**Дата поступления рукописи в редакцию: 21.07.2026 г.**
**Дата принятия рукописи в печать: 01.09.2026 г.**
DOI: 10.24412/2224-9133-2026-8-416-421

***РУСТАМОВА Людмила Рустамовна,***
*Доцент кафедры Информационных систем и технологий ФГБОУ ВО «Ингушский государственный университет»,*
*e-mail: rustamoval@mail.ru*

# *АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ РАСТУЩЕЙ УГРОЗЫ КИБЕРАТАК: СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ШИФРОВАНИЯ И АНОНИМИЗАЦИИ*

***Аннотация.*** *По мере развития цифровых технологий, обеспечивающих постоянный обмен данными, особенно важным становится решение вопросов защиты целостности и неприкосновенности персональных данных. Высокий уровень развития демонстрируют и цифровые технологии, которые применяют хакеры, использующие компьютеры и сетевые ресурсы для осуществления несанкционированного доступа к базам данных для их кражи, повреждения и блокировки. Закономерно, что в этом случае поиск и выбор методов защиты персональных данных должен быть основан, во-первых, на знании типа нуждающихся в защите данных, а во-вторых, на понимании специфики методов противодействия кибератакам. В связи с этим автор видит необходимость в сопоставлении таких технологий защиты персональных данных как шифрование и анонимизация. В статье охарактеризованы виды персональных данных и осуществлена их корреляция с уровнями угрозы, поскольку эти факторы в значительной мере обусловливают выбор методов защиты. Подробно рассмотрены особенности технологий шифрования и анонимизации, и проведено их сравнение по ключевым параметрам. Автор приходит к выводу, что оба метода обеспечивают высокий уровень защиты, обладают широким функционалом и надежностью, хотя каждый из них не лишен недостатков, а потому в каждом конкретном случае выбор должен осуществляться, исходя из целей и задач, а также обязательности соблюдения требований законодательства.*

***Ключевые слова:*** *персональные данные; кибератаки; шифрование; анонимизация; «цифровой след»; уровень угрозы.*

***RUSTAMOVA Lyudmila Rustamovna,***
*Associate Professor of the Department of Information Systems and Technologies of the Ingush State University*

# *ANALYSIS OF METHODS FOR PROTECTING PERSONAL DATA IN THE FACE OF A GROWING THREAT OF CYBER ATTACKS: A COMPARATIVE STUDY OF MODERN ENCRYPTION AND ANONYMIZATION TECHNOLOGIES*

***Annotation.*** *As digital technologies evolve, enabling constant data exchange, protecting the integrity and inviolability of personal data becomes increasingly important. Digital technologies are also highly developed, exploiting computers and network resources to gain unauthorized access to databases for theft, corruption, and blocking. Naturally, in this case, the search for and selection of personal data protection methods should be based, firstly, on knowledge of the type of data requiring protection and, secondly, on an understanding of the specific methods used to counter cyber attacks. Therefore, the author sees the need to compare personal data protection technologies such as encryption and anonymization. The article characterizes the types of personal data and correlates them with threat levels, as these factors significantly determine the choice of protection methods. The features of encryption and anonymization technologies are examined in detail, and their key parameters are compared. The author concludes that both methods provide*

*a high level of protection, have extensive functionality, and are reliable, although each has its drawbacks. Therefore, in each specific case, the choice should be made based on the goals and objectives, as well as the need to comply with legal requirements.*

***Key words:*** *personal data; cyber attacks; encryption; anonymization; digital footprint; threat level.*

В своем историческом развитии человечество прошло несколько глобальных эпох: Античность, Средневековье, Ренессанс, эпоха Великих географических открытий и эпоха Просвещения, промышленная революция, индустриальное и постиндустриальное общество, каждая из которых представляет значимый этап развития цивилизации, характеризующийся принципиальными изменениями всех сфер жизнедеятельности социума. Современный период, начало отсчета которому положила разработка в 1947 г. транзистора, существенно отличающийся от предыдущих временных отрезков, также получил свое название – эпоха глобализации и информации, информационная эра, информационная эпоха. Характерными признаками этой эпохи являются цифровизация, широкие возможности для каждого человека свободно передавать и получать информацию, доступ к различным сегментам информационного поля, что создает положительную картину современного цифрового мира. Но есть и оборотная сторона медали: доступ к данным, включая персональные, может носить несанкционированный характер, делать их мишенью кибератак, приводя к утечке и уязвимости.

На эти особенности информационной эпохи обращают внимание специалисты из Организации объединенных наций, отмечая, что «развитие цифровых технологий может способствовать поддержанию и ускорению достижения основных целей в области устойчивого развития…», и в то же время «технологии могут ставить под угрозу неприкосновенность частной жизни, подрывать безопасность и усугублять неравенство» [1]. Соответственно, возникает необходимость поиска путей использования цифровых технологий и контроля их развития. Учитывая, что цифровизация носит глобальный характер, охватывая практически все сферы человеческой жизнедеятельности, данная статья имеет целью сопоставление лишь некоторых методов защиты персональных данных, а именно технологий шифрования и анонимизации.

Очевидно, что сравнительный анализ указанных технологий требует четкого понимания содержания самих объектов, требующих защиты, и источников угрозы. В первую очередь остановим внимание на том, что относится к персональным данным не только в обиходном, но и в правовом смысле.

Опираясь на прямое значение словосочетания «персональные данные», любой человек безошибочно относит к этой категории фамилию, имя и отчество, адрес проживания и адрес электронной почты, номер телефона, сведения об образовании и ряд других сведений, позволяющих безошибочно идентифицировать конкретного человека. Что касается определения персональных данных в правовом поле, то оно, согласно ст. 3 федерального закона от 27 июля 2006 г. № 152 «О персональных данных», выглядит следующим образом: «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». Раскрывая данную формулировку, приходим к пониманию, что спектр этих данных достаточно широк, хотя непосредственно в законе строго определенный перечень персональных данных отсутствует. Это логично, поскольку суть заключается не в данных как таковых, а в том, что указанная в законе «любая информация» должна позволять установить конкретного человека. Поясним: ни номер телефона, ни адрес электронной почты, ни фотография сами по себе «без привязки» к конкретному человеку не являются персональными данными, тогда как они же в сочетании с ФИО их обладателя становятся таковыми.

Возвращаясь к теме эпох, затронутой в начале статьи, следует отметить, что персональные данные также претерпели изменения в современном информационном мире за счет отнесения к ним «цифровых следов» [2]. Это IP-адрес (internet protocol address), т.е. цифровой идентификатор, являющийся уникальным и присваиваемый каждому конкретному устройству для его идентификации и обмена данными в сети; файлы cookie, т.е. небольшие фрагменты текстовых данных, которые являются своего рода «памятью» для браузера, давая возможность сайтам «узнавать» пользователя; навигационные метки, поскольку именно такие характеристики позволяют идентифицировать человека.

Наконец, говоря о персональных данных, нельзя не акцентировать внимание на разнообразии их видов по степени доступности:

общие или общедоступные персональные данные – включают в себя сведения, которые известны достаточно широкому кругу лиц и размещены на общедоступных ресурсах, например, ФИО, дата рождения, местожительство и адрес электронной почти, номер телефона, место работы или учебы;

специальные персональные данные – без

прямого обращения к человеку, официального запроса в правоохранительные органы, суд или медицинское учреждение невозможно получить сведения о состоянии здоровья, наличии/отсутствии судимости, национальной принадлежности, религиозных взглядах и политических убеждениях;

биометрические персональные данные – сам термин «биометрические» правомерно применять к физиологическим или биологическим характеристикам человека только в том случае, когда их используют для идентификации; за пределами такого применения это просто характеристики человека, включающие в себя отпечатки пальцев и изображение лица, группу крови и информацию о генотипе, запись голоса;

иные персональные данные – могут быть разделены на две подгруппы, к первой из которых относятся обезличенные данные, не позволяющие идентифицировать человека без дополнительных данных (например, в социологических опросах и других аналитических исследованиях используются именно такие данные); вторую группу составляют данные, в отношении которых сам субъект дал разрешение на распространение, в силу чего они могут размещены на сайтах и базах данных [2].

Знание видовой принадлежности персональных данных особенно важно для решения вопросов их защиты. Очевидно, что первый из рассмотренных выше видов персональных данных относится к «наименее чувствительной категории», поскольку такие сведения обеспечивают идентификацию человека с использованием той информации, на размещение которой сам субъект изъявил согласие, той, которая фигурирует в договорах (например, об оказании услуг различного вида), или может быть свободно получена во исполнение закона. Следующая категория персональных данных в значительно большей степени затрагивает личную жизнь человека, его физическое и психическое состояние, убеждения, принадлежность к различным организациям, а потому не может становиться объектом доступа без прямого письменного согласия субъекта; исключение составляют случаи, когда речь идет о защите жизни и здоровья человека. Что касается биометрических данных, то, как было отмечено ранее, в эту категорию попадают физиологические и биологические данные человека в том случае, когда применяются для его идентификации [3]. Поясним: камера, сканирующая лицо человека или отпечатки пальцев, обрабатывает именно биометрические персональные данные, тогда как фотография к этой категории не относится, поскольку известно, кто на ней изображен. Наконец, наиболее свободно осуществляется обработка последнего вида персональных данных (обезличенных и разрешенных самим человеком для распространения). Это не означает отсутствие законодательного регулирования, но при соблюдении анонимности или условий отрытого доступа осуществляется с большими степенями свободы.

Следующий важный аспект, который необходимо прояснить, – это собственно защита персональных данных. Во-первых, от чего их следует защищать, и во-вторых, какие методы могут быть применены для решения этой задачи. В связи с этим следует определиться с основными терминами в данной сфере, одним из которых является понятие «кибератака». Согласно определению, кибератака в широком смысле может быть охарактеризована как преднамеренное действие злоумышленников, которые используют компьютеры и сетевые ресурсы для осуществления несанкционированного доступа к чужим системам и базам данных для их кражи, повреждения или блокировки [4]. Данное определение не единственное, однако вполне достаточное для установления ключевых признаков кибератаки. Если же говорить о кибератаке в узком смысле, применительно к персональным данным, то она представляет собой несанкционированный доступ к личным данным пользователей или конфиденциальной информации, которую аккумулируют различные структуры и организации (учреждения здравоохранения, образования, сферы обслуживания и торговли, работодатели, кадровые агентства).

Цели кибератак вариативны и зависят от того, на какой контент они направлены. В случае кибератаки на персональные данные целью становится нарушение их конфиденциальности, что достигается путем кражи или намеренной утечки личных данных, паролей, информации финансового характера.

Помимо вышеописанного, для выбора эффективных методов защиты требуется знание того, к какому типу относится угроза персональным данным. Всего существует три типа таких угроз, и они определены на законодательном уровне в Постановлении Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Перечислим эти типы по уровню возрастания угрозы:

третий уровень угрозы (самый низкий) – имеет относительно благоприятный характер, поскольку в этом случае затраты на защиту информационных систем персональных данных будут относительно невелики, поскольку в программном обеспечении изначально заложены так называемые «недокументированные возможности» (преднамеренно созданный разработчиками

скрытый функционал), который отсекает возможность получения доступа к персональным данным как со стороны сотрудников (случайно или целенаправленно), так и со стороны третьих лиц;

второй уровень угрозы – характерны для систем, в прикладных программах которых присутствуют скрытые утилиты, позволяющие собирать и систематизировать персональные данные и фактически оставляющие простор для направления таких недокументированных возможностей на несанкционированное внесение изменений в персональные данные или уничтожение информации;

первый уровень угрозы (самый высокий) – указывает на существование аппаратных или программных возможностей в информационной системе персональных данных, которые потенциально могут вызвать неправомерную блокировку, изменение, удаление или утечку персональных данных [5].

И вот здесь напрямую подходим к необходимости выбора конкретных методов защиты персональных данных, среди которых в качестве основных можно выделить шифрование и анонимизацию. Рассмотрим эти методы в сравнительном аспекте.

Шифрование данных определяется как метод защиты информации, предполагающий кодирование (шифрование) данных с использованием криптографических алгоритмов [6]. С чисто утилитарной точки зрения криптографический алгоритм можно представить как набор правил, который позволяет зашифровать информацию так, что она будет доступна для чтения только авторизованным сторонам [7]. Чисто технически это такой алгоритм, который генерирует зашифрованный текст, не доступный для прямого чтения, т.е. требующий для его понимания расшифровки. Заметим, что шифрование является одним из древнейших механизмов защиты информации: достаточно вспомнить «скиталу» в Спарте (V в. до н.э.), шифр Атбаш в Древней Иудее (VI в. до н.э.), шифр Цезаря в Римской империи (I в. до н.э.). На практике этот метод прошел путь от простейших механических подстановок, которые использовались в перечисленных и даже более поздних шифрах, до применения сложных математических алгоритмов, уже недоступных для ручного применения.

Принципиально важным признаком шифрования является то, что данный процесс полностью обратим, поскольку данные остаются доступными для расшифровки при условии, что у авторизованного пользователя имеется специальный ключ или система ключей. Шифрование как метод защиты информации, включая персональные данные, имеет своей целью сохранение конфиденциального характера и целостности информации, осуществление идентификации пользователей, предупреждение перехвата, утечки и несанкционированного доступа [6]. Заметим, что в настоящее время действует стандарт, согласно которому на законодательном уровне (ст. 7 федерального закона № 152 «О персональных данных») закреплена обязательность хранения паролей строго в зашифрованном виде. Шифрование реализуется в разных видах:

–симметричное – в этом случае для шифрования и для последующей расшифровки используется один и тот же ключ; с помощью симметричного шифрования кодируются большие объемы конфиденциальной информации, передаваемые между доверенными лицами;

–асимметричное – для шифрования используется открытый ключ, а для дешифровки – закрытый ключ, которые связаны между собой алгоритмом; этот способ применяется для аутентификации на различных сервисах, при использовании электронной цифровой подписи [6].

Анонимизация данных, как можно заключить из названия, представляет метод (точнее, группу методов) обеспечения сохранности конфиденциальной информации за счет удаления или изменения идентификаторов, позволяющих установить связь конкретных субъектов с относящимися к ним данными. Целью анонимизации является защита персональных данных и предотвращение их утечки в процессе использования, хранения и трансляции [8]. Такой подход позволяет защитить приватность данных, обезличивая их, однако сохраняя их достоверность. Эффективность этого метода позволяет обеспечить соблюдение наиболее строгих правил защиты, а потому анонимизация часто применяется при работе с контактной информацией, финансовыми и медицинскими данными человека. На практике анонимизация исключает возможность идентифицировать конкретного человека, тогда как сами данные сохраняют свою полезность для аналитики (например, при проведении социологических опросов) и тестирования различных систем. Равно как и шифрование, анонимизация данных отвечает требованиям законодательства о защите персональных данных, соответственно, компании, прибегающие к данному методу, действуют в рамках федерального закона № 152 и выполняют обязательства по защите персональных данных. Спектр видов анонимизации достаточно широк:

маскировка – представляет собой такой подход, при котором данные раскрываются с частичной или полной заменой их реальных значений; классический пример – указание номера телефона в виде определенного количества «звездочек» или «крестиков», в качестве других вариантов маскировки могут выступать перетасовка символов, отзеркаливание их порядка, использо-

вание терминов вместо символов, что затрудняет декодирование, а значит и идентификацию носителя данных;

обобщение – в этом случае некоторые данные преднамеренно исключаются для снижения уровня их идентификации и заменяются различными диапазонами; к такому способу часто прибегают для обезличивания данных участников опроса, когда точный возраст участника заменяется указанием возрастной группы;

псевдонимизация или токенизация – основана на замене личных идентификаторов ложными (псевдонимами), но также уникальными идентификаторами, которые называются токенами; статистическая точность данных в этом случае обеспечивается грамотным подходом к выбору токена (например, истинные фамилии заменяются псевдонимами, обладающими такой же частотностью в языке); данные в этом случае по-прежнему пригодны для тестирования, анализа и других действий, однако их конфиденциальность защищена;

изменение или зашумление – реализуется путем внесения незначительных случайных искажений в данные, например, это может быть округление возраста, номера дома и других величин, что позволяет сохранить статистические свойства данных, однако не позволяют установить по ним конкретного человека;

перестановка или перетасовка – представляет собой такую замену, в процессе которой атрибуты набора данных меняются так, что перестают соответствовать исходной информации (например, это может быть переключение столбцов, в которых содержатся легко узнаваемые данные типа даты рождения), не утрачивая своей достоверности;

синтез – алгоритмическая генерация данных, которые не связаны с конкретным человеком или ситуацией, т.е. создается искусственный набор данных, тем самым защищая конфиденциальность оригинальных данных; как правило, используются статистические методы (стандартные отклонения, линейная регрессия, медианные значения) [8].

Заметим, что, несмотря на принципиальные различия между шифрованием и анонимизацией, в обоих случаях точность самих данных сохраняется, кроме того, оба метода обеспечивают высокий уровень защиты.

Сравним теперь преимущества и недостатки каждого из рассмотренных методов защиты персональных данных. Следует заметить, что сравнение требует целый ряд параметров, поскольку очевидно, что даже абсолютно надежный метод защиты может оказаться неприменимым в силу технической сложности или финансовой составляющей. Так по цели применения: шифрование направлено в большей степени на защиту данных при их хранении и передаче, тогда как анонимизация – на обеспечение безопасной работы с данными при анализе, тестировании, обучении. Оба метода обеспечивают обратимость процесса при соблюдении определенных условий – наличия ключа при шифровании и доступа к оригиналу данных при анонимизации [6]. Существенные различия отмечаются по параметру «потребление ресурсов», поскольку шифрование требует их значительного количества, тогда как использование специализированных программных решения в случае анонимизации позволяет потреблять минимальное количество ресурсов.

Основными достоинствами шифрования является высокий уровень защиты в ходе хранения и передачи персональных данных; предотвращение перехвата и несанкционированного доступа; сохранение целостности и надежности данных; защита от их изменения; хорошая сочетаемость с другими методами, позволяющая обеспечить комплексную систему безопасности. Преимущества анонимизации лежат в поле минимизации рисков неправомерного использования данных, включая их инсайдерское применение; высокой эффективности управления данными и согласованности результатов; возможности анализировать большие объемы данных.

Что касается недостатков или, скорее сложностей, связанных с реализацией того или иного метода, то в случае шифрования это:

высокие затраты ресурсов (вычислительных мощностей), что приводит к задержкам при обработке запросов к базам данным, снижению производительности;

значительные финансовые затраты в силу необходимости использования мощных серверов, современного программного обеспечения и квалифицированных специалистов;

сложность управления ключами и утрата доступа к данным при утере ключа;

сложности резервного копирования – восстановление из копий требует больше времени в силу использования дополнительных алгоритмов;

сложности выполнения требований законодательства, поскольку в некоторых случаях для соблюдения требований федерального закона «О персональных данных» разрешено использование только конкретных сертифицированных средств криптографической защиты;

уязвимость системы в момент входа в нее авторизованного пользователя [6].

Использование анонимизации в свою очередь может вызывать: нарушение нормативных требований о получении разрешения от пользователя на сбор личной информации (файлы cookie, IP-адреса); ограничение извлечения значимой информации из результатов; невозмож-

ность использования анонимизированной информации для персонализации взаимодействия с пользователем; риск повторной идентификации за счет восстановления из нескольких наборов данных; необратимый характер ошибок; отсутствие стопроцентной гарантии приватности данных; ложное чувство абсолютной безопасности данных [7].

Подводя итог сопоставлению ключевых параметров шифрования и анонимизации, можно говорить о том, что каждый из них обладает значительным функционалом и надежностью в качестве метода защиты персональных данных. Тем не менее, в каждом конкретном случае требуется учитывать цели и задачи, которые стоят перед организацией, использующей персональные данные; требования законодательства, устанавливающие порядок обезличивания персональных данных и передачи их третьим лицам (федеральный закон № 152 «О персональных данных»); приемлемость объема потребляемых вычислительных ресурсов и допустимость снижения скорости обработки запросов к базам данных. Однако в целом, если речь идет именно о защите от кибератак, обеспечении конфиденциальности и целостности персональных данных при их передаче и хранении, то предпочтительным оказывается применение метода шифрования. социальное, экономическое и политическое развитие.

**Список литературы:**

[1] Последствия использования цифровых технологий // Организация объединенных наций [Электронный ресурс]. URL: https://www.un.org/ru/un75/impact-digital-technologies (дата обращения 29.06.2026).

[2] Что такое персональные данные и как их защищать: полный гид по 152-ФЗ (актуально на 2026 год) // VK Cloud [Электронный ресурс]. URL: https://cloud.vk.com/blog/chto-takoe-personalnye-dannye-ih-hranenie-i-obrabotka/ (дата обращения 29.06.2026).

[3] Что такое персональные данные: особенности работы, виды и хранение // Потенциал [Электронный ресурс]. URL: https://ptl-pro.ru/articles/personalnye-dannye-osobennosti-vidy-i-khranenie/ (дата обращения 30.06.2026).

[4] Комплексный обзор кибератак // Microsoft Security [Электронный ресурс]. URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-a-cyberattack (дата обращения 30.06.2026).

[5] Типы угроз персональных данных // Центр безопасности данных [Электронный ресурс]. URL: https://data-sec.ru/personal-data/threats-types/ (дата обращения 30.06.2026).

[6] Маскирование данных VS шифрование: в чем разница // Гарда [Электронный ресурс]. URL: https://garda.ai/blog/articles/maskirovanie-dannykh-vs-shifrovanie-v-chem-raznitsa (дата обращения 30.06.2026).

[7] Криптографический алгоритм // Лаборатория Касперского [Электронный ресурс]. URL: https://encyclopedia.kaspersky.ru/glossary/cryptographic-algorithm/ (дата обращения 01.07.2026).

[8] Вальцев А. Обезличивание данных: как защитить конфиденциальность пользователей // SF Education [Электронный ресурс]. URL: https://blog.sf.education/obezlichivanie-dannyh/ (дата обращения 01.07.2026).

**References:**

[1] Implications of the use of digital technologies // United Nations [Electronic Resource]. URL: https://www.un.org/ru/un75/impact-digital-technologies (дата обращения 29.06.2026).

[2] What is personal data and how to protect it: a complete 152-FZ guide (relevant for 2026 ) // VK Cloud [Electronic resource]. URL: https://cloud.vk.com/blog/chto-takoe-personalnye-dannye-ih-hranenie-i-obrabotka/ (дата обращения 29.06.2026).

[3] What is personal data: features of work, types and storage // Potential [Electronic resource]. URL: https://ptl-pro.ru/articles/personalnye-dannye-osobennosti-vidy-i-khranenie/ (дата обращения 30.06.2026).

[4] Comprehensive overview of cyber attacks // Microsoft Security [Electronic Resource]. URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-a-cyberattack (дата обращения 30.06.2026).

[5] Types of personal data threats // Data Security Center [Electronic Resource]. URL: https://data-sec.ru/personal-data/threats-types/ (date of contact 30.06.2026).

[6] Data masking VS encryption: what's the difference // Garda [Electronic resource]. URL: https://garda.ai/blog/articles/maskirovanie-dannykh-vs-shifrovanie-v-chem-raznitsa (дата обращения 30.06.2026).

[7] Cryptographic algorithm // Kaspersky Lab [Electronic resource]. URL: https://encyclopedia.kaspersky.ru/glossary/cryptographic-algorithm/ (дата обращения 01.07.2026).

[8] Valtsev A. Depersonalization of data: how to protect user privacy // SF Education [Electronic resource]. URL: https://blog.sf.education/obezlichivanie-dannyh/ (дата обращения 01.07.2026).