ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ МЕТОДА ВВЕДЕНИЯ ИДЕНТИФИКАТОРОВ

*Тавгень М.А., учащийся по направлению «Информационная безопасность»,
Янковец А.С., учащийся по направлению «Информационная безопасность»*

*Национальный детский технопарк
г. Минск, Республика Беларусь*

Аннотация. Разработаны структурные схемы обезличивания и деобезличивания персональных данных, построенные на базе симметричного блочного стандарта ГОСТ 28147-89. В предложенных схемах секретными параметрами являются ключи 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, посредством которой реализованы процедуры обезличивания и деобезличивания персональных данных.

В настоящее время одной из важнейших задач, решаемых при проектировании современных информационных систем, является обеспечение информационной безопасности персональных данных, что реализуется посредством обезличивания персональных данных [1 – 3]. В соответствии с требованиями законодательства Республики Беларусь одним из методов обезличивания персональных данных является метод введения идентификаторов. 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, свободных от этого недостатка.

В качестве объекта исследования использован стандарт шифрования данных ГОСТ 28147-89. 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.

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.

Список использованных источников:

1. Ворона, В. А. Биометрическая идентификация личности / В. А. Ворона. – Москва : Горячая линия-Телеком, 2023. – 228 с.
2. Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз. – Москва : ДМК Пресс, 2020. – 308 с.
3. Остапенко, Г. А. Информационные операции и атаки в социотехнических системах : организационно-правовые аспекты противодействия : учебное пособие / Г. А. Остапенко, Е. А. Мешкова ; под ред. В. Г. Кулакова. – 2-е изд., стер. – Москва : Горячая линия-Телеком, 2020. – 208 с.
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.

61-я научная конференция аспирантов, магистрантов и студентов БГУИР, 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*. – Boca Raton: CRC Press, 2013. – 500 с.

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.