УДК 621.383

СТРУКТУРНАЯ СХЕМА ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

А.М. ТИМОФЕЕВ[1], К.Р. ВОСКОВЦЕВА[2], Я.А. КЛИНДУХОВ[2]

1 – Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь,
2 – Национальный детский технопарк, Республика Беларусь

Поступила в редакцию 1 апреля 2025

Аннотация. С учетом требований законодательства Республики Беларусь в сфере защиты информации предложена структурная схема, посредством которой возможна реализация процедуры обезличивания персональных данных на базе метода изменения состава или семантики. Данная схема основа на применении набора доверительных вычислительных баз, разделении персональных данных на отдельные блоки и характеризуется достаточно высоким уровнем информационной безопасности, что определяется усложнением процедуры частотного анализа, который может быть применен со стороны нарушителя информационной безопасности по отношению к обезличенным персональным данным. Реализация обезличивания персональных данных с применением предложенной схемы предусмотрена на базе программных, аппаратных или программно-аппаратных средств, не требует больших вычислительных мощностей со стороны оборудования легитимных пользователей, может быть применена к любым атрибутам персональных данных и позволяет сохранить такое свойство обезличенных персональных данных, как полнота.

Ключевые слова: информационные системы, персональные данные, обезличивание персональных данных, методы обезличивания персональных данных, метод изменения состава или семантики.

Введение

В настоящее время одной из наиболее важных задач, решаемых при построении информационных систем и обработке содержащейся в ней информации, является обеспечение защиты информации [1–3].

Информационной системой называют совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств [4].

Защита информации подразумевает применение комплекса правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации [4].

В соответствие с требованиями законодательства Республики Беларусь [5, 6] собственник (владелец) информационной системы, предназначенной для обработки персональных данных (информации ограниченного распространения/предоставления) обязан принимать меры по обеспечению информационной безопасности персональных данных в случае, если персональные данные не являются общедоступными, а относятся к биометрическим, генетическим, специальным или иным персональным данным.

Персональными данными является любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано [5].

Физическое лицо, которое может быть идентифицировано, – это физическое лицо, которое может быть прямо или косвенно определено, в частности через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности [5].

Для обеспечения информационной безопасности персональных данных целесообразно использовать методы их обезличивания [6]. К числу таких методов относят метод изменения состава или семантики, сущность реализации которого заключается в обобщении, изменении или удалении части сведений, позволяющих идентифицировать субъекта персональных данных.

Субъект персональных данных – это физическое лицо, в отношении которого осуществляется обработка персональных данных [5].

Обезличивание персональных данных указанным выше методом не требует наличия больших вычислительных мощностей, однако характеризуется следующими недостатками. Во-первых, удаление части сведений, позволяющих идентифицировать субъекта персональных данных, без их сохранения в отдельной базе данных приводит к утрате такого свойства обезличенных персональных данных, как полнота. Во-вторых, простые замены исходных символов персональных данных обезличенными сохраняет вероятности появления соответствующих символов обезличенных персональных данных. В этом случае нарушитель информационной безопасности имеет возможность, получив доступ к обезличенным персональным данным, рассчитать вероятности появления отдельных символов и различных их сочетаний, что позволит ему раскрыть содержимое доверительной вычислительной базы (ДВБ). В связи с этим целью данной работы являлась разработка схемы обезличивания персональных данных, построенной на базе метода изменения состава или семантики, которая свободна от недостатков существующих схем обезличивания персональных данных и не требует больших вычислительных ресурсов от оборудования легитимных пользователей.

В качестве объекта исследования использован метод изменения состава или семантики. Данный метод выбран в качестве объекта исследования, поскольку он является одним из методов обезличивания персональных данных в соответствии с требованиями Оперативно-аналитического центра при Президенте Республики Беларусь [6], являющимся государственным органом, который осуществляет регулирование деятельности по обеспечению защиты информации.

Предметом исследования являлась разработка структурной схемы, реализующей обезличивание персональных данных на основе метода изменения состава или семантики с применением набора ДВБ.

Реализация метода изменения состава или семантики

На рис. 1 показана структурная схема обезличивания персональных данных, построенная на базе метода изменения состава или семантики.

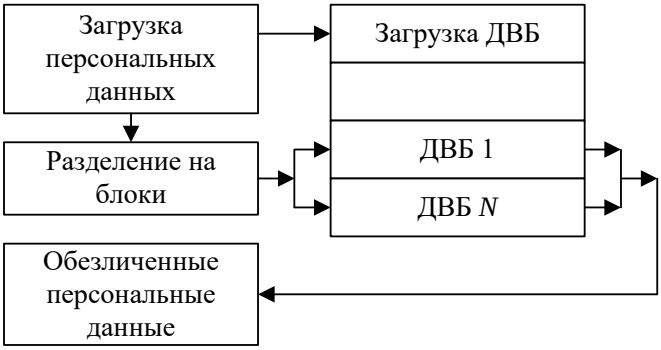

Рис. 1. Структурная схема обезличивания персональных данных, построенная на базе метода изменения состава или семантики с применением наборов ДВБ

Сущность функционирования данной схемы заключается в следующем. Персональные данные, подлежащие обезличиванию, загружают в ДВБ, которая содержит набор таблиц подстановки ДВБ 1, ДВБ 2, …, ДВБ N. Персональные данные разбивают на блоки, каждый из которых последовательно обезличивают с помощью ДВБ 1, ДВБ 2, …, ДВБ N, ДВБ 1, ДВБ 2, …, ДВБ N и т.д.

Важно отметить, что содержимое ДВБ необходимо сохранять в секрете и обновлять в соответствии с требованиями, предъявляемыми в месте эксплуатации информационной системы.

Заключение

Разработана структурная схема обезличивания персональных данных на основе набора доверительных вычислительных баз, содержащих символы исходных персональных данных и символы обезличенных персональных данных.

Предложены принципы обезличивания персональных данных на основе метода изменения состава или семантики, заключающиеся в использовании наборов доверительных вычислительных баз, что позволило повысить уровень информационной безопасности обезличенных персональных данных за счет изменения вероятности появления символов обезличенных персональных данных по отношению к соответствующим символам исходных персональных данных.

STRUCTURAL SCHEME OF DEPERSONALIZATION OF PERSONAL DATA

A.M. TIMOFEEV, K.R. VOSKOVTSEVA, Y.A. KLINDUKHOV

Abstract. A structural scheme of personal data depersonalization is proposed. This scheme is based on the method of changing the composition or semantics and complies with the requirements of the legislation of the Republic of Belarus in the field of information security. The scheme uses a set of trusted computing bases and division of personal data into separate blocks. This complicates the procedure of frequency analysis, which can be applied by an information security violator in relation to depersonalized personal data. The implementation of personal data depersonalization is provided on the basis of software and hardware. At the same time, no large computing power is required from the equipment of legitimate users. The scheme can be applied to any attributes of personal data and allows preserving such a property of depersonalized personal data as completeness.

Keywords: information systems, personal data, depersonalization of personal data, methods of depersonalization of personal data, method of changing the composition or semantics.

Список литературы

1. Ворона В.А. Биометрическая идентификация личности. М., 2023.
2. Коллинз М. Защита сетей. Подход на основе анализа данных. М., 2020.
3. Остапенко Г.А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия. М., 2020.
4. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=2012&oldDoc=2008-279/2008-279(014-027).pdf&oldDocPage=1. – Дата доступа: 28.02.2025 г.
5. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099. – Дата доступа: 28.02.2025 г.
6. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2024 г. № 259 «Об изменении приказов Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26 и от 20 февраля 2020 г. № 66» [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2024%20-%20259.pdf. – Дата доступа: 28.02.2025 г.