

Анализ потенциальных угроз системы управления БЛА средних и тяжелых классов М.В. Аменитский

Акционерное общество «Московский ордена Трудового Красного Знамени научно-исследовательский радиотехнический институт» (АО «МНИРТИ»)

В данной статье проведен синтез и анализ схемы управления средних и тяжелых БЛА на предмет возможности воздействия на нее извне. Определен перечень систем, подверженных вредоносному воздействию.

В 2012 военная система США увеличила свои инвестиции в исследования и производство беспилотных летательных аппаратов (БЛА) с 2.3 млрд. долл. в 2008 г. до 4.2. млрд. [1] В настоящее время БЛА применяются для решения широкого спектра задач, таких как патрулирование границ, разведки, транспортировки и вооруженных атак. В настоящее время в России также активно ведется разработка комплексов БЛА, о чем свидетельствует большое количество НИР и ОКР данной направленности.

Такие происшествия как захват RQ-170 Sentinel Вооружёнными силами Ирана 4 декабря 2011 [2] или вирус-шпион, т.н. «кейлогер», инфицировавший флот американских беспилотников на авиабазе ВВС США Крич (Creech Air Force Base) в Неваде в сентябре 2011, [3] доказывают недостаточность защиты БЛА. В связи с повсеместным распространением БЛА возникает необходимость анализа технических уязвимостей и слабых мест БЛА.

Синтез объекта воздействия

В России в данный момент не существует каких-либо требований и стандартов, регламентирующих систему управления БЛА, в связи с чем для синтеза системы управления целесообразно использовать систему стандартов НАТО.

Схема БЛА в странах НАТО, определена в [4] и представлена на рисунке 1.

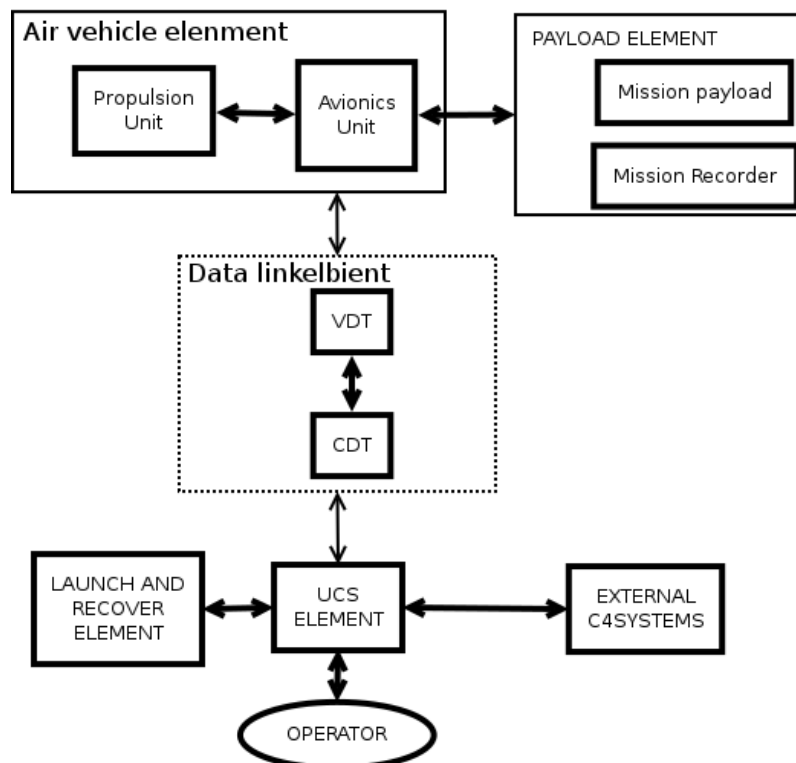


Рисунок 1 - Схема БЛА[4]

Согласно [3] БЛА должен состоять из трех основных элементов: **системы полета** БЛА (air vehicle element), целевой нагрузки (Payload element) и **системы управления** (UAV air component). Для анализа возможности внешнего воздействия целесообразно рассмотреть элементы, которые могут взаимодействовать с другими компонентами посредством беспроводной линии связи (радио, оптической, акустической). В данном случае это может быть система управления и целевая нагрузка. Рассмотрим более подробно систему управления, схема представлена на рисунке 2.

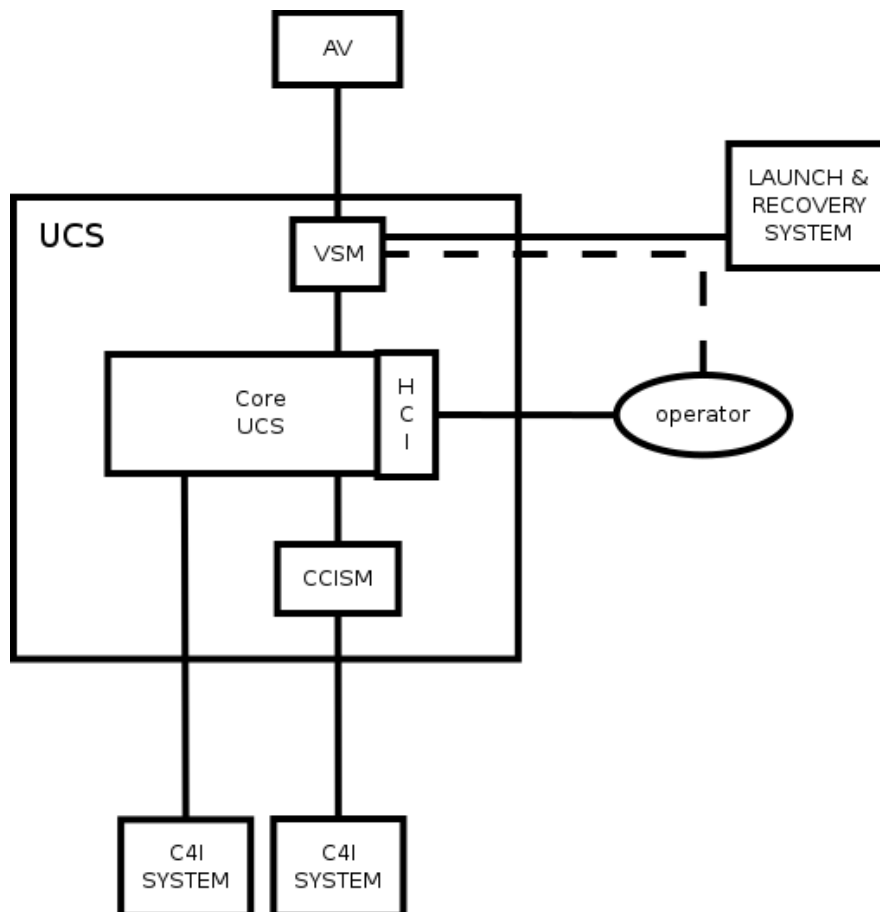


Рисунок 2 - Система управления БЛА[4]

[4] устанавливает требования к системе управления беспилотным летательным аппаратом (СУБЛА), и имеет следующую функциональную архитектуру:

- двигатель, средства маневрирования и поддержания полета (air vehicle/**AV**);
- **контролер управления** для **AV** (**VSM**);
- интерфейс оператора (**HCI**);
- ядро (core **USC**)
- система запуска и возвращения (launch and recovery system)
- **согласующий блок целевой нагрузки** (**CCISM**);
- внешние подключаемые системы **c4I** могут быть целевой нагрузкой (**c4I system**).

Контролер управления для **AV** осуществляет согласование протоколов и синхронизацию

между **air vehicle** , ядром UCS, а также выполняет следующие функции:

- оптимизирует пакеты;
- ведет базу данных событий;
- следит за состоянием AV;
- может управлять каналом запуска и возвращения;
- осуществляет аналого-цифровое преобразование данных с сенсоров двигателя и другого оборудования;
- передает данные, необходимые для контроля состояния летательного аппарата, а также передает команды управления от ядра.

Контролер управления для AV как правило разрабатывается производителем БЛА и является необязательным при условии что БЛА выполнен с применением протокола, указанного в STANAG 4586 [4].

Ядро UCS должно предоставлять интерфейс оператору, который позволяет **управлять и отображать** параметрические данные состояния БЛА и целевой нагрузки.

В зависимости от требуемого уровня взаимодействия в конкретной системе БЛА, ядро выполняет следующие задачи [4]:

- прием, обработка и передача данных от **Контролера управления для AV**, оператору и обратно;
- выполнение и планирование задач;
- наблюдение и контроль за ЛА, целевой нагрузкой;
- предоставление оператору необходимого инструмента для постановки, планирования и выполнения задачи;
- готовность принять на себя функции **Контролера управления для ЛА**.

[4] выдвигает требования к ядру системы управления БЛА и не накладывает никаких ограничений на внешний вид системы ручного управления (например, количество дисплеев ручного управления, переключатели и др.), но выставляются требования к дисплею оператора и средствам ввода, предназначенным для взаимодействия с ядром; определен формат данных, которые должны быть отображены. Некоторые требования наложены для обеспечения эффективного функционирования систем БЛА.

Согласующий блок целевой нагрузки обеспечивает функцию, аналогичную **контролеру управления AV**, то есть инкапсуляцию данных, полученных от ядра для внешних подключенных систем, а также обратную совместимость[4] для устаревших систем.

Внешние подключаемые системы с4I - это и есть непосредственно целевая нагрузка, или могут быть какие-либо дополнительные системы, необходимые для эффективного функционирования БЛА.

Согласно [5] современные БЛА должны иметь возможность продолжать выполнение задания даже в случае потери связи с наземным центром, для чего требуется навигационная система, способная предоставлять для системы управления БЛА сведения о его пространственном положении. Проведенный анализ [4] и требования, выставляемые в [5], позволяют синтезировать дополнительную схему организации связи системы управления БЛА, представленную на рисунке 3.

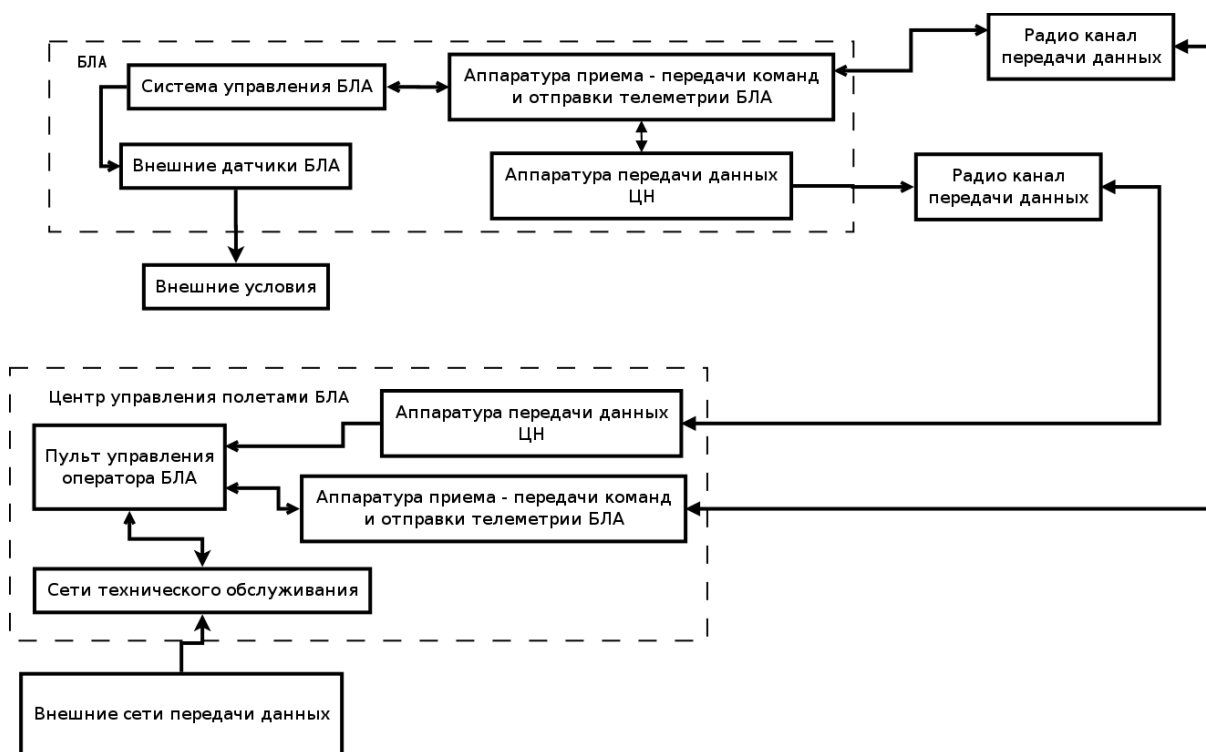


Рисунок 3 - Схема организации связи системы управления БЛА

Анализ угроз безопасности системы управления БЛА

Проведя анализ схемы организации связи системы управления БЛА, можно предположить возможность наличия трех векторов воздействия на систему.

- центр управления полетом БЛА.
- БЛА
- радиоканал БЛА

Воздействие на центр управления полетом можно вести с двух сторон.

Первое воздействие со стороны внешних сетей передачи данных, путем обхода защиты и последующих действий вредоносного влияния (внедрение программных закладок, перенаправление трафика с последующей подменой пакетов и команд управления, а также других воздействий).

Достоинства:

- полный контроль над БЛА с функционалом оператора;
- вероятностная возможность воздействия на другие подчиненные центру управления полетом БЛА составные части системы управления.

Недостатком подхода становится огромное количество зачастую непреодолимых факторов:

- для реализации подхода необходима высокая квалификация специалистов, производящих перехват управления;
- необходимо большое количество знаний конфиденциального характера (требуется долгая разведка архитектуры сети, протоколов взаимодействия и много другой информации);
- необходим доступ к внешним сетям передачи данных, имеющим соединение с сетями технического обслуживания БЛА;
- результат взаимодействия не определен, т.к. на него влияет много вероятностных факторов.

Вторым вектором взаимодействия на центр управления БЛА является навязывание оператору ложной информации касательно состояния БЛА и его пространственного положения через аппаратуру приема-передачи команд и отправки телеметрии или приема данных от целевой нагрузки, путем подмены трафика, приходящего на входной тракт приемного устройства центра управления: состояние объекта БЛА (скорости, угла атаки, высоты и состояния других датчиков), передача ложных данных с целью провокации оператора на действия, необходимые атакующему, и другие

воздействия.

Достоинства:

- сравнительно несложная реализация;
- есть реальная возможность спровоцировать оператора на действия, необходимые атакующему;
- сбой полетного задания.

Недостатки:

- необходимо находится в прямой радиовидимости антенн аппаратуры приема-передачи данных центра управления полетов;
- нет полного контроля над БЛА;
- реализация воздействия и его последствия сильно зависят от опыта оператора;
- для реализации атаки необходим деятельный анализ протоколов связи БЛА с ЦУП, что может быть затруднено;
- канал передачи данных телеметрии и данных с целевой нагрузки может быть защищен криптографически (имитовставка или шифрование), что сводит воздействия на нет.

Воздействие на БЛА можно осуществить с трех направлений:

Перехват управления путем навязывания приемнику ложного (завышенного) значения сигнал/шум на входе приемного тракта, тем самым заставить систему приема снизить чувствительность приемника и таким образом исключить возможность воспринимать команды оператора, что даст возможность перехватить управление.

Достоинством методики является возможность осуществить полный захват управления БЛА.

Недостатки:

- необходимость знания протоколов связи;
- как и в случае воздействия на оператора наличие СКЗИ в канале сведет к минимуму вероятность перехвата управления;
- некоторые системы связи могут быть невосприимчивы к данному виду атаки.

Воздействие на целевую нагрузку

Данный вид воздействия возможен в тех случаях, когда отказ или неправильное функционирование целевой нагрузки приводит к немедленному изменению или прекращению полетного задания. Эффективным может стать воздействие через радиоканалы на целевую нагрузку. Особенности реализации воздействия зависят от конкретного типа целевой нагрузки.

Достоинством такого воздействия является то, что в некоторых случаях оно может привести к срыву полетного задания.

Недостатки:

- не может или очень редко может привести к захвату управления БЛА;
- использование СКЗИ сведет на нет эффект от воздействия.

Воздействие на систему пространственного позиционирования БЛА

Воздействие на систему пространственного позиционирования БЛА открывает большие возможности для комбинирования различных действий на внешние датчики БЛА.

Данное воздействие наиболее эффективно в момент управления с помощью автопилота или активного радиоподавления каналов управления БЛА и может привести к частичному или полному перехвату управления БЛА, срыву полетного задания или переводению системы в неопределенное состояние.

Также важной особенностью воздействия на систему пространственного позиционирования является тот факт, что изначально подобные системы разрабатывались для пилотируемой авиации и в самой идее их построения не вставал так остро вопрос противодействия целенаправленному злонамеренному воздействию. В связи с изложенным, вероятность выявления уязвимости гораздо выше, чем в других методах воздействия.

Достоинства:

- может привести к частичному или полному захвату управления;
- сравнительно легкая реализация;
- воздействие плохо детектируется со стороны оператора, в особенности, если оно производится в режиме автоматического пилотирования;
- Для противодействия необходима разработка новых изделий.

Недостатки

- требуется предварительная разведка (?Что значит разведка аппаратуры? Изучение?) аппаратуры пространственного позиционирования;
- из-за широкого спектра диапазона воздействия необходимо иметь большое количество различного оборудования, работающего на разных частотных диапазонах, что не всегда представляется возможным.

Воздействие на ретрансляторы связи в данной работе не рассматривается ввиду зависимости возможного воздействия от конкретной реализации.

Воздействие на систему управления БЛА путем организации прямого и обратного канала управления, с применением технологии выявления и эксплуатации программных уязвимостей в рамках данной работы не рассматривается ввиду того, что их наличие также зависит от конкретной реализации системы управления БЛА.

Вывод

В данной работе было проведено синтезирование и анализ схемы организации передачи информации БЛА с выполнением требований [4]. Проведенный анализ показал наличие каналов воздействия на систему управления БЛА.

Были рассмотрены различные направления воздействия, целью которых является перехват управления над системой управления БЛА, выявлены различные достоинства и недостатки каждого из них.

Из синтезированной схемы видно, что при разработке схем воздействий на конкретную реализацию системы управления необходимо учитывать подверженность линии связи к внешним атакам.

Важным фактором при осуществлении воздействий является взаимовлияние различных составляющих системы друг на друга.

При организации воздействия на конкретную реализацию системы управления немаловажным фактором является наличие доступа к документации. Также необходимо учитывать наличие программных уязвимостей, которые могут предоставить возможность организации недокументированного канала управления.

При проведении анализа угроз безопасности БЛА было выявлено, что наиболее уязвимым элементом системы управления БЛА является воздействие на систему пространственного позиционирования. Это обусловлено большим количеством комбинаций различных действий на внешние датчики БЛА и тем фактом, что изначально при разработки подобных систем не вставал так остро вопрос противодействия целенаправленному злонамеренному воздействию. На основании вышеизложенного было принято решение дальнейшие исследования направить на оценку уязвимости системы пространственного позиционирования.

Литература

1. *Lolita C. Baldor*, Flashy drone strikes raise status of remote pilots, The Boston Globe, pp. online at 01.11.2012: <http://www.bostonglobe.com/news/nation/2012/08/11/air-force-works-fill-need-for-drone-pilots/ScoF70NqiiOnv3bD3smSXI/story.html>, 2012.
2. *CNN Wire Staff*, «Obama says U.S. has asked Iran to return drone aircraft,» 2011
3. *Noah Shachtman*, Wired, pp. online at 01.11.2012: , 2011. «<http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleetcomputer> Virus Hits U.S. Drone Fleet,»
4. STANAG 4586 Edition No 3 Control System (UCS) Unmanned Aerial Vehicle (UAV) NATO Standardization Agreement 4586
5. *Podins K., Stinissen J., Maybaum M.*, (Eds.) The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment, NATO CCD COE Publications, Tallinn, 2013 5th International Conference on Cyber Conflict.