**Исследование методов обеспечения конфиденциальности и защиты данных в встраиваемых системах**

## Тезисы исследования

Представляю Вашему вниманию тезисы научно-исследовательской работы, посвящённой актуальной проблеме обеспечения конфиденциальности и защиты данных в современных встраиваемых системах. В условиях стремительной интеграции встраиваемых устройств в глобальное информационное пространство, что формирует основу Интернета вещей (IoT), критической инфраструктуры и интеллектуальных систем, наблюдается значительное расширение потенциальных векторов атак и повышение рисков реализации киберугроз. Эти угрозы могут привести не только к утечке данных, но и к катастрофическим физическим последствиям, что подтверждается инцидентами, такими как Stuxnet.

Ключевым аспектом исследования является фундаментальное противоречие между ограниченными ресурсами встраиваемых систем (вычислительная мощность, память, энергопотребление) и растущими требованиями к уровню защиты данных. Традиционные методы обеспечения безопасности, эффективные в серверных и настольных средах, зачастую оказываются неприменимыми или недостаточно эффективными в условиях встраиваемых систем.

В рамках исследования проведён всесторонний анализ современных методов защиты данных, которые классифицированы на аппаратные и программные. Аппаратные методы защиты, такие как использование доверенных платформенных модулей (TPM), аппаратных модулей безопасности (HSM), средств защиты от побочных электромагнитных излучений (ПЭМИН) и биометрических сканеров, обеспечивают физическую защиту, высокую производительность криптографических операций и устойчивость к физическому вмешательству. Однако внедрение этих методов сопряжено с высокой стоимостью, увеличением энергопотребления и ограниченной гибкостью реализации.

Программные методы защиты, включая легковесные криптографические алгоритмы (AES, ECC), адаптированные протоколы защищённой связи (TLS/DTLS), механизмы контроля доступа и обеспечения целостности данных (безопасная загрузка, IMA), характеризуются низкой стоимостью, высокой гибкостью и возможностью обновления. Основной недостаток этих методов заключается в их уязвимости к программным атакам и повышенных требованиях к вычислительным ресурсам.

Сравнительный анализ показал, что ни один из рассмотренных подходов не является универсальным решением. В связи с этим центральным результатом работы является научное обоснование и разработка концепции адаптивной комбинированной системы защиты данных, сочетающей аппаратные и программные методы. Данная концепция предполагает создание многоуровневой архитектуры, которая динамически конфигурирует параметры безопасности на основе оценки текущего контекста работы системы, уровня угроз и доступных ресурсов. Такой подход позволяет достичь синергетического эффекта, оптимизируя баланс между безопасностью, производительностью и стоимостью.

В качестве практической реализации предложена архитектурная модель для типичного IoT-устройства, включающая микроконтроллер с поддержкой технологии TrustZone, аппаратный модуль генерации случайных чисел (HRNG), легковесные криптографические протоколы и систему удалённой аттестации целостности. Эффективность предложенной системы формализована через целевую функцию, максимизирующую общий уровень защиты при заданных ограничениях.

Проведённое исследование вносит значительный вклад в область кибербезопасности встраиваемых систем, предлагая систематизированный подход к выбору и проектированию механизмов защиты данных. Перспективными направлениями дальнейших исследований являются разработка более точных моделей оценки угроз в реальном времени, создание стандартизированных API для адаптивных систем безопасности и углублённое изучение устойчивости предложенных решений к квантовым атакам. Результаты работы могут найти применение при проектировании нового поколения безопасных и киберустойчивых встраиваемых систем, предназначенных для использования в критически важных областях.

**Автор:** Рассказова Анна Павловна  
**Образовательная автономная некоммерческая организация высшего образования «МОСКОВСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ», факультет информационных технологий, Направление подготовки: 09.04.03 Прикладная информатика**  
**Дата:** 2025 год