

Зайнуллин Б.И., Масальский Н.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.

Уфимский университет науки и технологий, Уфа

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК МЕТОД ЗАЩИТЫ

Аннотация. Обезличивание персональных данных представляет собой эффективный метод защиты конфиденциальной информации. Оно включает в себя такие техники, как перемешивание, введение идентификаторов и декомпозиция, позволяющие исключить возможность идентификации личности при обработке данных. Эти методы находят применение при сборе, хранении, поиске, актуализации и передаче персональных данных, обеспечивая соблюдение требований информационной безопасности и законодательства.

Ключевые слова: обезличивание, персональные данные, защита информации, идентификаторы, безопасность, конфиденциальность, метод перемешивания, декомпозиция, обработка данных, актуализация, хранение, поиск, информационные системы, идентификация, передача данных.

Обезличивание персональных данных – это действия, которые направлены на защиту информации от несанкционированного использования. В ходе процедуры персональные данные претерпевают значительные изменения, поэтому расшифровать их без использования дополнительной информации нет возможности.

Актуальность защиты персональных данных обусловлено тем, что с начала 2024 г. злоумышленники слили в сеть 286 млн телефонных номеров и 96 млн адресов электронных почт. Утечка информации с каждым годом увеличивается, так, например, в 2013 г. было слито 213 млн данных. В связи с этим был принят законопроект, который предусматривает максимальный штраф до трех процентов от годовой выручки компании за неправомерную передачу персональных данных третьим лицам.

Целью обезличивания является защита персональных данных при попытке несанкционированного доступа. Так как отсутствие ключа для восстановления базы усложнит работу мошенников.

Преимущества обезличивания данных:

- соответствие требованиям законодательства о персональных данных;
- снижение риска утечки личной информации;
- защита конфиденциальности.

Согласно приказу Роскомнадзора от 05.09.2013 № 996 существует несколько видов обезличивания персональных данных (рис. 1).

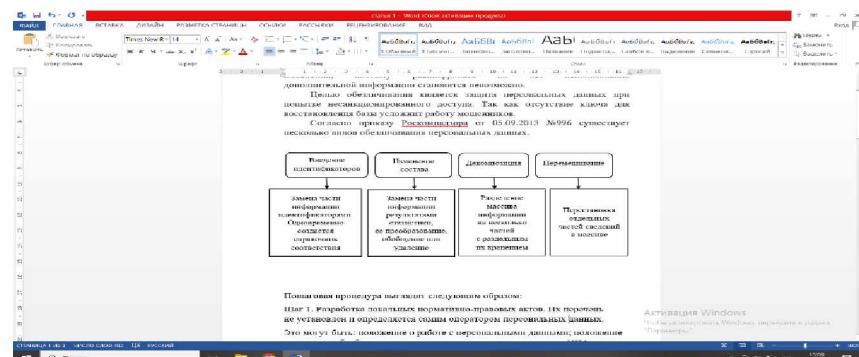


Рис. 1. Виды обезличивания персональных данных

При использовании метода обезличивания персональных данных, необходимо составлять план мероприятий. Примерная поэтапная структура:

1 этап. Необходимо разработать локальные нормативно-правовые акты.

В перечень нормативно-правовых актов могут включаться: положения о работе с персональными данными и положения о защите и обработке персональных данных.

2 этап. Назначить ответственных лиц.

3 этап. Провести обучение для ответственных лиц по правилам обработки персональных данных.

4 этап. Издать приказ о проведении обезличивания персональных данных.

5 этап. Проведение защиты персональных данных. По результатам составляется акт в произвольной форме.

В акте необходимо указать следующую информацию:

- проведенные процедуры;
- перечень персональных данных;
- ответственные лица.

Для того чтобы произвести выбор методов обезличивания персональных данных, необходимо учитывать класс задач. Данная классификация позволит ответственному лицу применить наиболее эффективные методы (табл. 1).

Таблица 1
Выбор методов обезличивания персональных данных

Класс задач	Задачи обработки	Метод обезличивания
Сбор и хранение персональных данных	внесение персональных данных в информационную систему на основе заявлений	метод перемешивания; метод введения идентификаторов
Обработка поисковых запросов	поиск информации и выдача документов, которые содержат персональные данные	метод перемешивания; метод введения идентификаторов; метод декомпозиции
Актуализация персональных данных	внесение изменений в базу персональных данных	метод перемешивания; метод введения идентификаторов; метод декомпозиции
Интеграция данных различных операторов	поиск информации и передача данных смежным органам	метод перемешивания; метод введения идентификаторов; метод декомпозиции
Ведение учета субъектов персональных данных	ведение учета персональных данных и прием заявлений	метод перемешивания; метод введения идентификаторов; метод декомпозиции

Хэширование – это такой же способ защиты персональных данных, как обезличивание данных.

Криптографические хэш-функции являются одним из эффективных методов обезличивания персональных данных. Хэш-функции применяются для преобразования входных данных в выходные данные фиксированной длины, которые называются хэшем.

Преимущества использования хэш-функций:

- устойчивость к коллизиям (вероятность того, что два разных ввода выдадут одинаковый хэш очень низка);
- необратимость (невозможность получить исходные данные имея только хэш).

Использование хэш-функции в обезличивании персональных данных можно применять для замены идентификаторов на их хэш-значения. Вследствие этого, данные теряют прямую связь с конкретным человеком, но остаются в форме, которая пригодная для дальнейшего использования. Для того, чтобы применить замену можно использовать алгоритм SHA-256. В базе данных, где хранятся фамилия, имя, отчество и пароли, можно заменить фамилию, имя и отчество (рис. 2).

Фамилия, имя и отчество	Хэш-функция
Петров Петр Петрович	9f87d02365456
Иванова Мария Ивановна	efy548der2656

Рис. 2. Пример базы данных

Основным преимуществом использования алгоритма SHA-256 заключается в том, что даже при получении доступа к базе данных, злоумышленник не сможет узнать настоящие имена пользователей, так как хэш невозможно преобразовать в исходные данные. При необходимости аутентификации, пользователь может ввести свои данные, которые будут хэшированы по такому же принципу и система сравнит полученный хэш с хранимой хэш-функцией.

Обезличивание персональных данных с помощью применения хэш-функций является эффективным средством защиты информации. Оно обеспечивает высокий уровень безопасности данных. Для того, чтобы повысить надежность защиты, необходимо комбинировать данный метод с другими средствами защиты.

Список использованных источников:

1. Байдуллина В.В. К вопросу о защите персональных данных: учебное пособие / В.В. Байдуллина, И.А. Шагапов. Уфа: БашГУ, 2016. 28 с.
2. Ломакин С.Т. Информационная безопасность: учебное пособие / С.Т. Ломакин. Сургут: СиУт, 2021. 121 с.
3. Васильков А.В. Безопасность и управление доступом в информационных системах: учебное пособие / А.В. Васильков. М.: ФРУМ, 2021. 121 с.

Zainullin B.I., Masalsky N.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

DEPERSONALIZATION OF PERSONAL DATA AS A METHOD OF PROTECTION

Abstract. Depersonalization of personal data is an effective method of protecting confidential information. It includes techniques such as mixing, introducing identifiers, and decomposition to eliminate the possibility of personal identification during data processing. These methods are used in the collection, storage, retrieval, updating and transfer of personal data, ensuring compliance with information security requirements and legislation.

Keywords: depersonalization, personal data, information protection, identifiers, security, confidentiality, mixing method, decomposition, data processing, updating, storage, search, information systems, identification, data transmission.