УДК 004 **Информационные технологии**

Кадомец Кристина Сергеевна, *магистрант*
ДГТУ, Ростов-на-Дону, РФ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ С ПОМОЩЬЮ ШИФРОВАНИЯ

Аннотация: В эпоху, отмеченную растущей цифровизацией, персональные данные стали ценным активом, и их защита имеет первостепенное значение. Шифрование, как фундаментальный инструмент, играет жизненно важную роль в защите персональных данных от несанкционированного доступа и обеспечении конфиденциальности. В этой статье исследуется концепция защиты персональных данных с помощью шифрования, обсуждается ее важность, преимущества, проблемы и потенциальные изменения в будущем. Шифрование данных является фундаментальным аспектом современной информационной безопасности. Это включает в себя преобразование простых, удобочитаемых данных в нечитаемый формат, чтобы защитить их от несанкционированного доступа. Рассмотрим различные типы методов шифрования данных, включая симметричное шифрование, асимметричное шифрование и хэширование. Каждый метод обладает своими уникальными характеристиками, областями применения и преимуществами, способствующими общей защите конфиденциальных данных.

Ключевые слова: персональные данные, защита данных, информационная безопасность, шифрование.

Abstract: In an era marked by increasing digitalization, personal data has become a valuable asset and its protection is of paramount importance. Encryption, as a fundamental tool, plays a vital role in protecting personal data from unauthorized access and maintaining confidentiality. This article explores the concept of protecting personal data with encryption, discussing its importance, benefits, challenges, and

potential changes in the future. Data encryption is a fundamental aspect of modern information security. This includes converting simple, human-readable data into an unreadable format to protect it from unauthorized access. Let's look at different types of data encryption methods, including symmetric encryption, asymmetric encryption, and hashing. Each method has its own unique characteristics, applications and benefits that contribute to the overall protection of sensitive data.

Key words: personal data, data protection, information security, encryption.

Основная часть

1. Понимание шифрования: Шифрование - это процесс преобразования информации открытого текста в нечитаемую форму, известную как зашифрованный текст, с использованием криптографических алгоритмов. Зашифрованный текст может быть расшифрован в его первоначальном виде только с помощью уникального ключа шифрования. Шифрование обеспечивает безопасный канал связи и хранения персональных данных.

2. Важность защиты персональных данных: Персональные данные охватывают широкий спектр конфиденциальной информации, включая финансовые данные, медицинские записи, активность в социальных сетях и многое другое. Защита персональных данных имеет решающее значение для предотвращения кражи личных данных, мошенничества, несанкционированной слежки и других киберпреступлений. Шифрование действует как защитный экран, снижая риски, связанные с утечкой данных и несанкционированным доступом.

3. Преимущества шифрования для защиты персональных данных: a. Конфиденциальность: Шифрование гарантирует, что персональные данные остаются конфиденциальными и доступны только уполномоченным физическим или юридическим лицам. Даже в случае перехвата зашифрованные данные не имеют смысла без ключа шифрования. b. Целостность: Методы шифрования также гарантируют целостность персональных данных. Любое изменение или фальсификация зашифрованных данных делает их нечитаемыми, тем самым

сохраняя целостность и достоверность данных. c. Аутентификация: Шифрование может использоваться для проверки подлинности персональных данных с помощью цифровых подписей или сертификатов. Это позволяет пользователям проверять источник и целостность получаемых ими данных. d. Соблюдение нормативных требований: Шифрование играет жизненно важную роль в соблюдении правил защиты данных и законов о конфиденциальности, таких как Общие правила защиты данных (GDPR) и Калифорнийский закон о защите прав потребителей (CCPA).

4. Проблемы и ограничения шифрования: a. Управление ключами: Эффективное шифрование зависит от надежных методов управления ключами. Защита ключей шифрования и обеспечение их доступности в случае необходимости может быть сложной задачей, особенно в крупномасштабных системах или при работе с несколькими устройствами. b. Удобство использования и доступность: Шифрование иногда может усложнять работу пользователей, особенно для лиц, не обладающих техническими знаниями. Достижение баланса между надежным шифрованием и удобными интерфейсами остается сложной задачей. c. Бэкдоры шифрования: балансирование интересов конфиденциальности и безопасности с точки зрения доступа правоохранительных органов и правительства к зашифрованным данным было спорным вопросом. Дебаты вокруг бэкдоров для шифрования подчеркивают необходимость поиска равновесия между личной неприкосновенностью частной жизни и общественной безопасностью.

5. Будущие разработки в области защиты персональных данных: a. Квантово-стойкое шифрование: По мере развития квантовых вычислений возникает потребность в алгоритмах шифрования, устойчивых к квантовым атакам. Исследователи изучают постквантовую криптографию для разработки надежных методов шифрования. б. Гомоморфное шифрование: Гомоморфное шифрование позволяет выполнять вычисления с зашифрованными данными без их расшифровки. Эта новая технология обещает обеспечить безопасный анализ данных при сохранении конфиденциальности. c. Многофакторная

аутентификация: Сочетание шифрования с многофакторной аутентификацией повышает защиту персональных данных. Использование биометрических данных, аппаратных токенов и других факторов аутентификации повышает безопасность зашифрованных данных.

Виды шифрования

1. Симметричное шифрование: Симметричное шифрование, также известное как шифрование с секретным ключом или обычное шифрование, использует один секретный ключ как для процессов шифрования, так и для дешифрования. Один и тот же ключ используется как отправителем, так и получателем для преобразования открытого текста в зашифрованный и наоборот. Ключ хранится в тайне и должен быть надежно передан обменивающимися данными сторонами.

Преимущества симметричного шифрования:

a. Скорость и эффективность: Алгоритмы симметричного шифрования эффективны в вычислительном отношении, что позволяет осуществлять высокоскоростные процессы шифрования и дешифрования.

b. Простота: Симметричное шифрование относительно простое и требует меньшего количества вычислительных операций по сравнению с асимметричным шифрованием.

c. Универсальность: Симметричное шифрование хорошо подходит для массовых данных шифрование, например, шифрование файлов или целых жестких дисков.

Области применения симметричного шифрования: a. Защищенная связь: Симметричное шифрование обычно используется для защиты каналов связи, таких как виртуальные частные сети (VPN), где данные должны быть защищены во время передачи. b. Хранение данных: Оно используется для шифрования конфиденциальных данных, хранящихся на локальных устройствах, облачных серверах или других устройствах, которые могут быть использованы для передачи конфиденциальных данных. носитель информации.

2. Асимметричное шифрование: Асимметричное шифрование, также

известное как шифрование с открытым ключом, использует пару математически связанных ключей: открытый ключ и закрытый ключ. Открытый ключ распространяется свободно, в то время как закрытый ключ остается секретным. Отправитель использует открытый ключ получателя для шифрования сообщения, а получатель расшифровывает его с помощью своего закрытого ключа.

Преимущества асимметричного шифрования:

a. Распределение ключей: Асимметричное шифрование устраняет необходимость в безопасном обмене ключами, поскольку открытый ключ может быть свободно передан.

b. Аутентификация и неотрицание: Асимметричное шифрование позволяет использовать цифровые подписи, которые обеспечивают аутентификацию и гарантируют, что отправитель не сможет отрицать происхождение своего сообщения.

c. Защищенный обмен ключами: Это позволяет безопасно устанавливать общие секретные ключи для симметричного шифрования между сторонами, которые никогда ранее не общались.

Области применения асимметричного шифрования:

a. Защищенная электронная почта: Асимметричное шифрование обычно используется для шифрования сообщений электронной почты и вложений, обеспечивая конфиденциальность и целостность.

b. Защищенная веб-связь: Асимметричное шифрование используется в защищенных протоколах, таких как Transport Layer Security (TLS), для установления защищенных соединений для онлайн-транзакций и передачи конфиденциальных данных.

3. Хеширование: Хеширование - это метод одностороннего шифрования, который преобразует данные в строку символов фиксированной длины, известную как хэш-значение или дайджест. Это необратимо, что означает, что исходные данные не могут быть извлечены из хэш-значения. Хэш-функции являются детерминированными, что означает, что один и тот же ввод всегда

будет выдавать одно и то же хэш-значение.

Преимущества хеширования:

a. Целостность данных: Хеширование используется для проверки целостности данных. Если исходные данные будут изменены, значение хэша изменится, указывая на подделку.

b. Хранение паролей: функции хэширования обычно используются для безопасного хранения паролей путем их хэширования и сравнения значений хэша в целях аутентификации.

c. Снятие отпечатков пальцев с данных: Хэширование используется для проверки целостности файлов и цифровых подписей, позволяя пользователям для проверки подлинности файлов.

Области применения хеширования:

a. Проверка целостности данных: Хеширование используется для проверки целостности данных во время передачи или хранения, гарантируя, что полученные данные соответствуют оригиналу.

b. Защита паролем: Хеширование используется в системах хранения паролей для защиты пользовательских паролей и предотвращения несанкционированного доступа к учетным записям пользователей.

c. Цифровая криминалистика: Хэширование используется для идентификации уникальных файлов или блоков данных, что обеспечивает эффективный анализ данных и идентификацию при судебно-медицинских расследованиях.

Вывод: Защита персональных данных является важнейшей задачей в эпоху цифровых технологий, а шифрование служит мощным инструментом защиты конфиденциальной информации. Его роль в обеспечении конфиденциальности, целостности, аутентификации и соответствия требованиям невозможно переоценить. Хотя шифрование сталкивается с проблемами в области управления ключами, удобства использования и бэкдоров шифрования, текущие разработки в области квантово-стойкого шифрования, гомоморфного шифрования и многофакторной аутентификации обещают

будущее. По мере развития технологий непрерывное совершенствование методов шифрования будет играть жизненно важную роль в сохранении личной конфиденциальности и безопасности данных.

Библиографический список:

1. Конституция Российской Федерации от 12дскабря 1993 г.: по сост. на 21 июля 2014 г. Н Собрание законодательства Российской Федерации. — 2014. — № 31. — Ст. 4398.
2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. И Собрание законодательства Российской Федерации. — 2014. — № 5. — Ст. 419.
3. Конвенция Содружества Независимых Государств о правах и основных свободах человека от 26 мая 1995 г. // Собрание законодательства Российской Федерации. — 1999.- № 13.-Ст. 1489.
4. Трудовой кодекс Российской Федерации от 30 ноября 2001 N 197-ФЗ: по сост. на 1 июня 2019 г.// Собрание законодательства Российской Федерации. — 2002. — № 1. — Ст. 3.
5. Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 г. № 14-ФЗ: по сост. на 1 июня 2019 г. // Собрание законодательства Российской Федерации. — 1996. — № 5. — Ст. 410.
6. Об оперативной и розыскной деятельности: федеральный закон от 12.08.1995 N 144-ФЗ по сост. на 29 нюня 2018 г. // Собрание законодательства Российской Федерации. — 1995. — № 33. — Ст. 3349.
7. Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования: федеральный закон от 01 апреля 1996 г. № 27-ФЗ по сост. на 1 декабря 2018 г. // Собрание законодательства Российской Федерации. — 1996- № 14. — Ст. 1401.
8. О персональных данных: федеральный закон от 27 июля 2006 г. N 152-ФЗ // Собрание законодательства Российской Федерации. — 2006. — № 31 (часть I). — Ст. 3451.

9. Бачило, ИЛ. Информационное право РФ: Учебник для вузов / И.Л. Бачило. — М.: Издательство Юрайт. 2016.- 522 с.

10. Бачило, И.Л. Персональные данные в структуре информационных ресурсов. Основы правового регулирования /И.Л. Бачило, Л.А. Сергиенко, Б.А. Кристальный., А.Г. Арешев // Информационное право. — 2016. — N 3.

11. Бондаренко, Э.Н. Конфиденциальная информация в трудовых отношениях. / Э.Н. Бондаренко, Иванов ДВ. — СПб.; Издательство «Юридический центр-Пресс». — 2014.

12. Болик, В.Н. О правомерности законодательных ограничений конституционного права на неприкосновенность частной жизни / В.Н. Болик., А.М. Туркиашвили А.М. // Законы России: опыт, анализ, практика. — 2015. — N 7. С. 78 — 84.

13. Бондаренко, К.А. Взаимосвязь признаков индивидуального трудового договора и особенностей договорного регулирования трудовых отношений / К.А. Бондаренко // Трудовое право в России и за рубежом. 2015. — № 3. — С. 23 — 27.

14. Буркова, А.Ю. Локализация баз данных на территории Российской Федерации: первые толкования // Законодательство и экономика. 2015.- № 9.- С. 59 — 64.