УДК *004.056:336.71(076)*

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ МЕТОДА ИЗМЕНЕНИЯ СОСТАВА

А.М. Тимофеев[1], Д.В. Шляхтун[2], Ли Чэнтинъюй[1], Хуан Цзыхань[1]

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

[2]*Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь*

Аннотация. Разработана процедура обезличивания персональных данных, основанная на базе метода изменения состава. Данная процедура позволяет обезличивать

персональные данные буквенного и числового типов, не требует использования больших вычислительных ресурсов для оборудования легитимных пользователей и обеспечивает достаточно высокий уровень информационной безопасности за счет изменения статистических свойств полученных обезличенных персональных данных, в сравнении с исходными персональными данными.
Ключевые слова: информационные системы; персональные данные; защита информации; обезличивание персональных данных; методы обезличивания персональных данных; метод изменения состава.

DEPERSONALIZATION OF PERSONAL DATA BASED ON THE METHOD OF CHANGING THE COMPOSITION

A.M. Timofeev [1], D.V. Shliakhtun[2], Chengtingyu Li[1], Huang Zihan[1]
[1]*Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus*
[2] *Educational Institution "National Children's Technopark", Minsk, Republic of Belarus*

Abstract. The procedure for depersonalization of personal data, based on the composition change method, was developed. This procedure allows for the depersonalization of personal data of the letter and numeric types, does not require the use of large computing resources for the equipment of legitimate users and ensures a sufficiently high level of information security by changing the statistical properties of the received depersonalized personal data in comparison with the original personal data.
Keywords: information systems; personal data; information protection; depersonalization of personal data; methods of depersonalization of personal data; method of changing the composition.

Введение

В настоящее время в большинстве существующих информационных систем обрабатываются персональные данные [1–3]. Под персональными данными будем понимать любую информацию о физическом лице, посредством которой физическое лицо либо идентифицировано, либо может быть идентифицировано.

К числу персональных данных относят, например, физиологические и биологические особенности человека, наследуемые и приобретенные генетические характеристики, а также информацию, касающуюся его национальной, расовой принадлежности, членства в профессиональных союзах и прочие [1–3]. Важно отметить, что в Республике Беларусь информационная безопасность систем, в которых обрабатываются персональные данные, может быть обеспечена посредством обезличивания персональных данных. Обезличиванием персональных данных называют любое действие или совокупность действий, совершаемых с персональными данными, в результате которых становится невозможным определение их принадлежности субъекту персональных данных без дополнительной информации.

В соответствии с требованиями законодательства Республики Беларусь в сфере защиты персональных данных одним из методов обеспечения их информационной безопасности является метод изменения состава. Сущность этого метода заключается в следующем. Часть персональных данных, подлежащих обезличиванию, удаляют, другую часть изменяют, а оставшуюся часть преобразуют таким образом, что изменяется семантическое представление данных. В случае удаления персональных данных или изменения их отдельных частей требуется отдельно хранить информацию о том, какие именно данные удалены и изменены. В противном случае становится невозможным выполнение процедуры деобезличивания.

Деобезличивание – это процесс, в результате которого обезличенные персональные данные принимают исходный вид.

Важно отметить, что существующие реализации метода изменения состава характеризуются достаточно низким уровнем информационной безопасности, поскольку в случае изменения семантического представления данных статистические свойства обезличенных данных остаются такими же, как и для естественного языка. В связи с этим целью данной работы являлась разработка структурной схемы, позволяющей реализовывать обезличивание персональных данных на основе метода изменения состава, которая свободна от недостатков существующих схем обезличивания персональных данных.

Объектом исследования являлся метод изменения состава, применяемый для обезличивания персональных данных в соответствии с требованиями законодательства Республики Беларусь в сфере защиты информации.

Предметом исследования являлось установление процедуры обезличивания персональных данных, в результате реализации которой обеспечивается повышение уровня их информационной безопасности за счет изменения статистических свойств, в сравнении с исходными персональными данными.

Реализация процедуры обезличивания персональных данных

Процедура обезличивания персональных данных реализована программно и заключается в следующем. Исходные персональные данные, подлежащие обезличиванию, подают на блок загрузки персональных данных, в котором выделяются атрибуты персональных данных, подлежащих обезличиванию. Затем исходные персональные данные поступают на блок фрагментации, где персональные данные разделяют на 64-битные части. После этого осуществляют итерационный процесс обезличивания, в который входит использование 64-битного вектора инициализации, значение которого для каждого текущего блока инкрементируют, а также процедура генерации раундовых секретных

ключей и операции сложения по модулю 2^{32}, нелинейной подстановки, согласно секретной таблице замены, и циклического сдвига влево на 11 разрядов согласно ГОСТ 28147-89. После выполнения всех 32 циклов итерационного процесса полученные блоки конкатенируют и формируют обезличенные персональные данные. Первичный анализ обезличенных персональных данных показал, что статистические свойства этих данных изменились, в сравнении со статистическими свойствами исходных персональных данных. В связи с этим авторам настоящей работы видится перспективным проведение исследований, направленных на оценку достигнутого уровня информационной безопасности персональных данных, что планируется выполнить в дальнейшем.

Заключение

При реализации обезличивания персональных данных буквенного и числового типов достаточно важным является осуществление процедуры обезличивания таким образом, чтобы статистические свойства обезличенных персональных данных не совпадали со статистическими свойствами исходных персональных данных, что повышает достигаемый уровень информационной безопасности. Предложена процедура обезличивания персональных данных буквенного типа на основе метода изменения состава, использование которой позволяет достичь эффекта, при котором статистические свойства исходных персональных данных отличаются от статистических свойств, обезличенных персональных данных. Данная процедура не требует наличия больших вычислительных ресурсов, что расширяет область ее возможного практического применения.

Список использованных источников

1. Ворона, В. А. (2023) *Биометрическая идентификация личности*. Москва, Горячая линия-Телеком.

2. Коллинз, М. (2020) *Защита сетей. Подход на основе анализа данных*. Москва, ДМК Пресс.

3. Остапенко, Г. А. (2020) *Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия*. Москва, Горячая линия-Телеком.

References

1. Vorona V. A. (2023) *Biometric Identification of Personality*. Moscow, Goryachaya Liniya-Telecom (in Russian).

2. Collins M. (2020) *A Data-Based Approach*. Moscow, DMK Press (in Russian).

3. Ostapenko G. A. (2020) *Information Operations and Attacks in Socio-Technical Systems: Organizational and Legal Aspects of Counteraction*. Moscow, DMK Press (in Russian).

Сведения об авторах

Тимофеев А.М., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», tambsuir@bsuir.by.

Шляхтун Д.В, учащаяся по направлению «Информационная безопасность», учреждение образования «Национальный детский технопарк», rd2859002@gmail.com.

Ли Ч., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», lcaomi@outlook.com.

Хуан Ц., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», 1913017013@qq.com.

Information about the authors

Timofeev A., Cand. Sci. (Tech.), Assosiate Professor, Associate Professor of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", tambsuir@bsuir.by.

Shliakhtun D., Student of the direction "Information Security", Educational Institution "National Children's Technopark", rd2859002@gmail.com.

Chengtingyu Li, Master's Student of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", lcaomi@outlook.com.

Huang Z., Master's Student of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", 1913017013@qq.com.