www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2023.3.5

УДК 004.056.5
ББК 16.8

ИЗУЧЕНИЕ ТЕХНОЛОГИЙ, ПОВЫШАЮЩИХ КОНФИДЕНЦИАЛЬНОСТЬ

Яна Алексеевна Чумбуридзе

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
chumburidze@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Олеся Александровна Какорина

Кандидат физико-математических наук, доцент,
заведующий кафедрой информационной безопасности,
Волгоградский государственный университет
davletova.olesya@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Конфиденциальная информация является ценным активом для организаций, и ее защита является критически важной для обеспечения безопасности бизнеса и сохранения доверия клиентов и партнеров. Вопрос конфиденциальности данных становится все более актуальным в свете растущего количества утечек данных как по всему миру, так и в России. В этой связи, появляются новые технологии, которые позволяют защитить данные от несанкционированного доступа и сохранить их конфиденциальность. В данной работе рассматриваются различные технологии, повышающие конфиденциальность данных, такие как анонимизация данных, псевдонимизация, методы множественных вычислений, блокчейн, дифференциальная конфиденциальность, гомоморфное шифрование их преимущества и недостатки. Приведена классификация технологий, повышающих конфиденциальность.

Ключевые слова: конфиденциальность, информационная безопасность, утечка информации, анонимизация, гомоморфное шифрование, блокчейн.

Данные и конфиденциальная информация являются критическими ресурсами для организаций, так как они содержат важную информацию о бизнес-процессах, клиентах, партнерах и т. д. Конфиденциальная информация может включать в себя данные о финансах, интеллектуальной собственности, персональных данных клиентов и сотрудников и другие данные. Утечки конфиденциальной информации приводят к финансовым потерям, потере репутации и доверия клиентов.

По данным аналитического отчета InfoWatch в 2022 г. было зафиксировано 6856 случаев утечки конфиденциальной информации по всему миру (см. рис. 1), в 3,57 раза больше, чем за 2021 г. [4].

В 2022 г. в России произошел скачок количества зарегистрированных утечек информации – 710 случаев (см. рис. 2). По сравнению с предыдущим годом количество утечек выросло более чем в 2,1 раза [3].

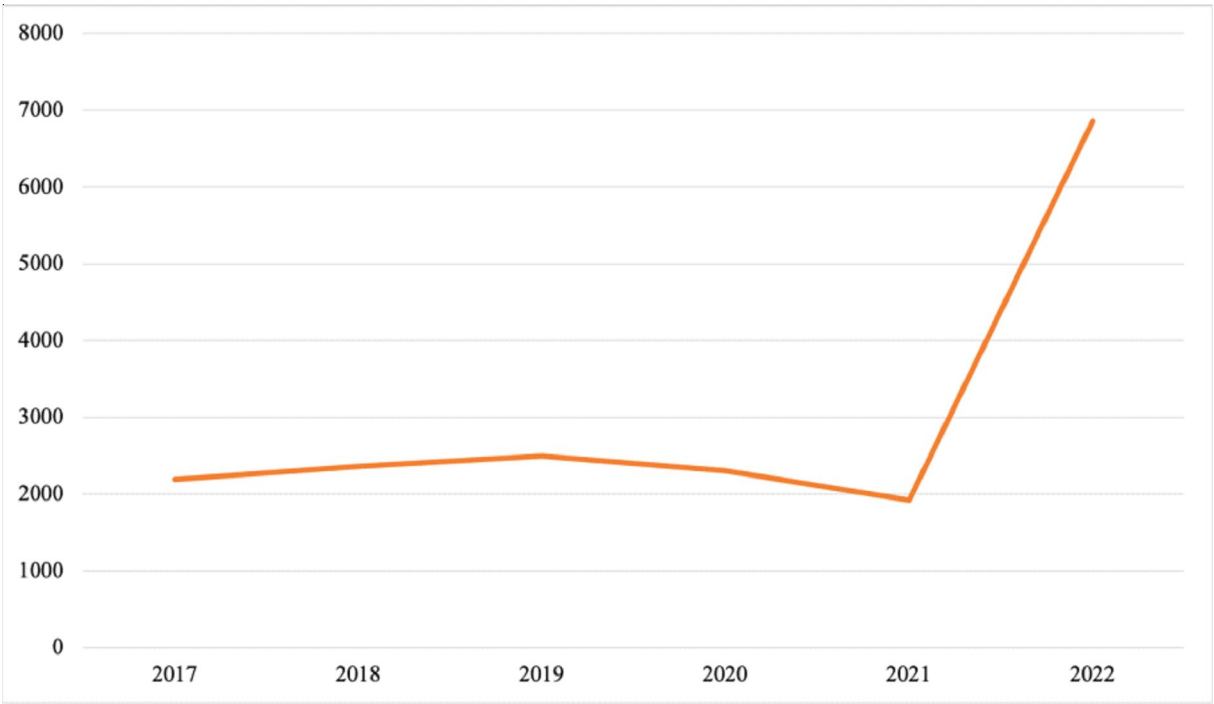

Рис. 1. Количество утечек данных: Мир, 2017–2022 гг.

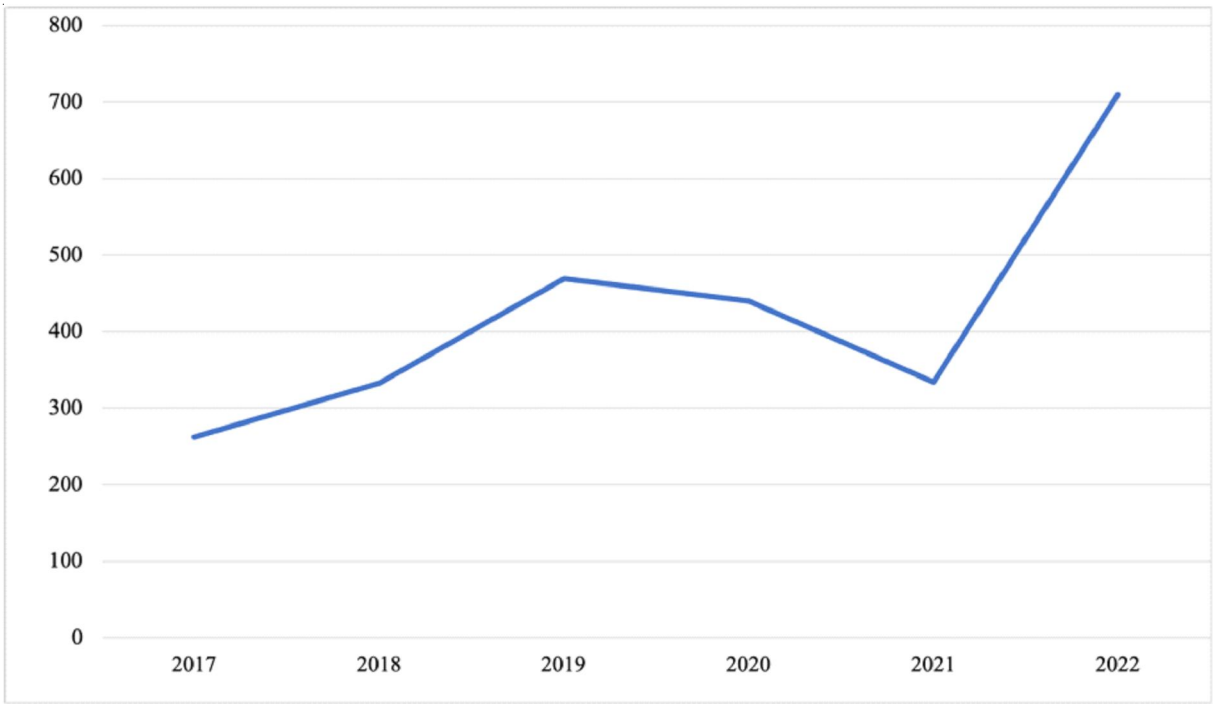

Рис. 2. Количество утечек данных: Россия, 2017–2022 гг.

Данная статистика подчеркивает необходимость использования технологий, повышающих конфиденциальность, для защиты данных и предотвращения утечек.

Технологии, повышающие конфиденциальность (Privacy-Enhancing Computation) – это методы обработки данных, которые позволяют сохранять конфиденциальность и защищать данные во время их обработки. Они используются для защиты информации от несанкционированного доступа и раскрытия конфиденциальной информации.

Технологии, повышающие конфиденциальность, можно разделить на несколько ка-

тегорий. Первая категория – это методы, которые изменяют сами данные. Обычно они стремятся нарушить связь между данными и человеком, с которым они связаны (анонимизация, псевдонимизация, дифференциальная конфиденциальность). Вторая группа фокусируется на сокрытии данных, а не на их изменении (гомоморфное шифрование). Третья категория представляет собой новые системы и архитектуры данных для обработки, управления и хранения данных. Некоторые из этих систем разделяют данные для вычисления или хранения, в то время как другие предоставляют уровни управления для отслеживания и аудита того, куда поступает информация и с какой целью (методы множественных вычислений, блокчейн) [1].

Технологии, повышающие конфиденциальность, являются важным инструментом в области информационной безопасности и помогают защитить конфиденциальную информацию пользователей и организаций. Технологии, повышающие конфиденциальность, влияют на безопасность информации, обеспечивая высокий уровень защиты данных от несанкционированного доступа и использования.

Существуют различные технологии, повышающие конфиденциальность. Рассмотрим каждую из них.

I. *Анонимизация данных* – это метод удаления прямых или косвенных идентификаторов из набора данных, который позволяет скрыть личную информацию о пользователе, сохраняя при этом необходимые данные для анализа. Например, при анонимизации данных о здоровье, можно скрыть имя и фамилию пациента, но сохранить информацию о заболевании.

Преимущества:

1. Предотвращение утечек данных и кражи личных данных.

2. Соответствие законодательству о защите персональных данных.

3. Уменьшение риска нарушения конфиденциальности.

4. Обеспечение безопасности взаимодействия с другими организациями.

Недостатки анонимизации данных для обеспечения конфиденциальности:

1. Сложность реализации и использования.

2. Не всегда возможна полная анонимизация данных.

3. Необходимость соблюдения определенных правил и требований при использовании анонимизации данных.

II. *Псевдонимизация* (*pseudonymisation*) – это обработка данных таким образом, что их больше невозможно отнести к конкретному субъекту данных без использования дополнительной информации. В таком случае дополнительная информация хранится отдельно, в целях предотвращения ее отнесения к идентифицируемому лицу [2].

Преимущества:

1. Сохранение возможности использования данных для анализа и исследований.

2. Уменьшение риска нарушения конфиденциальности при передаче данных.

3. Соответствие законодательству о защите персональных данных.

4. Более простая реализация и использование по сравнению с полной анонимизацией.

5. Возможность проведения анализа данных с сохранением конфиденциальности.

Недостатки:

1. Не всегда возможна полная защита конфиденциальности.

2. Возможность деанонимизации данных при наличии дополнительной информации.

3. Необходимость соблюдения определенных правил и требований при использовании псевдонимизации данных.

III. *Методы множественных вычислений* (*multi-party computation*) – это метод, который позволяет нескольким сторонам выполнять вычисления над общими данными, не раскрывая при этом эти данные друг другу. Этот метод подразделяет данные на множество общих ресурсов, которые распределяются и анализируются различными организациями. Разделение информации означает, что, если какой-либо один объект будет скомпрометирован, весь набор данных не будет подвергнут риску.

Преимущества:

1. Гарантированная конфиденциальность данных, так как они не раскрываются ни одной из сторон.

2. Возможность совместной обработки данных нескольких участников без необходимости раскрытия информации друг другу.

3. Высокий уровень защиты от кражи данных.

4. Возможность проведения анализа данных и исследований с сохранением конфиденциальности.

Недостатки:

1. Сложность реализации и использования, требующая высокой квалификации специалистов.

2. Необходимость соблюдения определенных правил и требований при использовании multi-party computation.

3. Низкая скорость обработки данных по сравнению с другими методами.

IV. *Блокчейн* (*blockchain*) – это метод, который использует распределенную реестр для хранения и защиты данных. Блокчейн позволяет создать надежную систему хранения данных, которая не может быть изменена без согласия всех участников.

Преимущества:

1. Децентрализация блокчейн не имеет централизованного управления, что делает его более защищенным от хакерских атак.

2. Неподдельность данных.

3. Прозрачность операций, что позволяет пользователям проверять историю транзакций.

4. Высокая анонимность.

Недостатки:

1. Сложность использования – блокчейн является новой технологией, которая требует особого знания и опыта для использования.

2. Масштабируемость – блокчейн может иметь проблемы с масштабированием, особенно если он используется для больших объемов данных.

3. Невозможность удаления данных – данные, сохраненные в блокчейне, не могут быть удалены или изменены.

4. Высокая стоимость – создание и использование блокчейна может быть дорогим, особенно для малых и средних компаний.

V. *Дифференциальная конфиденциальность* (*differential privacy*) – это метод, который позволяет сохранять конфиденциальность данных при анализе больших наборов данных. Вместо удаления или изменения элементов данных для скрытия идентификаторов дифференциальная конфиденциальность добавляет случайные, дополнительные данные или шум. Цель метода – добавить достаточное количество случайных дополнительных данных, чтобы реальная информация была скрыта среди шума.

Преимущества:

1. Обеспечивает высокую конфиденциальность данных, даже если злоумышленник получает доступ к части информации.

2. Позволяет использовать данные для статистического анализа и исследований без нарушения конфиденциальности.

Недостатки:

1. Некоторые данные могут быть недоступны для анализа из-за ограничений на конфиденциальность.

2. Результаты анализа могут быть менее точными из-за скрытия некоторых данных.

3. Дифференциальная конфиденциальность может быть сложна для реализации и требует специальных навыков и знаний.

VI. *Гомоморфное шифрование* (*homomorphic encryption*) – это метод шифрования данных, который позволяет выполнять операции над зашифрованными данными, не расшифровывая их. Это означает, что данные могут быть зашифрованы и переданы по открытому каналу связи, а затем обработаны на удаленном сервере, не раскрывая их содержимое.

Преимущества:

1. Обеспечивает более высокий уровень конфиденциальности, чем традиционные методы.

Недостатки:

1. Вычисления с зашифрованными данными могут быть медленными.

2. Гомоморфное шифрование может быть сложно реализовать и требует специальных навыков и знаний.

3. Метод требователен к ресурсам, что может снизить производительность системы.

4. Существует риск ошибок при вычислениях с зашифрованными данными, что может привести к ошибкам в результате обработки данных.

5. Гомоморфное шифрование может быть дороже, чем традиционные методы шифрования.

Каждая из рассмотренных технологий, повышающих конфиденциальность, имеет свои преимущества и недостатки, но все они направлены на обеспечение безопасности информации. Однако необходимо понимать, что ни один метод не является абсолютно надежным и может быть подвержен атакам. Поэтому для обеспечения максимальной бе-

зопасности данных необходимо использовать несколько методов защиты и постоянно совершенствовать систему защиты данных.

СПИСОК ЛИТЕРАТУРЫ

1. Asrow, K. Privacy Enhancing Technologies: Categories, Use cases and Considerations / K. Asrow // Federal Reserve Bank of San Francisco. – Electronic text data. – Mode of access: https://www.frbsf.org/economic-research/wp-content/uploads/sites/4/Privacy-Enhancing-Technologies-Categories-Use-Cases-and-Considerations.pdf. – Title from screen.

2. Дегтярев, Д. И. Безопасная компиляция и архитектуры защищенных модулей / Д. И. Дегтярев, О. А. Какорина // Безопасность информационных систем и технологий в условиях цифровой экономики : материалы IX Всерос. науч.-практ. конф. с междунар. участием (Волгоград, 27–28 окт. 2021 г.) / редколл.: О. А. Какорина, Ю. С. Бахрачева, Т. А. Попова. – Волгоград : Волгоград. гос. ун-т, 2021. – С. 23–26.

3. Россия: утечки информации ограниченного доступа в 2022 г. // Информационная безопасность в цифровой экономике | Российская DLP-система. – Электрон. текстовые дан. – Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god.pdf. – Загл. с экрана.

4. Утечки информации ограниченного доступа в мире 2022 г. // Информационная безопасность в цифровой экономике | Российская DLP-система. – Электрон. текстовые дан. – Режим доступа: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g. – Загл. с экрана.

REFERENCES

1. Asrow K. *Privacy Enhancing Technologies: Categories, Use Cases and Considerations. Federal Reserve Bank of San Francisco*. URL: https://www.frbsf.org/economic-research/wp-content/uploads/sites/4/Privacy-Enhancing-Technologies-Categories-Use-Cases-and-Considerations.pdf

2. Degtjarev D.I., Kakorina O.A. *Bezopasnaja kompiljacija i arhitektury zashhishhennyh modulej* [Secure Compilation and Architectures of Secure Modules]. *Bezopasnost informacionnyh sistem i tehnologij v uslovijah cifrovoj ekonomiki: materialy IX Vseros. nauch.-prakt. konf. s mezhdunar. uchastiem (Volgograd, 27–28 okt. 2021 g.)* [Security of Information Systems and Technologies in the Digital Economy. Proceedings of the 9th All-Russian Scientific and Practical Conference with International Participation. Volgograd, October 27–28, 2021]. Volgograd, Volgograd. gos. un-t, 2021, pp. 23-26.

3. Rossija: utechki informacii ogranichennogo dostupa v 2022 g. [Russia: Leaks of Restricted Information in 2022]. *Informacionnaja bezopasnost v cifrovoj ekonomike | Rossijskaja DLP-sistema* [Information Security in the Digital Economy | Russian DLP-System]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god.pdf

4. *Utechki informacii ogranichennogo dostupa v mire 2022 g.* [Leaks of Restricted Information in the World 2022]. *Informacionnaja bezopasnost v cifrovoj ekonomike | Rossijskaja DLP-sistema* [Information Security in the Digital Economy | Russian DLP-system]. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g

STUDYING OF PRIVACY-ENHANCING TECHNOLOGIES

Yana A. Chumburidze

Student, Department of Information Security,
Volgograd State University
chumburidze@volsu.ru
Prosp. Universitetskiy, 100, 400062 Volgograd, Russian Federation

Olesya A. Kakorina

Candidate of Sciences (Physics and Mathematics), Associate Professor,
Head of the Department of Information Security,
Volgograd State University
davletova.olesya@volsu.ru
Prosp. Universitetskiy 100, 400062 Volgograd, Russian Federation

Abstract. Confidential information is a valuable asset for organizations, and its protection is critical to ensure business security and maintain the trust of customers and partners. The issue of data privacy is becoming increasingly relevant in light of the growing number of data leaks both around the world and in Russia. This paper discusses various privacy-enhancing technologies. In this regard, new technologies are emerging that allow you to protect data from unauthorized access and maintain their confidentiality. This paper discusses various technologies that increase data privacy, such as data anonymization, pseudonymization, multiple computing methods, blockchain, differential confidentiality, homomorphic encryption, their advantages and disadvantages. The classification of technologies that increase privacy is given.

Key words: privacy, information security, data leak, anonymization, homomorphic encryption, blockchain.