УДК 621.383

ПРОЦЕДУРА ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ МЕТОДА ИЗМЕНЕНИЯ СОСТАВА

А.М. ТИМОФЕЕВ[1], Д.В. ШЛЯХТУН[2]

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

Поступила в редакцию 1 апреля 2026

Аннотация. Предложена структурная схема программной реализации алгоритма обезличивания данных на основе метода изменения состава, которая соответствует требованиям законодательства Республики Беларусь в сфере защиты информации. Процедура обезличивания включает в себя разделение исходных данных на 64-битные блоки и их последующее итерационное преобразование в соответствии с ГОСТ 28147-89 и характеризуется достаточно высоким уровнем информационной безопасности, так как значительно затрудняет статистический анализ со стороны нарушителя из-за изменения статистических свойств обезличенных персональных данных. Предложенная структурная схема процедуры обезличивания универсальна для любых атрибутов персональных данных и допускает реализацию при помощи программных, аппаратных или аппаратно-программных средств. Благодаря оптимизации алгоритма решение не налагает высоких требований к вычислительным мощностям пользовательского оборудования, обеспечивая высокую доступность технологии для информационных систем легитимных пользователей.

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

Введение

Обеспечение конфиденциальности в современных информационных системах напрямую зависит от качественного обезличивания персональных данных [1 – 3]. Сегодня для этого активно применяют методы обезличивания персональных данных. Актуальность этой задачи в Республике Беларусь продиктована требованиями законодательства, которое обязывает операторов принимать меры по защите прав и свобод субъектов персональных данных при обработке их личных сведений [4, 5].

В соответствии с требованиями законодательства Республики Беларусь в сфере защиты информации одним из основных способов обезличивания персональных данных является метод изменения состава [4]. Суть этого метода заключается в том, что часть сведений о субъекте персональных данных обобщается, изменяется или удаляется. Однако этот подход имеет существенные недостатки. Он не обеспечивает достаточный уровень информационной безопасности при семантических преобразованиях исходных персональных данных, так как оставляет возможность их деобезличивания при помощи сопоставления с внешними источниками. Кроме того, удаление или изменение части данных заставляет оператора хранить исходные персональные данные отдельно для обеспечения их целостности и возможности восстановления. Это неизбежно увеличивает нагрузку на инфраструктуру и существенно увеличивает объем баз данных.

В настоящей работе представлена процедура обезличивания на основе метода изменения состава, лишенная описанных недостатков. Предложенный алгоритм не требует больших вычислительных ресурсов и подходит для оборудования легитимных пользователей. При этом предложенная процедура обезличивания позволяет существенно сократить объем хранимых

персональных данных по сравнению с существующими способами реализации метода изменения состава. Повышение уровня информационной безопасности достигается за счет трансформации статистических свойств данных, что исключает возможность их успешного анализа злоумышленником.

Потому целью исследования стала разработка такой процедуры обезличивания, которая повысит уровень информационной безопасности обезличенных персональных данных и оптимизирует ресурсы системы. Объектом работы стал метод изменения состава. Предметом исследования являлось повышение уровня информационной безопасности обезличенных персональных данных благодаря изменению их вероятностных характеристик.

Процедура обезличивания персональных данных

На рис. 1 представлена структурная схема, описывающая процедуру обезличивания персональных данных на основе метода изменения состава или семантики.

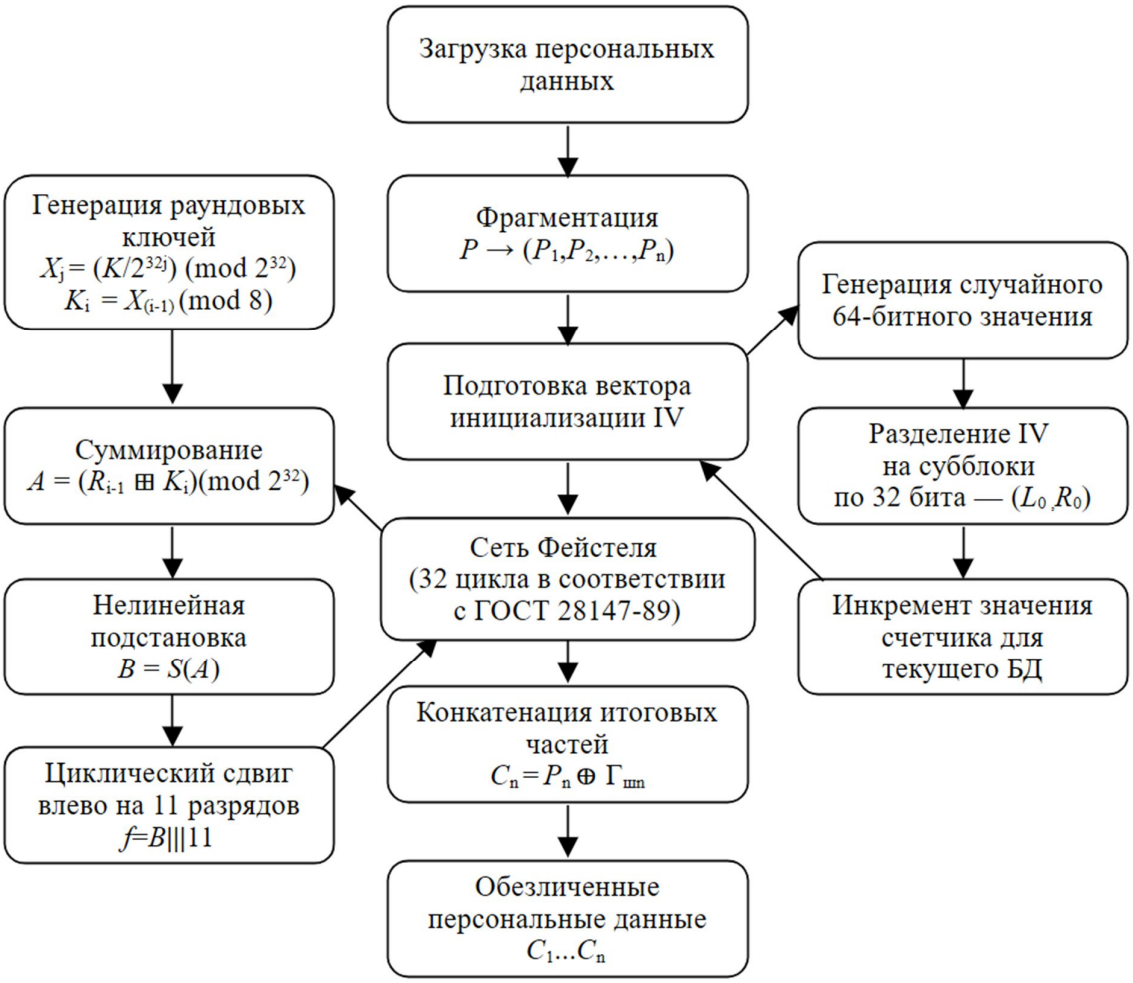

Рис. 1. Структурная схема обезличивания персональных данных, построенная на основе метода изменения состава

Процедура обезличивания персональных данных в соответствии с данной структурной схемой представляет собой итерационный программный алгоритм, который преобразует данные при помощи их посимвольного перевода в кодировку UTF-16, разбиения на 64-битные блоки и 32-циклового шифрования с использованием вектора инициализации и нелинейных подстановок [6]. Результатом процесса является конкатенация преобразованных блоков и их обратное преобразование в символьный вид.

Заключение

Разработана структурная схема программной реализации алгоритма обезличивания персональных данных на основе метода изменения состава, которая полностью соответствует требованиям законодательства Республики Беларусь в сфере защиты информации.

Применение итерационного процесса на основе ГОСТ 28147-89 с использованием изменяющегося вектора инициализации и процедур нелинейной подстановки позволяет изменить структуру исходных данных. Статистический анализ показывает, что энтропия полученных обезличенных персональных данных значительно выше, чем для исходных. Это сводит к минимуму вероятность распознавания содержания обезличенных персональных данных злоумышленником при помощи методов частотного или статистического анализа из-за изменения их статистических свойств.

Эффективность предложенного решения дополнительно повышается за счет внедрения предложенного метода фрагментации, который позволяет существенно сократить объем обрабатываемой информации. Переход от стандартного 16-битного представления UTF-16 к использованию 9-битного формата (управляющий флаг и 8 бит значимой части кода) обеспечивает значительную экономию дискового пространства и оперативной памяти. Такой подход гарантирует уменьшение объема данных при сохранении их полноты и возможности корректного восстановления исходного текста легитимными пользователями.

PERSONAL DATA DEPERSONALIZATION PROCEDURE BASED ON THE COMPOSITION CHANGE METHOD

A.M. TIMOFEEV, D.V. SHLIAKHTUN

Abstract. A structural diagram of the software implementation of the data depersonalization algorithm based on the composition change method is proposed, which complies with the requirements of the legislation of the Republic of Belarus in the field of information security. The anonymization procedure involves dividing the source data into 64-bit blocks and then iteratively transforming them in accordance with GOST 28147-89. This procedure offers a high level of information security, as it significantly complicates statistical analysis by an attacker due to changes in the statistical properties of the anonymized personal data. The proposed structural diagram of the anonymization procedure is universal for any personal data attributes and can be implemented using software, hardware, or a combination of hardware and software. Thanks to algorithm optimization, the solution does not place high demands on the computing power of user equipment, ensuring high availability of the technology for the information systems of legitimate users.

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. 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: 19.03.2026 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: 19.03.2026 г.
6. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200007350. – Дата доступа: 19.03.2026.