными ПД.

Обоснованность и достоверность научных положений, сформулированных в диссертации

Обоснованность и достоверность научных результатов исследования заключается в корректной постановке цели и задач исследования, выборе адекватного поставленным задачам математического аппарата, обширной экспериментальной базе.

Результаты исследования опубликованы в 13 научных работах, 6 из которых – в ведущих рецензируемых журналах, рекомендованных ВАК РФ и Аттестационным советом УрФУ. Получен 1 патент на полезную модель.

Практическая значимость результатов диссертации

Практическая значимость заключается в:

– возможности применения критерия необходимости обезличивания ПД для обоснования выбора обезличиваемых атрибутов ФЛ и их сочетаний;

– обосновании значения возможного показателя вероятности идентификации ФЛ по атрибуту при разработке нормативной базы параметров обезличивания ПД;

– возможности применения функциональной схемы передачи информации между частями базы ПД, разделенными методом введения идентификаторов, при построении системы защиты ИСПДн.

Полученные результаты внедрены в системе льготного лекарственного обеспечения АО «Областной аптечный склад» (Челябинск, Россия).

Оценка содержания диссертации и её оформления

Диссертационная работа содержит 141 страницу основного текста (всего 165 с.), 58 рисунков (без приложений) и 22 таблицы (без приложений). Состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, списка литературы из 93 наименований, 4 приложений.

В первой главе приведен анализ состояния разработанности области исследования, как в отечественных, так и в зарубежных нормативных документах, а также подробно рассмотрены варианты внедрения методов обезличивания ПД. Сделан акцент на общих проблемах реализации различных методов обезличивания,

связанных с отсутствием методик выбора атрибутов для обезличивания, а также методик количественной оценки эффективности применяемых методов. С целью поиска закономерностей влияния характеристик атрибутов на выбор их в качестве обезличиваемых автор анализирует использование этих характеристик в различных сферах деятельности, например в демографии и медицине. На основе анализа предметной области автор обосновывает актуальность темы исследования, формулирует цель и осуществляет постановку задачи исследования.

Во второй главе сформулирован критерий необходимости обезличивания ПД физического лица по заданному атрибуту, в основу которого положено сравнение вероятности идентификации физического лица и компетенции нарушителя. Разработана модель идентификации физического лица, учитывающая диапазон значений и семантику атрибутов и их сочетаний, а также объем базы ПД. Для подтверждения достоверности полученных результатов использовались две БД большого объема, включающие атрибуты, имеющие различную семантику и диапазон значений. Критерий необходимости обезличивания был определен для всех чувствительных атрибутов и некоторых их сочетаний. Были аппроксимированы эмпирические зависимости вероятности идентификации от количества записей базы ПД, доказана гипотеза о степенном характере этих зависимостей, что позволило определить минимальное количество записей базы данных, при котором обезличивание по заданному атрибуту становится необходимым.

В третьей главе предложена методика оценки эффективности обезличивания для методов изменения состава или семантики и перемешивания, основанных на искажении ПД. Компетенция нарушителя учтена в разработанной модели нарушителя в виде двух параметров, одним из которых является количество записей физических лиц в обезличенной базе, ПД которых достоверно известны нарушителю. Вторым параметром является максимальное количество записей, полученных нарушителем в результате деобезличивания, которое нарушитель считает эффективным для дальнейшей обработки. Предполагается, что эти два параметра будут задаваться регулятором в качестве нормативов. Автор предлагает четыре алгоритма деобезличивания, основанные на перемещении элементов (символов и битов) в пределах заданной области. и делает обобщенные выводы об эффективности рассмотренных алгоритмов обезличивания.

В четвертой главе рассмотрена усовершенствованная функциональная схема передачи информации между разделенными частями базы ПД для метода введения идентификаторов. Особенностью представленной схемы является использование внешнего бумажного носителя, являющегося стандартным элементом технологии в сфере здравоохранения. Данная особенность позволила облегчить процесс внедрения функциональной схемы в этой сфере.

Замечания и вопросы по работе

Вместе с этим следует отметить некоторые замечания и вопросы по содержанию диссертации:

1. Модель нарушителя ограничена базовыми возможностями по реализации угроз безопасности информации (Н1) с.32 п.9 «нарушитель не может разрабатывать специальное программное обеспечение для вскрытия алгоритма искажений, но может пользоваться готовыми программными средствами», с.122 диссертации «Так как в ручном режиме произвести такой объем вычислений практически невозможно…»
2. Список литературы содержит только 30 % работ, изданных за последние 5 лет, и 25% ссылок на литературу, изданную более 10 лет назад.
3. При оценке эффективности алгоритмов обезличивания (стр. 28 диссертации) используется термин «условное деобезличивание», указывается связь этого термина с параметрами модели нарушителя. В чем эта связь заключается?
4. В описанном на стр. 102-103 диссертации алгоритме действий нарушителя в процессе деобезличивания базы данных вводится ограничение на количество полученных записей, равное 20. Как это значение связано с параметром возможностей нарушителя $U = 20$ записей, содержащих ПД не известного (искомого) физического лица?
5. На стр. 38 диссертации говорится о влиянии на параметр возможностей нарушителя U внешних условий, одно из которых – время поиска, при этом применяется понятие «приемлемое время», под которым понимается максимальное время, которое нарушитель готов затратить на дальнейшую обработку полученной группы записей. Как определяется это время?

Сделанные замечания имеют дискуссионный характер и не снижают научной ценности работы.

Заключение по работе

Исследовательская работа изложена грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости, личному вкладу автора, отражению результатов в публикациях, а также полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ и специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Автор диссертации Мищенко Евгений Юрьевич заслуживает присуждения ему учёной степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

Доктор технических наук, доцент

Заведующая кафедрой информатики и информационной безопасности

ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова»

Адрес: 455000, г. Магнитогорск, пр. Ленина, д.38, УК 1, ауд. 368

Тел.: +7 (3519) 23-27-51

e-mail: inna_barankova@mail.ru

_____ Баранкова Инна Ильинична

(подпись) (дата) 02.02.2023г

Подпись Баранковой И.И. заверяю _____

(подпись) (дата)

ПОДПИСЬ ЗАВЕРЯЮ
Начальник отдела делопроизводства
ФГБОУ ВО «МГТУ им. Г.И. Носова»
Д.Г. Семенова