ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора Захарова Александра Анатольевича 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

После выхода закона о персональных данных (ПД) происходит активное внедрение системы защиты персональной информации в государственных органах и коммерческих организациях, совершенствуются методы и, соответственно, способы защиты персональных данных физических лиц с целью сохранения их конфиденциального характера. Особенно остро вопрос информационной безопасности встает перед медицинскими учреждениями, которые собирают и хранят ПД, крайне чувствительные для пациента, – результаты лабораторных и инструментальных исследований, диагнозы, истории болезней. Известно четыре основных технологии защиты персональных данных в информационных системах: физические, аппаратные, программные, и организационные. Целью диссертационной работы является разработка моделей процесса обезличивания ПД и оценка эффективности реализации методов обезличивания. Автор предлагает оригинальный программный метод обезличивания с обоснованием невозможности определения принадлежности ПД конкретному физическому лицу, что позволяет безопасно передавать и обрабатывать обезличенные данные в незащищенной среде. Отметим, что, например, для ввода дополнительных данных необходимо осуществить обратное преобразование (деобезличивание), что невозможно сделать без дополнительной информации. Дополнительная информация, необходимая для деобезличивания, может содержаться как в составе обезличенных ПД, так и отдельно от них в зависимости от метода обезличивания.

В первом случае необходимо оценить уязвимость, возникающую при хранении дополнительной информации, которая зависит и от сложности алгоритма обезличивания, и от возможностей нарушителя по ее восстановлению (деобезличиванию). Методика оценки указанной уязвимости основывается на модели нарушителя и оценки возможности использования алгоритмов деобезличивания.

Во втором случае необходимо нейтрализовать уязвимость, возникающую при передаче дополнительной информации от базы идентификаторов к обезличенной базе. Способ нейтрализации указанной уязвимости обязан учитывать особенности

технологического процесса обработки ПД, не ограничивая его функциональности и производительности, то есть должен быть ориентирован на практическую реализацию.

Кроме того, в обоих случаях уязвимость обезличенных ПД в целом зависит от обоснованного выбора группы идентификаторов для обезличивания. Для обоснования такого выбора необходимо использовать количественные характеристики атрибутов. Методика выбора обезличиваемых атрибутов должна обеспечивать невозможность деобезличивания ПД.

Научная новизна полученных результатов

В соответствии с актуальными задачами исследования в диссертационной работе получены следующие, обладающие новизной научные результаты:

1. Построена математическая модель идентификации ФЛ, отличающаяся применением количественных оценок вероятности идентификации по атрибуту в целом, а также определен и обоснован критерий необходимости обезличивания ПД по любым идентификаторам или их совокупности при любом количестве записей БД.

2. Разработана функциональная модель нарушителя, который реализует итерационный алгоритм деобезличивания ПД для методов обезличивания, основанных на искажении ПД.

3. Для реализации безопасной передачи информации между таблицей идентификаторов и обезличенными ПД разработана функциональная схема передачи информации между базами ПД, основанная на методе введения идентификаторов и использующая внешний носитель идентификационной информации

Обоснованность и достоверность научных положений диссертации

Обоснованность и достоверность научных результатов исследования заключается в следующем:

1) цели и задачи исследования поставлены корректно и в соответствии с проблемой исследования;

2) общая методология исследования и используемые математические методы в частности релевантны поставленным задачам;

3) экспериментальная база достаточно представительна для достоверности опирающихся на нее результатов.

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

1) сформулирован и обоснован критерий необходимости обезличивания по атрибутам физического для базы любого объема, что повышает результативность процедур обезличивания ПД;

2) обоснована необходимость использования показателя вероятности идентификации ФЛ по атрибуту при разработке нормативной базы параметров обезличивания ПД, что способствует корректному выбору параметров;

3) разработана функциональная схема передачи информации между частями базы ПД, разделенными методом введения идентификаторов, реализованная для ИСПДн в системе льготного лекарственного обеспечения.

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 проводится подробный анализ состояния разработанности темы исследования. Делается акцент на процедуре выбора атрибутов физического лица для обезличивания ПД, способах реализации методов обезличивания в России и за рубежом, а также при оценке эффективности реализации методов обезличивания ПД. Проведенный анализ позволяет сделать выводы о недостаточной обоснованности выбора обезличиваемых атрибутов и отсутствии методик количественной оценки эффективности процедуры обезличивания. По вопросу реализации алгоритмов обезличивания отмечается наличие уязвимости защищаемой дополнительной информации на этапах ввода и вывода ПД. **Сделанные выводы позволяют сформулировать цель и определить задачи исследования.**

Во второй главе формулируется критерий необходимости обезличивания ПД. С одной стороны, для этого вводится показатель вероятности идентификации физического лица по заданному атрибуту, как количественной характеристики объекта процесса обезличивания, зависящей от его семантики и объема базы обезличиваемых данных. С другой стороны, вводится показатель компетенции нарушителя, как количественной характеристики субъекта процесса обезличивания, отражающей эффективность деобезличивания. Сравнение этих характеристик позволяет сделать вывод о необходимости обезличивания рассматриваемого атрибута для базы ПД заданного объема. На основе показателя вероятности идентификации по атрибуту построена модель идентификации физического лица, применимая для любых атрибутов и их сочетаний. На

основе показателя компетенции нарушителя построены алгоритмы действий нарушителя безопасности ПД. Достоверность полученных результатов подтверждена большим объемом и различной структурой экспериментальных баз ПД. Автором исследована зависимость вероятности идентификации от объема базы ПД, построены эмпирические зависимости для различных атрибутов. С помощью критериев согласия первого и второго рода был доказан степенной вид этих зависимостей, что позволило экстраполировать их поведение для количества записей базы, значительно превышающего значения в экспериментальных базах.

В третьей главе предлагается методика оценки эффективности методов обезличивания, искажающих атрибуты-идентификаторы: метода изменения состава или семантики (искажения внутри строки идентификаторов) и метода перемешивания (изменение положения элементов внутри группы строк). Задаются значения двух параметров модели нарушителя (компетенция нарушителя): количество записей физических лиц в обезличенной базе, ПД которых известны нарушителю, и количество записей, полученных нарушителем в результате деобезличивания, которое нарушитель считает максимально возможным для дальнейшей обработки (организационными мерами). Автор рассматривает четыре алгоритма обезличивания ПД и предлагает соответствующие им алгоритмы действий нарушителя (деобезличивания), имеющие циклический характер, и использует количество циклов деобезличивания для оценки эффективности примененных алгоритмов обезличивания ПД.

В четвертой главе рассматривается усовершенствованная функциональная схема для метода введения идентификаторов, обеспечивающая безопасную передачу информации между защищенной таблицей идентификаторов и незащищенной частью базы ПД. В качестве хранилища идентификатора связи используется внешний бумажный носитель, являющийся стандартным элементом технологии (рецепт на выдачу лекарств). Рассмотренная функциональная схема внедрена в сфере здравоохранения.

Замечания и вопросы по работе

При изучении автореферата и диссертации возникли следующие замечания и вопросы к их содержанию:

1. Из текста о портрете предполагаемого нарушителя (пункты 1-9 стр. 32)) трудно определить его участие в процессах создания или обработки записей (медицинский работник?) или передачи базы данных из медучреждения в ЕГИСЗ (сотрудник – сетевой администратор?). Поэтому остается неясным, сколько нарушителей с такими правами и 9-ю необходимыми компетенциями может реально существовать и что их может мотивировать на незаконные действия.

2. Во втором абзаце на стр. 35 диссертации ссылка на формулу (5) некорректна. По контексту это должна быть ссылка на формулу (4).

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, профессор
Профессор Учебно-научного центра «Информационная безопасность»
Института радиоэлектроники и информационных технологий ФГАОУ ВО
«Уральский федеральный университет им. первого Президента России Б.Н. Ельцина»

620002, г. Екатеринбург,
ул. Мира, 19
Телефон: +7 (343) 375-95-57
Адрес электронной почты: aazaharov@yandex.ru

06.02.2023 Захаров Александр Анатольевич

(подпись) (дата)

Подпись д.т.н., доцента
Захарова А.А. заверяю _____

ДОКУМЕНТОВЕД УДиОВ
ГАФУРОВА А. А.
06.02.2023

(подпись) (дата)