Алгоритмы криптографической защиты командно-телеметрической информации в каналах связи с беспилотными летательными аппаратами

УДК 004.056.55

Анатолий Белецкий[1], Бахытжан Ахметов[2], Денис Навроцкий[1]

[1] *Национальный авиационный университет, [1]abelnau@ukr.net, [3]g6336@yandex.ua*

[2] *Казахский национальный исследовательский технический университет имени К.И. Сатпаева, [2]bakhytzhan.akhmetov.54@mail.ru*

Беспилотные летательные аппараты (БПЛА) в настоящее время составляют основу авиации специального применения. БПЛА используются для патрулирования границ, аэрофотосъемок, разведки геофизическими методами, контроля радиационного фона, а также для сбора различной информации по заявкам гражданских и военных ведомств. И как следствие, актуальной становится проблема обеспечения надлежащей криптографической защиты (КЗ) каналов передачи данных между летательным аппаратом и наземным пунктом управления (НПУ), именуемые как «Борт» и «Земля» соответственно.

К важнейшим видам информации, которыми обмениваются Борт и Земля, относятся командно-телеметрическая информация (КТИ). *Командная информация* представляет собой цифровые блоки (пакеты) фиксированной длины, которые поступают по радиоканалу с Земли на Борт для корректировки положения органов управления аппарата с целью выполнения маневров, задаваемых оператором (пилотом) НПУ. *Телеметрическая информация*, передаваемая с Борта на Землю также в виде цифровых пакетов, содержит сведения о положении органов управления БПЛА. Пренебрежение криптографической защитой КТИ чревато опасностью несанкционированного доступа противника в канал управления БПЛА, что может привести (и по сведениям из Интернета – приводит) к захвату аппаратов.

Следует отметить, что в открытой отечественной и зарубежной печати практически отсутствуют сведения о способах построения систем КЗ КТИ в каналах связи «НПУ – БПЛА – НПУ». Ниже излагается один из подходов к решению указанной проблемы, не претендующий на «истину в последней инстанции» и отражающий лишь предварительный опыт, накопленный авторами доклада в процессе работы над созданием систем КЗ КТИ в каналах связи с БПЛА, разрабатываемых в Национальном авиационном университете.

В основу построения системы КЗ КТИ для БПЛА положен оригинальный байт-ориентированный алгоритм поточного шифрования, в котором шифрующая гамма-последовательность стохастических битов формируется совокупностью равномерно плотных примитивов нелинейной подстановки (ПНП), сведенных в так называемые блоки преобразования байтов (БПБ). Равномерно плотными являются такие ПНП, отклики которых равномерно распределены на диаграмме рассеивания.

Вариант предлагаемого поточного шифра показан на рис. 1, где $\boldsymbol{X}$ – входной байт, $\boldsymbol{Y}$ – байт гаммирования и $\boldsymbol{Z}$ – выходной байт.

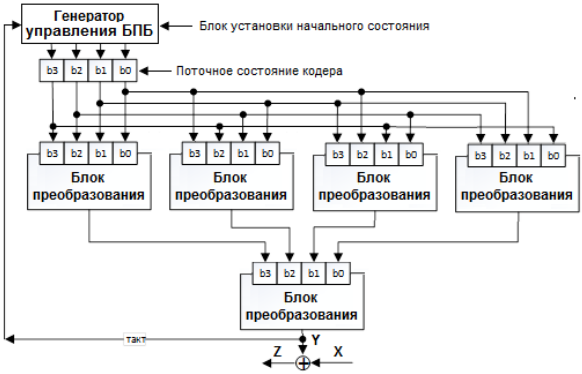

Рис. 1. Структурно-логическая схема алгоритма поточного шифрования

В основу протоколов шифрования положены правила, регламентирующие использование криптографических преобразований и алгоритмов в информационных процессах. Обобщенная схема построения криптографического *протокола зашифрования данных* приведена на рис. 2.

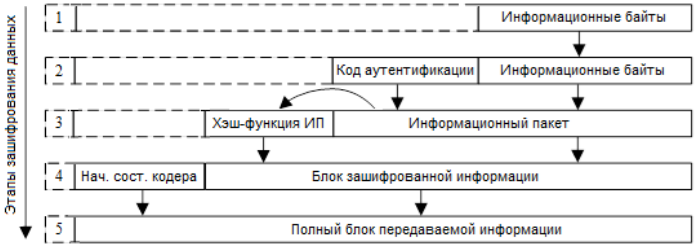

Рис. 2. Структурно-логическая схема протокола зашифрования данных

На приемной стороне этапы расшифрования данных выполняются в последовательности, обратной последовательности этапов зашифрования.

Роль *синхронизирующего элемента* в протоколах обмена данными выполняет содержимое блока установки начального состояния генератора управления БПБ (рис. 2), которое передается по каналу связи в открытом виде, что не нарушает секретности передачи данных, так как третья сторона не в состоянии воспроизвести расшифровующую гамму, поскольку для него (противника) остаются закрытыми ПНП шифратора (рис. 1).

Отличительная особенность предлагаемого способа КЗ КТИ состоит в простоте алгоритмическо-программного обеспечения системы защиты. Есть все основания высказать предположение, что разработан новый, не имеющий отечественных и зарубежных аналогов, оригинальный алгоритм поточного шифрования данных, который по критериям быстродействия передачи информации и степени «отбеливания» исходного текста, оцениваемой энтропией шифрограммы, не уступает лучшим образцам зарубежных шифров.