УДК 621.383

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

А.М. ТИМОФЕЕВ[1], М.А. ТАВГЕНЬ[2], А.С. ЯНКОВЕЦ[2]

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

Поступила в редакцию 1 апреля 2025

Аннотация. Разработана структурная схема генерации идентификаторов, построенная на базе симметричного блочного стандарта ГОСТ 28147-89. Применение этого стандарта является обязательным для всех организаций и предприятий Республики Беларусь, осуществляющих криптографическую защиту информации. В предложенной схеме секретными параметрами являются ключ шифрования данных длиной 256 бит и 8 узлов замены, содержащихся в блоке подстановки. Шифротексты, полученные с помощью ГОСТ 28147-89, использованы в качестве псевдослучайной величины. Разработана структурная схема деобезличивания персональных данных, которая, как и схема обезличивания персональных данных, построена на базе ГОСТ 28147-89. Это позволило выполнить процедуру деобезличивания аналогичным образом, как и процедуру обезличивания, что упростило реализацию разработанных схем, в сравнении с существующими.

Ключевые слова: информационные системы, персональные данные, обезличивание персональных данных, методы обезличивания персональных данных, метод введения идентификаторов.

Введение

В настоящее время одной из важнейших задач, решаемых при проектировании современных информационных систем, является обеспечение информационной безопасности персональных данных [1–3].

Под персональными данными будем понимать любую информацию, относящуюся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано [4].

Отметим, что для этого целесообразно выполнять обезличивание и деобезличивание любых персональных данных, за исключением общедоступных персональных данных [5].

В соответствии с требованиями законодательства Республики Беларусь одним из методов обезличивания персональных данных является метод введения идентификаторов. Сущность реализации данного метода заключается в том, что персональные данные, позволяющие идентифицировать субъекта персональных данных, заменяют их идентификаторами с последующим созданием таблицы соответствия.

Известные способы реализации обезличивания персональных данных на основе метода введения идентификаторов [6–9] подразумевают использование в качестве идентификаторов хэшированных значений персональных данных. Это не позволяет деобезличить персональные данные без знания таблиц соответствия, что является недостатком способов [6–9]. В связи с этим целью данной работы являлось разработать структурные схемы обезличивания и деобезличивания персональных данных на основе метода введения идентификаторов.

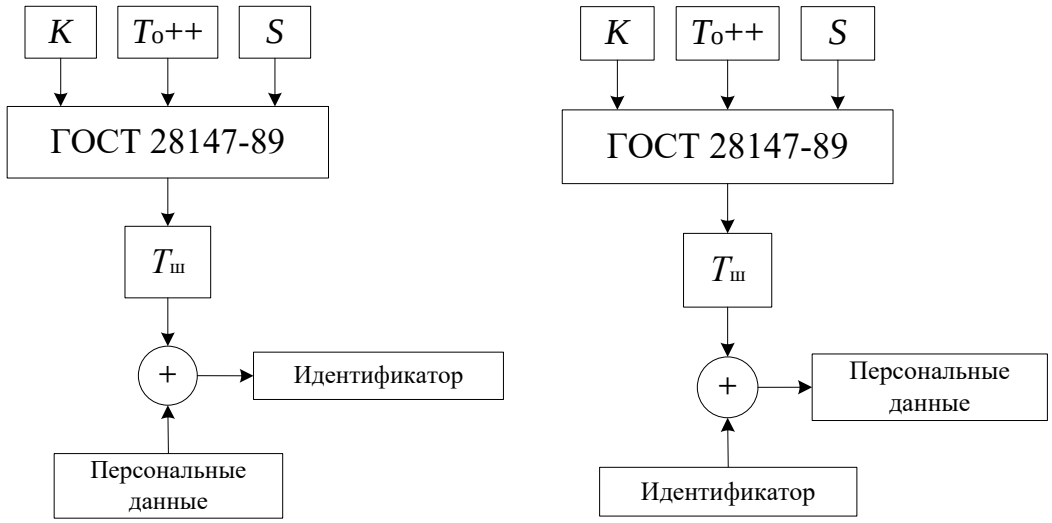
В качестве объекта исследования использован стандарт шифрования данных ГОСТ 28147-89. Данный стандарт выбран в качестве объекта исследования, поскольку он является одним из обязательных алгоритмов криптографического преобразования данных для

всех организаций и предприятий Республики Беларусь в соответствии с требованиями Оперативно-аналитического центра при Президенте Республики Беларусь [5].

Предметом исследования являлось установить криптографические операции, позволяющие выполнить обезличивание и деобезличивание персональных данных на основе метода введения идентификаторов, которые не требуют обязательного использования таблиц соответствия.

Реализация метода введения идентификатора

На рис. 1 показаны структурные схема, реализующие процедуры вычисления идентификаторов и персональных данных.



а *б*

Рис. 1. Структурные схемы: *а* – процедуры вычисления идентификаторов; *б* – процедуры вычисления персональных данных

Схема деобезличивания персональных данных функционирует схожим образом, как и схема обезличивания, за исключением следующего. В процессе деобезличивания на первый вход блока ГОСТ 28147-89 подаются ранее сформированные секретный криптографический ключ K и узлы подстановки S, а на второй вход – блоки открытого текста T_o, которые были использованы при обезличивании. На выходе блока ГОСТ 28147-89 формируются шифротексты $T_ш$, которые используются в качестве псевдослучайных последовательностей. Далее выполняют сложение по модулю 2 блоков шифротекстов $T_ш$ и идентификаторов, что позволяет восстановить исходные персональные данные. Процесс повторяется до тех пор, пока не будут обработаны все блоки идентификаторов.

Важно отметить, что схема деобезличивания персональных данных, предложенная в настоящей работе, не требует использования таблиц соответствия, что выгодно отличает данную схему, по сравнению с существующими [6–9].

Заключение

При реализации метода введения идентификаторов чрезвычайно важно применять алгоритмы и математические вычисления, которые позволят не только преобразовывать персональные данные к виду идентификаторов (обезличивать их), но и вычислительно выполнить обратную процедуру, т.е. на основе идентификаторов рассчитывать персональные данные.

В рамках выполненных исследований разработана структурная схема генерации идентификаторов, построенная на базе симметричного блочного стандарта ГОСТ 28147-89. Применение этого стандарта является обязательным для всех организаций и предприятий Республики Беларусь, осуществляющих криптографическую защиту информации.

В предложенной схеме секретными параметрами являются ключ шифрования данных длиной 256 бит и 8 узлов замены, содержащихся в блоке подстановки. Шифротексты использованы в качестве псевдослучайной величины.

Разработана структурная схема деобезличивания персональных данных, которая, как и схема обезличивания персональных данных, построена на базе ГОСТ 28147-89. Это позволило выполнить процедуру деобезличивания аналогичным образом, как и процедуру обезличивания. Таким образом, реализовав программное обеспечение для обезличивания персональных данных, появляется возможность использовать это же программное обеспечение для деобезличивания персональных данных, что упрощает практическую реализацию схем обезличивания и деобезличивания персональных данных.

ENSURING INFORMATION SECURITY OF PERSONAL DATA WHEN PROCESSING THEM IN INFORMATION SYSTEMS

A.M. TIMOFEEV, M.A. TAVGEN, A.S. YANKOVETS

Abstract. A block diagram of identifier generation based on the symmetric block standard GOST 28147-89 has been developed. The application of this standard is mandatory for all organizations and enterprises of the Republic of Belarus engaged in cryptographic protection of information. In the proposed scheme, the secret parameters are a 256-bit data encryption key and 8 replacement nodes contained in the substitution block; ciphertexts are used as a pseudorandom value. A structural scheme of depersonalization of personal data has been developed, which, like the scheme of depersonalization of personal data, is based on GOST 28147-89. This made it possible to perform the depersonalization procedure in the same way as the depersonalization procedure.

Keywords: information systems, personal data, depersonalization of personal data, methods of depersonalization of personal data, method of introducing identifiers.

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 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.
5. 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.
6. Raghunathan, S. The Complete Book of Data Anonymization: From Planning to Implementation. CRC Press, 2013.
7. Ali, J., Dyo, V. Practical Hash-based Anonymity for MAC Addresses [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2005.06580. – Дата доступа: 28.02.2025 г.
8. Determe J.-F., Azzagnuni S., Horlin F., De Doncker P. MAC Address Anonymization for Crowd Counting [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2009.09876. – Дата доступа: 28.02.2025 г.
9. European Data Protection Supervisor. Introduction to the Hash Function as a Personal Data Pseudonymisation Technique [Электронный ресурс]. – Режим доступа: https://www.edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, свободный. – Дата доступа: 28.02.2025 г.