РАЗРАБОТКА СТРУКТУРНОЙ СХЕМЫ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Восковцева К.Р., учащаяся по направлению «Информационная безопасность»,
Клиндухов Я.А., учащийся по направлению «Информационная безопасность»

Национальный детский технопарк
г. Минск, Республика Беларусь

Тимофеев А.М. – канд. техн. наук, доцент, доцент кафедры защиты информации БГУИР (научный руководитель)

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 характеризуется достаточно высоким уровнем информационной безопасности, достигаемого посредством парирования частотного анализа обезличенных персональных данных.

В настоящее время одной из наиболее важных задач, решаемых при построении информационных систем, является обеспечение защиты информации [1 – 3]. 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. 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. Обезличивание персональных данных указанным выше методом не требует наличия больших вычислительных мощностей, однако характеризуется следующими недостатками. Например, 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. Также важно отметить, что простые замены исходных символов персональных данных обезличенными сохраняют 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. Предметом исследования являлась разработка структурной схемы, реализующей обезличивание персональных данных на основе метода изменения состава или семантики с применением набора ДВБ.

В рамках выполненных исследований разработана структурная схема обезличивания персональных данных, построенная на базе метода изменения состава или семантики.

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.

Выполненная оценка показала, что предложенные принципы обезличивания персональных данных на основе метода изменения состава или семантики, заключающиеся в использовании наборов ДВБ, позволили повысить уровень информационной безопасности обезличенных персональных данных за счет изменения вероятности появления символов обезличенных персональных данных по отношению к соответствующим символам исходных 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 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.