УДК 62-50

КЛАССИФИКАЦИЯ УГРОЗ ДЛЯ ДАННЫХ, ПЕРЕДАВАЕМЫХ МЕЖДУ НАЗЕМНОЙ СТАНЦИЕЙ УПРАВЛЕНИЯ И БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ

Степанов В.Ю., Хвитько Е.А.
Белорусский национальный технический университет, Минск, Беларусь,
vovchik-13a@yandex.ru, evgeni.hvitko@bntu.by

Беспилотные летательные аппараты (БПЛА) предназначены для дистанционного мониторинга и контроля местности, объектов, окружающей среды с передачей видеоизображения на землю в реальном масштабе времени.

Значительный прогресс в создании и использовании БПЛА объясняется тем, что они, как минимум, минимизируют риск для жизни пилотов.

К типичным задачам БПЛА относятся: пограничное и морское патрулирование, поисково-спасательные работы, обнаружение лесных пожаров, мониторинг стихийных бедствий, измерение загрязнений, наблюдение за дорожным движением, инспектирование источников энергии и трубопроводов, наблюдение за земной поверхностью и т.д.

Из приведѐнного списка выполняемых задач беспилотным летательным аппаратом, становится понятно, насколько важно передать данные, собранные с датчиков БПЛА, на наземную станцию управления (НСУ), в целости и сохранности.

В общем случае, схема дистанционного взаимодействия БПЛА и НСУ выглядит следующим образом (рисунок 1):

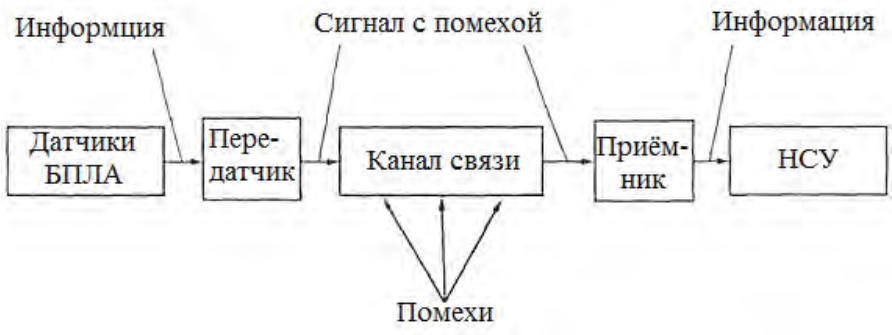

Рисунок 1 – Схема дистанционного взаимодействия БЛА и НСУ

Направление передачи данных (от БПЛА к НСУ или наоборот) значения не имеет.

Как видно из данного рисунка, помехи могут настигнуть полезную информацию практически на любом этапе взаимодействия. Также, более опасной ситуацией, по сравнению с простыми шумами, является возможные попытки перехвата и/или искажения «злоумышленниками» данной информации с целью манипулирования ею. В целом, угроза безопасности есть потенциально возможное событие, действие, процесс, явление, которое может привести к нанесению ущерба защищаемому объекту системы [1].

Самым простым и очевидным способом защиты информации является еѐ шифрование.

В настоящее время применяются два вида алгоритмов шифрования: симметричные алгоритмы (DES, 3-DES, FEAL, IDEA, CAST,) в которых для шифрования и расшифровки используется один и тот же секретный ключ, и асимметричные алгоритмы (RSA, ECC, Эль-Гамаль), в которых для шифрования и расшифровки используется два разных ключа, один из которых известен всем, а другой держится в тайне [2].

В целом, для предотвращения манипуляции с данным необходимо использовать идентификацию объекта, а подтверждение подлинности должно осуществляться при помощи никому неизвестного ключа (кроме передающего и получающего информацию). Перед установкой соединения секретный ключ, естественно, должен быть известен обеим заинтересованным сторонам.

Возможность объекта шифровать сообщения специальным секретным ключом позволяет применить методы подтверждения подлинности, так что проблема сводится к созданию защищѐнной процедуры распределения и защиты секретных ключей между объектами. На стадии передачи данных целостность сообщения обеспечивается соответствующим способом шифрования. При передаче информации (как с БПЛА, так и управляющих команд к БПЛА) необходимы так называемые обратные связи, чтобы гарантировать невозможность (если даже перехват успешно осуществлѐн) удаления пакетов данных, и/или их выборочной модификации или переупорядочивания информации в рамках сообщения.

Чтобы защитить отдельные пакеты от искажения используются специальные криптографические поля в протоколах типа «запрос – ответ». Итак, каждый участник соединения периодически передаѐт нумерованный, шифрованный запрос и ожидает ответа от второго участника. Предельный интервал ожидания и частоты использования протокола могут быть определены из оценок интервалов прохождения команд установления соединения. Если достигнут предельный интервал ожидания, информация передается в центр распределения ключей или управления защитой. Если отдельные или последовательные пакеты сообщений задерживаются преднамеренно нарушителем в течение интервала, превышающего предельный интервал ожидания, то вторжение будет выявлено. На стадии завершения связи вторжение может быть направлено на удаление протокола завершения, продление соединения и добавление запрещѐнных данных к сообщению. Приѐмы защиты, направленные на обеспечение целостности данных, позволяют предотвратить такое вторжение.

Прогресс не стоит на месте и существует ещѐ несколько способов борьбы с беспилотными летательными аппаратами:

- использование средств радиотехнической разведки, при помощи которых вычисляется точное местоположение НСУ;

- постановка радиопомех, прерывающих связь между пультом оператора НСУ и беспилотным летательным аппаратом. В результате такого прерывания связи БПЛА, в зависимости от заложенной программы, может либо вернуться на базу, либо выполнить аварийную посадку. Так, в декабре 2011 года иранские военные сумели перехватить американский разведывательный БПЛА RQ-170. Этот аппарат управлялся по спутнику (канал был зашифрован, а ключи шифрования менялись один раз в несколько секунд). Для непосредственного взлома такого сигнала потребовалось бы очень много времени и мощные вычислительные системы. Однако иранские военные заглушили канал управления RQ-170; БПЛА перешѐл в автоматический режим и направился на базу ВВС США в Афганистане по сигналам GPS. Считается, что иранские военные сумели успешно подменить или исказить навигационный сигнал GPS, в результате чего RQ-170 сбился с курса и совершил посадку на территории Ирана [3].

ЛИТЕРАТУРА

1 Алгулиев, Р.М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей / Р.М. Алгулиев. – М.: УРСС, 2001. – С. 56.

2 Петров, А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. – М.: ДМК, 2000. – С. 238.

3 nplus1.ru – Электронный ресурс. Метод доступа:– https://nplus1.ru/news/2016/09/08/uavs. Дата доступа: 05.11.2017