УДК 681.3

СИСТЕМА АУТЕНТИФИКАЦИИ С НУЛЕВОЙ ПЕРЕДАЧЕЙ ИНФОРМАЦИИ

Студент гр. 113017 Ермолович П.А.,
кандидат техн. наук, доцент Артамонов В.А.
Белорусский национальный технический университет

Быстрый рост глобальной сети Internet и стремительное развитие информационных технологий привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. К числу наиболее перспективных направлений применения современных информационных технологий относится бизнес. Важнейшим условием существования электронного бизнеса является информационная безопасность, под которой понимается защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации. В данной работе предлагается использование протоколов с нулевым разглашением для безопасного соединения в сети Internet.

Протоколы с нулевым разглашением на практике не являются в точном математическом смысле протоколами с абсолютно нулевым разглашением. Однако совсем не этот фактор имеет в данном случает решающее значение.

Многие протоколы в том числе протоколы на основе систем с открытым ключом требуют выполнения объемных вычислений с обоих сторон. В то же время они обладают тем существенным преимуществом, что для полной проверки доказываемого знания достаточно одной итерации. В случае же с протоколами с нулевым разглашением вычисления как правило более просты, но требуют выполнения большого количества итераций прежде чем проверяющая сторона сможет убедиться в идентичности доказывающей стороны с достаточной степенью вероятности.

Описанные свойства и определили в основном возможные применения протоколов с нулевым разглашением. Очевидно, в силу требования к большому количеству итераций их применение в компьютерных сетях связано с трудностями. С другой стороны использование протоколов со сложными вычислениями невозможно на сравнительно простых устройствах с малым объемом памяти таких как смарт-карты. Последние и приводятся чаще всего в качестве основного примера, где возможно использование протоколов с нулевым разглашением.