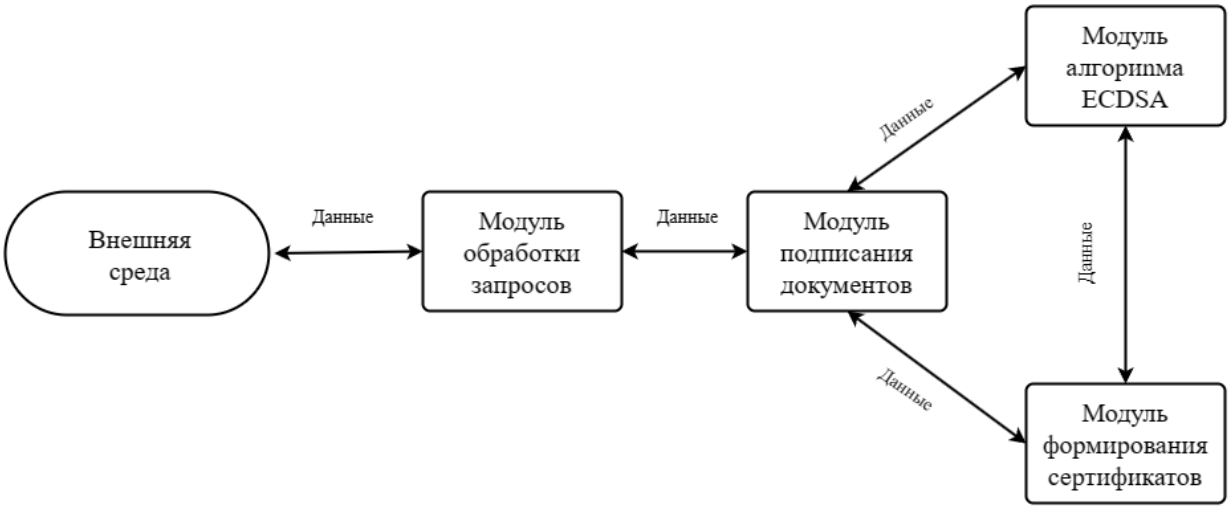
Электронные подписи в настоящее время позволяют решить ряд задач информационной безопасности. К задачам, которые позволяет решить ЭП относятся: защита электронного документа от подделки, однозначная идентификация владельца документа, подтверждение достоверности источника документа. Возможности электронной подписи позволяют обеспечить безопасность при пересылке в сети Интернет.

В настоящее время наибольший интерес представляют электронные подписи, которые базируются на эллиптической криптографии, так как они могут обеспечить такой же уровень безопасности, как электронные подписи на базе конечных полей, но при меньшей длине ключа. Кроме вышеупомянутой особенности, алгоритм ECDSA соответствует требованиям современных приложений и современной IT–индустрии, поэтому разработка программного модуля для внедрения электронной подписи на базе ECDSA является актуальной задачей.



Алгоритм	Значение хэш-функции (бит)	Длина сообщения (бит)	Количество итераций в цикле	Скорость (МБ/с)
SHA-256, SHA-224	256/224	$2^{64} - 1$	64	139
SHA-512, SHA-384, SHA-512/256, SHA-512/224	512/384/256/224	$2^{128} - 1$	80	154