3. Разработка внутренних регламентов и инструкций по работе с информацией.
4. Повышение квалификации сотрудников и обучение работе с современными ИТ-решениями.
5. Применение технологий искусственного интеллекта для анализа и прогнозирования данных [4].

Заключение. Информационные ресурсы, будучи стратегическим активом организации, играют ключевую роль в ее способности эффективно управлять бизнес-процессами, принимать обоснованные решения и уверенно развиваться в условиях динамичной цифровой экономики. Однако управление этими ресурсами сопряжено с рядом серьезных вызовов, включая устаревание и дублирование данных, что снижает их достоверность и ценность. Угрозы информационной безопасности, такие как утечки конфиденциальной информации и кибератаки, представляют серьезную опасность для непрерывности бизнеса и репутации организации. Кроме того, отсутствие четких регламентов и стандартов работы с информацией, а также недостаточный уровень компетенций персонала, снижают эффективность использования информационных ресурсов в целом. Решение этих проблем требует комплексного подхода, включающего внедрение современных информационных систем, обеспечивающих эффективную обработку и анализ данных, разработку нормативной базы, регламентирующей все аспекты работы с информацией, и систематическое повышение уровня компетенций сотрудников в области информационных технологий и безопасности. Только таким образом организация сможет в полной мере использовать потенциал своих информационных ресурсов для достижения стратегических целей и укрепления конкурентных позиций на рынке.

Список цитируемых источников

1. *Беляев, В. И.* Информационные ресурсы и их использование в управлении / В. И. Беляев. — М. : Инфра-М, 2021. — 312 с
2. Национальный статистический комитет Республики Беларусь. — URL: https://www.belstat.gov.by/ (дата обращения: 10.09.2025).
3. *Лебедев, А. Н.* Информационный менеджмент / А. Н. Лебедев. — СПб. : Питер, 2020. — 368 с.
4. SAP. Официальный сайт ERP-систем SAP. — URL: https://www.sap.com/ (дата обращения: 10.09.2025).

УДК 004.8

Е. Ю. Чембрович, Е. Э. Шельпук
Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь

МЕТРОЛОГИЯ, СЕРТИФИКАЦИЯ И СТАНДАРТИЗАЦИЯ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

Введение. Современные информационные технологии являются фундаментом цифровой экономики. Их эффективность и надежность во многом зависят от точности измерений параметров, соблюдения международных и национальных стандартов, а также подтверждения качества продукции и услуг. Поэтому в информационных технологиях ключевую роль играют три взаимосвязанных направления — метрология, стандартизация и сертификация [1].

Основная часть. Метрология обеспечивает точность и воспроизводимость измерений характеристик оборудования и программного обеспечения. В условиях цифровой трансформации именно корректные измерения позволяют объективно сравнивать производительность различных систем и выбирать оптимальные решения.

Основные направления метрологии в ИТ включают (таблица 1):

- производительность вычислительных систем;
- параметры сетей связи (пропускная способность, задержка, вероятность ошибок);
- качество программного обеспечения (время отклика, надежность, уровень отказов);
- измерение параметров кибербезопасности (время обнаружения угроз, уровень защищенности) [2].

Таблица 1— Примеры применения метрологии в информационных технологиях

Область	Измеряемые параметры	Цель
Вычислительные системы	скорость обработки данных, объем памяти	оценка производительности
Сети связи	задержка, пропускная способность, уровень ошибок	обеспечение надежности передачи данных
Программное обеспечение	время отклика, устойчивость, надежность	повышение качества ПО
Кибербезопасность	время отклика на угрозы, уровень защиты	оценка безопасности системы

Примечание — Источник [3].

Стандартизация направлена на установление единых требований к системам и их компонентам. Она способствует развитию совместимости и интероперабельности систем, а также играет важную роль в обеспечении безопасности данных и надежности ИТ-инфраструктуры.

Ключевые цели стандартизации:

– совместимость и интероперабельность;
– повышение качества и надежности;
– информационная безопасность;
– гармонизация международных и национальных требований [4].

Примеры международных стандартов:
– ISO/IEC 27001 — управление информационной безопасностью;
– ISO/IEC 25010 — модель качества ПО;
– IEEE 802.11 — стандарты беспроводных сетей (Wi-Fi);
– ISO/IEC 12207 — процессы жизненного цикла программного обеспечения [5].

Стандарты разрабатываются с участием международных экспертов, что обеспечивает учет различных точек зрения и интересов. Они также оказывают влияние на законодательство, создавая основу для нормативных требований и повышения уровня соблюдения правил в индустрии.

Сертификация — это подтверждение соответствия продукции или услуг установленным стандартам. В ИТ-сфере сертификация выполняет роль гарантии качества и доверия со стороны пользователей.

Основные направления сертификации (таблица 2):
– оценка безопасности информационных систем;
– подтверждение качества программного обеспечения;
– сертификация средств защиты информации (например, Common Criteria);
– сертификация соответствия международным стандартам ISO/IEC [6].

Таблица 2 — Примеры элементов методологии, стандартизации и сертификации в ИТ

Элемент	Основная функция	Пример в ИТ
Метрология	Измерение параметров и характеристик	Скорость передачи данных, надежность ПО
Стандартизация	Установление единых требований и правил	ISO/IEC 27001, IEEE 802.11
Сертификация	Подтверждение соответствия стандартам	Common Criteria, сертификация ПО

Примечание — Источник [7].

Совокупность метрологии, стандартизации и сертификации формирует основу доверия к цифровым системам. Эти процессы обеспечивают конкурентоспособность продукции и услуг на международном рынке, а также позволяют государствам развивать электронное правительство, кибербезопасность и инновационные отрасли.

В практической деятельности организаций метрология, стандартизация и сертификация позволяют не только гарантировать качество продукции, но и обеспечивают доверие со стороны партнеров и заказчиков. Например, в сфере облачных технологий сертификация по международным стандартам ISO/IEC 27001 является необходимым условием для выхода на зарубежные рынки. В свою очередь, стандартизация протоколов связи позволяет создавать совместимые устройства, а метрологические исследования обеспечивают устойчивую работу аппаратных и программных решений.

Особое значение данные процессы приобретают в условиях развития киберфизических систем, Интернета вещей (IoT) и искусственного интеллекта. Без единых стандартов и объективных измерений невозможно обеспечить масштабируемость, совместимость и безопасность таких технологий [8].

Заключение. Внедрение комплексного подхода к метрологии, стандартизации и сертификации в информационных технологиях обеспечивает формирование цифровой экосистемы, способной гарантировать качество, надежность и безопасность. В условиях цифровизации экономики данные процессы становятся неотъемлемой частью стратегий развития организаций и государств. Современные вызовы — киберугрозы, интероперабельность устройств, трансграничная обработка данных — усиливают значение этих направлений.

Таким образом, можно заключить, что метрология обеспечивает объективность измерений, стандартизация создает правила взаимодействия и совместимости, а сертификация формирует доверие. Только их совместное применение позволяет строить устойчивые и конкурентоспособные цифровые системы.

Список цитируемых источников

1. BIPM. Metrology in the Digital Age. — URL: https://www.bipm.org/en/metrology/metrology-in-digital-age (дата обращения: 10.09.2025).
2. National Institute of Standards and Technology (NIST). Performance Measurement Guide for Information Security (NIST SP 800-55). — URL: https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final (дата обращения: 10.09.2025).
3. ISO/IEC TR 9126. Software engineering — Product quality. — URL: https://www.iso.org/standard/22749.html (дата обращения: 10.09.2025).
4. International Organization for Standardization (ISO). Benefits of standards. — URL: https://www.iso.org/benefits-of-standards.html (дата обращения: 10.09.2025).
5. ISO/IEC 27001:2013 Information security management systems; ISO/IEC 25010:2011 Systems and software quality models; IEEE 802.11 Wireless LAN standards; ISO/IEC/IEEE 12207:2017 Software life cycle processes. — URL: https://www.iso.org (дата обращения: 10.09.2025).
6. Common Criteria Portal. Common Criteria for Information Technology Security Evaluation. — URL: https://www.commoncriteriaportal.org (дата обращения: 10.09.2025).
7. ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories. — URL: https://www.iso.org/standard/66912.html (дата обращения: 10.09.2025).

8. United Nations Economic Commission for Europe (UNECE); Bureau International des Poids et Mesures (BIPM). Role of Metrology, Standards and Conformity Assessment in Global Quality Infrastructure. — URL: https://unece.org/trade/wp6 (дата обращения: 10.09.2025).

УДК 004.056.55:004.272.2

И. С. Чередайло
Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь

Научный руководитель А. И. Калько

МНОГОПОТОЧНАЯ БРУТФОРС-ПОДБОРКА ПАРОЛЕЙ: ВЛИЯНИЕ ДЛИНЫ КЛЮЧА И ЧИСЛА ПОТОКОВ

Введение. В современном цифровом пространстве пароли остаются основным механизмом защиты информации, от учётных записей в интернете до конфиденциальных документов Microsoft Office. С развитием вычислительных платформ и распространением многопоточности брутфорс-подбор однажды простых паролей может быть выполнен в считанные минуты, что существенно повышает риски несанкционированного доступа и кражи данных. Оценка времени, необходимого для полного перебора ключевого пространства, позволяет настроить требования к длине и сложности пароля, а также определить слабые места в используемом оборудовании [1].

В рамках исследования ставились следующие задачи:

1. Получить экспериментальные данные по времени перебора паролей длиной от 3 до 6 символов на ПК уровня Intel Core i5-10400 при 1, 2, 4 и 8 потоках.

2. Экстраполировать различные сценарии многопоточности на более длинные пароли (8, 10, 12, 16 и 20 символов) и оценить теоретическое время полного перебора.

3. Проанализировать зависимость ускорения от числа потоков, нагрузку на процессор и объём потребляемой оперативной памяти для всех сценариев.

Основная часть. Брутфорс — универсальный метод подбора паролей, основанный на полном переборе всех возможных комбинаций символов из заданного алфавита. При этом любая потенциальная строка формируется последовательно и проверяется на совпадение с заданным ключом до тех пор, пока подбор не завершится успехом или пока не будут исчерпаны все варианты.

Многопоточность — способ организации выполнения программы, при котором её алгоритм разделяется на несколько независимых или слабо связанных «потоков» (threads). Каждый поток работает в своём контексте, выполняя часть общего объёма задач параллельно с другими. Это позволяет задействовать несколько ядер процессора и ускорять обработку больших наборов данных за счёт одновременного выполнения нескольких последовательностей инструкций [2].

Экстраполяция — метод прогнозирования значений за пределами области экспериментальных данных на основе построенной модели. В контексте данного исследования экстраполяция используется для оценки времени перебора длинных паролей ($L \geq 8$), не замеренных напрямую.

Теоретические основы:

При алфавите из N символов (латинские прописные буквы и цифры, $N = 36$) объём пространства ключей длины L выражается формулой: $V = 36^L$.

Последовательное время перебора пропорционально V, а при T потоках в идеале сокращается примерно в T раз. Фактическое ускорение ниже из-за:

– накладных расходов на создание и завершение потоков;
– дисбаланса задач между потоками;
– переключений контекста ОС;
– конкуренции за кэш и подсистему памяти.

Аппаратная платформа и методика. Эксперименты проводились на следующем оборудовании:

– Процессор: Intel Core i5-10400 (6 физических ядер / 12 логических потоков, 2,9 ГГц, Turbo Boost до 4,3 ГГц).
– Оперативная память: 16 ГБ DDR4-2666.
– Накопитель: SSD Samsung 970 EVO NVMe 500 ГБ.
– Операционная система: Windows 10 Pro (64-bit).
– Среда разработки: Delphi 10.4 Sydney, Win64.

Алфавит: 26 латинских прописных букв + 10 цифр (0–9) = 36 символов. Сценарии многопоточности: 1, 2, 4, 8 потоков. Длины паролей L: 3, 4, 5, 6 (эксперимент), 8, 10, 12, 16, 20 (теоретическая экстраполяция).

Методика:

1. Каждый эксперимент повторялся трижды, результаты усреднялись.
2. Измерялись:
1. Полное время перебора (в секундах или часах);