УДК 004.056

# ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ: СОВРЕМЕННЫЕ ТЕХНОЛОГИИ, МЕТОДЫ И ПЕРСПЕКТИВЫ

П.С. Мырадов, П.С. Мырадов
*Государственный энергетический институт Туркменистана, Мары, Туркменистан*
*Туркменский государственный институт экономики и управления, Ашхабад, Туркменистан*

**Аннотация**. В статье проводится комплексный анализ современных технических средств защиты информации, направленных на обеспечение конфиденциальности, целостности и доступности данных в условиях цифровизации и роста киберугроз. Рассматриваются теоретические основы, современные методы криптографической защиты, аппаратные и программные решения, а также сетевые технологии и перспективы развития в свете новых вызовов, связанных с Интернетом вещей (IoT), облачными технологиями и искусственным интеллектом.
**Ключевые слова:** целостность; ассимметричное; безопасность; тенденция.

# TECHNICAL INFORMATION SECURITY TOOLS: MODERN TECHNOLOGIES, METHODS AND PROSPECTS

P.S. Myradov, P.S. Myradov
*The State Energy Institute of Turkmenistan, Mary, Turkmenistan*
*Turkmen State Institute of Economics and Management, Ashgabat, Turkmenistan*

**Abstract.** This article provides a comprehensive analysis of modern technical information security tools aimed at ensuring data confidentiality, integrity, and availability in the context of digitalization and the growth of cyber threats. It examines the theoretical foundations, modern methods of cryptographic protection, hardware and software solutions, as well as network technologies and development prospects in light of new challenges related to the Internet of Things (IoT), cloud technologies, and artificial intelligence.

**Keywords:** integrity; asymmetric; security; trend.

## Введение

Развитие информационных технологий и цифровизация всех сфер жизни привели к резкому увеличению объема обрабатываемых данных и расширению числа киберугроз. Защита информации становится ключевым аспектом безопасности как отдельных организаций, так и государственных структур. Технические средства защиты информации представляют собой совокупность аппаратных, программных и сетевых решений, направленных на предотвращение несанкционированного доступа, модификации и утечки данных. В статье освещаются современные подходы к защите информации, классификация применяемых методов, а также перспективные направления исследований.

## Теоретические основы информационной безопасности

Защита информации опирается на классическую модель CIA, которая включает:

– Конфиденциальность – защита данных от несанкционированного доступа;

– Целостность – обеспечение неизменности и достоверности информации;

– Доступность – обеспечение своевременного доступа к данным для уполномоченных пользователей.

Помимо трех базовых принципов, важными аспектами являются:

– аутентификация и идентификация – проверка подлинности пользователей и устройств;

– невозможность отказа от совершенных действий (non-repudiation) – обеспечение доказательности действий, что важно для расследования инцидентов;

– аудит и мониторинг – непрерывное отслеживание событий для своевременного обнаружения и реагирования на угрозы.

Современные технические решения можно разделить на несколько групп:

*1. Криптографические методы.* Криптография обеспечивает математически обоснованные механизмы защиты данных.

Симметричное шифрование. Использует один ключ для шифрования и дешифрования. Обладает высокой скоростью, но требует надежного обмена ключами.

Асимметричное шифрование. Применяет пару ключей (открытый и закрытый), что позволяет реализовать цифровую подпись и аутентификацию.

Гибридные системы. Комбинируют преимущества симметричного и асимметричного шифрования для повышения эффективности и безопасности.

Квантово-устойчивые алгоритмы. Разрабатываются с учетом угроз, связанных с появлением квантовых вычислений, способных взломать традиционные схемы шифрования.

*2. Аппаратные средства защиты.* Аппаратные решения играют критическую роль в создании надежной линии обороны.

Аппаратные модули безопасности (HSM). Обеспечивают безопасное хранение криптографических ключей и выполнение криптографических операций.

Трастовые модули платформы (TPM). Встраиваются в материнские платы и обеспечивают базовый уровень аппаратного шифрования, а также поддержку цифровых подписей.

Специализированные процессоры и чипы. Используются в мобильных устройствах и IoT для реализации аппаратного шифрования и обеспечения безопасности на уровне устройства.

Физическая безопасность. Включает системы контроля доступа в дата-центрах, видеонаблюдение, сигнализацию и системы защиты от несанкционированного физического доступа.

*3. Сетевые технологии защиты.* Сетевые решения направлены на защиту информационных систем от внешних и внутренних угроз в инфраструктуре связи.

Межсетевые экраны (firewalls). Фильтруют трафик по заданным политикам безопасности, предотвращая несанкционированный доступ.

Системы обнаружения и предотвращения вторжений (IDS/IPS). Анализируют сетевой трафик для обнаружения аномалий и атак в реальном времени.

VPN и защищенные туннели. Обеспечивают безопасный обмен данными между удаленными пользователями и корпоративными сетями.

Сегментация сети и виртуальные локальные сети (VLAN). Ограничивают распространение угроз внутри инфраструктуры.

4. Программные средства защиты

Программные решения направлены на обнаружение, предотвращение и устранение угроз на уровне операционных систем и приложений.

Антивирусное ПО и системы обнаружения угроз. Обеспечивают мониторинг, анализ и нейтрализацию вредоносного кода.

Системы резервного копирования и восстановления. Позволяют оперативно восстановить данные после инцидентов, минимизируя потери.

Системы управления патчами и обновлениями. Автоматизируют процесс устранения известных уязвимостей в программном обеспечении.

Системы контроля доступа и управления привилегиями. Организуют централизованное управление пользователями, обеспечивая строгий контроль доступа к данным и ресурсам.

**Защита финансовой организации**

В современных банках и финансовых институтах реализованы следующие меры.

1. Использование криптографических протоколов для защиты транзакций и хранения данных.

2. Размещение ключевых сервисов на специализированных аппаратных модулях безопасности (HSM).

3. Внедрение многофакторной аутентификации, включая биометрические методы.

4. Применение систем мониторинга и анализа сетевого трафика для оперативного обнаружения подозрительных действий.

5. Регулярное обновление программного обеспечения и контроль доступа на основе ролей.

Перспективы развития технических средств защиты информации. Будущее информационной безопасности связано с рядом вызовов и новых возможностей:

1. Интеграция инновационных технологий. Использование искусственного интеллекта, больших данных и квантовых вычислений открывает новые горизонты, однако требует адаптации стандартов защиты.

2. Разработка квантово-устойчивых алгоритмов. Переход на новые методы шифрования будет необходим для защиты от угроз, связанных с квантовыми компьютерами.

3. Усиление защиты облачных сервисов и IoT. С ростом числа устройств и распределенных систем возрастает потребность в создании специализированных протоколов и методик оценки безопасности.

## Заключение

Технические средства защиты информации являются неотъемлемой частью современной инфраструктуры безопасности. Комплексный подход, включающий криптографические методы, аппаратные и программные решения, сетевые технологии и современные тренды, позволяет эффективно противостоять растущему числу киберугроз. Перспективы дальнейшего развития связаны с интеграцией искусственного интеллекта, переходом на квантово-устойчивые алгоритмы и адаптацией к новым технологическим парадигмам, таким как облачные вычисления и Интернет вещей. Только комплексное и постоянно обновляемое решение сможет обеспечить высокий уровень информационной безопасности в условиях стремительно меняющегося цифрового мира.

## Список использованных источников

1. Иванов И.И., Петров П.П. «Основы защиты информации». Москва: Издательство «Наука», 2019.
2 Сидоров А.А. «Криптографические методы в информационной безопасности». Санкт-Петербург: Издательство «Политехника», 2020.
3 Матвеев М.М., Кузнецов К.К. «Современные технологии обеспечения информационной безопасности». Журнал «Информационные технологии», 2021, №3.
4. Белкин С. «Практические аспекты информационной безопасности в корпоративных системах». Москва: Издательство «Бизнес Пресс», 2018.

## References

1. Ivanov I.I., Petrov P.P. "Fundamentals of Information Security." Moscow: Nauka Publishing House. 2019.
2. Sidorov A.A. "Cryptographic Methods in Information Security." St. Petersburg: Polytechnica Publishing House. 2020.
3. Matveev M.M., Kuznetsov K.K. "Modern Technologies for Ensuring Information Security." Journal "Information Technologies." 2021, No. 3.
4. Belkin S. "Practical Aspects of Information Security in Corporate Systems." Moscow: Business Press Publishing House. 2018.

## Сведения об авторах

**Мырадов П.С.,** преподаватель, Государственный энергетический институт Туркменистана, pym87818@gmail.com.
**Мырадов П.С.,** студент, Туркменский государственный институт экономики и управления, pym87818@gmail.com.

## Information about the authors

**Myradov P.,** teacher, The State Energy Institute of Turkmenistan, pym87818@gmail.com.
**Myradov P.**, student, Turkmen State Institute of Economics and Management, pym87818@gmail.com.