DOI 10.37882/2223-2966.2025.09.22

ПРОТИВОДЕЙСТВИЕ БЕСПИЛОТНЫМ ЛЕТАЛЬНЫМ АППАРАТАМ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАДАЧ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

COUNTERACTION TO UNMANNED AERIAL VEHICLES TO ENSURE PUBLIC SAFETY

G. Plotnikov
V. Elin
A. Tsaregorodtsev

Summary. The article reveals a number of features of counteraction to unmanned aerial vehicles to ensure public safety based on the fact that the modern use of UAVs is aimed, among other things, at destroying social and critical infrastructure facilities that have a purely civilian purpose and are located deep in the rear of the country, which creates the need for the use of comprehensive measures to counter UAVs. Comprehensiveness implies the adoption of a law and other regulations, as well as the adoption of technical measures.

Keywords: public safety, counteraction to unmanned aerial vehicles.

Плотников Герман Геннадьевич
к.т.н., МОСУ МВД России имени В.Я. Кикотя (Москва)
gr175@mail.ru
Елин Владимир Михайлович
к.п.н., МОСУ МВД России имени В.Я. Кикотя (Москва)
elin_vm@mail.ru
Царегородцев Анатолий Валерьевич
д.т.н., профессор, ФГАОУ ВО РУДН (Москва)
tsaregorodtsev_av@pfur.ru

Аннотация. В статье раскрывается ряд особенностей противодействия беспилотным летальным аппаратам для обеспечения задач общественной безопасности исходя из того факта, что современное применение БПЛА ориентировано, в т.ч. и для поражения объектов социальной и критической инфраструктуры, имеющих сугубо гражданское назначение и находящихся в глубоком тылу страны, что порождает необходимость применения комплексных мер противодействия БПЛА. Комплексность предполагает под собой принятие закона и иных нормативных актов, а также принятие мер технического характера.

Ключевые слова: общественная безопасность, противодействие беспилотным летальным аппаратам.

Концепция применения беспилотных летательных аппаратов (БПЛА) при осуществлении военных действий разработана достаточно давно, под имеющуюся тактику применения подготовлено значительное количество типов БПЛА[1]. Неожиданной новеллой современности стало не только применение БПЛА в ходе ведения военных действий, но применение БПЛА для поражения объектов социальной и критической инфраструктуры, имеющих сугубо гражданское назначение и находящихся в глубоком тылу страны и не являющуюся участником боевых действий[2]. Зачастую, при осуществлении атак с применением БПЛА, противник использует современные разработки в сфере искусственного интеллекта[3].

В сложившейся ситуации возникает необходимость применения комплексных мер по обеспечению общественной безопасности, как состояния защищённости граждан, материальных и духовных ценностей общества от преступных и иных противоправных посягательств, социальных и межнациональных конфликтов, а также от чрезвычайных ситуаций природного и техногенного характера. Общественная безопасность не сводится исключительно к пресечению преступности, а охватывает широкий спектр факторов, включая экологическую безопасность, безопасность в сфере здравоохранения, транспортную безопасность и другие аспекты, влияющие на качество жизни граждан.

В указанных целях в нашей стране принят Закон о противодействии беспилотным аппаратам[4] направленный на расширение полномочий отдельных феде-

[1] Макаренко С.И., Тимошенко А.В., Васильченко А.С. Анализ средств и способов противодействия беспилотным летательным аппаратам//Системы управления, связи и безопасности №1. 2020. с. 109–146. DOI: 10.24411/2410-9916-2020-10105

[2] Беспилотник упал в Минске — посмотрели, что сейчас на месте крушения// https://tochka.by/articles/incidents/bespilotnik_upal_v_minske_posmotreli_chto_seychas_na_meste_krusheniya/

[3] Жарова, А.К. О возможности совершения компьютерных атак по типу man in the Middle attack с применением генеративного искусственного интеллекта / А.К. Жарова // Актуальные проблемы расследования преступлений в сфере компьютерной информации или с применением компьютерных технологий в условиях цифровизации экономики и государственного управления: Материалы Межвузовского круглого стола, Москва, 28 ноября 2024 года. — Москва: Российский экономический университет им. Г.В. Плеханова, ООО «РУСАЙНС», 2025. — С. 45–51. — EDN WLWCKL.

[4] Федеральный закон от 04.08.2023 г. № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»// http://www.kremlin.ru/acts/bank/49674

ральных органов исполнительной власти в части, касающейся пресечения функционирования беспилотных воздушных, подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов (далее — беспилотные аппараты), в том числе посредством подавления или преобразования сигналов дистанционного управления беспилотными аппаратами, воздействия на их пульты управления, а также повреждения или уничтожения этих аппаратов. Пресечение деятельности беспилотных аппаратов осуществляется в целях защиты жизни и здоровья граждан, обеспечения безопасности важных государственных, критически важных и потенциально опасных объектов, а также иных объектов.

Органами МВД России определен порядок принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях защиты жизни, здоровья и имущества граждан над местом проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-разыскных мероприятий[5]. Приказом определена последовательность действий должностных лиц органов внутренних дел, уполномоченных на принятие решений о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях защиты жизни, здоровья и имущества граждан над местом проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-разыскных мероприятий, по принятию такого решения.

Определен также комплекс обязанностей, возлагаемых на частные охранные предприятия в части реализации права пресекать функционирование беспилотных воздушных, подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов.

В связи с этим актуальным представляется вопрос об особенностях функционирования и навигации БПЛА, а также о возможностях противодействия БПЛА мерами подавления, имеющимися в распоряжении гражданского сообщества.

Многие задачи, решаемые современными комплексами беспилотных летательных аппаратов (БПЛА), требуют наличия высокоскоростных линий передачи информации между БПЛА и наземным комплексом управления (НКУ). Например, задачи оперативного мониторинга или разведки с помощью технологий БПЛА предполагают получение на борту и доставку на НКУ растровых изображений разного разрешения, получаемых с датчиков различных диапазонов длин волн. Наиболее распространенная на сегодняшний день технология передачи информации заключается в непрерывной трансляции изображения по мере его получения в цифровом или аналоговом формате, структура которого не меняется в течение всего полета.

Как правило, на борту БПЛА размещаются не менее двух систем связи: дуплексная/полудуплексная аппаратура передачи командно-телеметрической информации и симплексная система передачи информации полезной нагрузки. Аппаратура передачи командно-телеметрической информации предназначена для низкоскоростной передачи командной информации с НКУ на борт БПЛА и низкоскоростной передачи телеметрической информации с борта БПЛА на НКУ. Аппаратура передачи информации полезной нагрузки предназначена для односторонней высокоскоростной передачи информации полезной нагрузки с борта БПЛА на НКУ, как это представлено в таблице 1.

Прямая связь между БПЛА и НКУ в диапазонах СВЧ возможна только в пределах прямой видимости. Для повышения надежности комплекса БПЛА на борту устанавливаются несколько приемо-передатчиков различных диапазонов длин волн[6]. Передача телеметрической информации при полетах на большие расстояния может осуществляться с помощью спутниковых систем связи (Iridium, Globalstarи др.).

Высокоскоростная передача информации полезной нагрузки может также осуществляться через малоразмерные спутниковые терминалы, что требует установки на борт БПЛА высоконаправленной антенны с возможностью сканирования. В простейшем случае это параболическая антенна на опорно-поворотном устройстве.

Несмотря на большое количество возможных вариантов реализации систем передачи командно-телеметрической информации и информации полезной нагрузки, оптимальным и наиболее часто используемым остается вид связи, при котором данные передаются напрямую между БПЛА и НКУ.

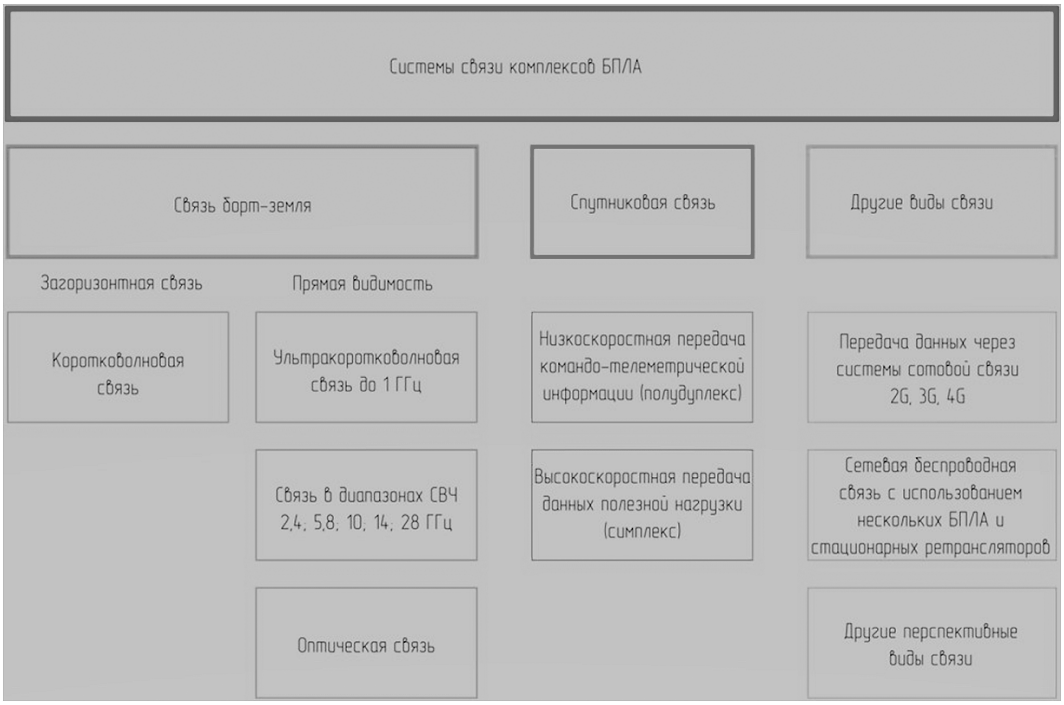
В настоящее время существуют четыре глобальные СРНС: GPS (США), Galileo (Евросоюз), ГЛОНАСС (РФ), BeiDou

[5] Приказ МВД России от 30 апреля 2020 г. № 252 «Об утверждении Порядка принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях защиты жизни, здоровья и имущества граждан над местом проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-разыскных мероприятий и Перечня должностных лиц, уполномоченных на принятие такого решения»

[6] Боев Н.М., Шаршавин П.В., Нигруца И.В. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния//https://uav-siberia.com/news/postroenie-sistem-svyazi-bespilotnykh-letatelnykh-apparatov-dlya-peredachi-informatsii-na-bolshie-ra/

Таблица 1.

Возможные варианты реализации систем связи комплексов БПЛА



(Китай). Каждая из этих радионавигационных систем обладает группировкой навигационных космических аппаратов (НКА), которые непрерывно передают специальные навигационные радиосигналы. Измеряя время приема каждого радиосигнала, можно оценить расстояние от точки приема до каждого из НКА. Измерив не менее трех указанных сигналов, можно рассчитать местоположение (координаты) навигационного приемника.

Каждый аппарат излучает несущее колебание в двух частотных диапазонах L1 и L2. Все НКА системы GPS излучают на общих частотах, 1575,42 МГц и 1227,60 МГц для L1 и L2 соответственно.

Навигационные сообщения также содержат параметры ионосферы (позволяет учитывать задержку сигналов в ионосфере), разницу между системной шкалой времени и мировой координированной шкалой времени и много еще всякой другой полезной информации.

Каждый спутник системы GPS непрерывно генерирует радиоволны двух частот — L1=1575.42МГц и L2=1227.60МГц. Мощность передатчика составляет 50 и 8 Ватт соответственно. Навигационный сигнал представляет собой фазово-манипулированный псевдослучайный код PRN (Pseudo Random Number code). PRN бывает двух типов: первый, C/A-код (Coarse Acquisition code — грубый код) используется в гражданских приемниках, второй P-код (Precision code — точный код), используется в военных целях, а также, иногда, для решения задач геодезии и картографии. Частота L1 модулируется как C/A, так и P-кодом, частота L2 существует только для передачи P-кода.

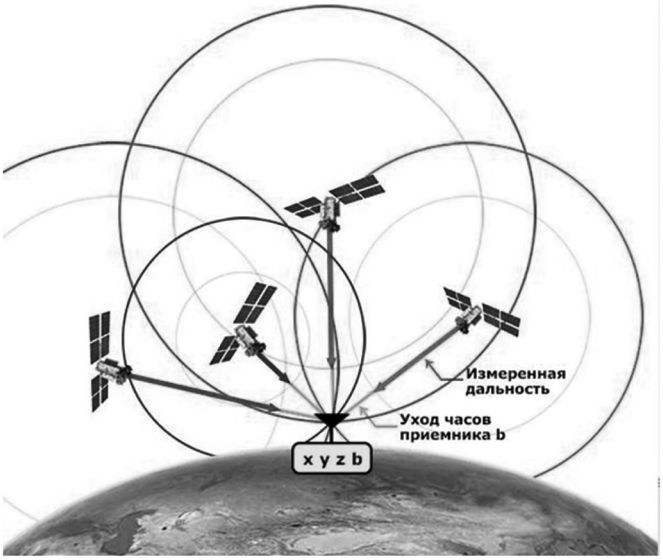
Кроме описанных существует еще и Y-код, представляющий собой зашифрованный P-код (в военное время система шифровки может меняться).

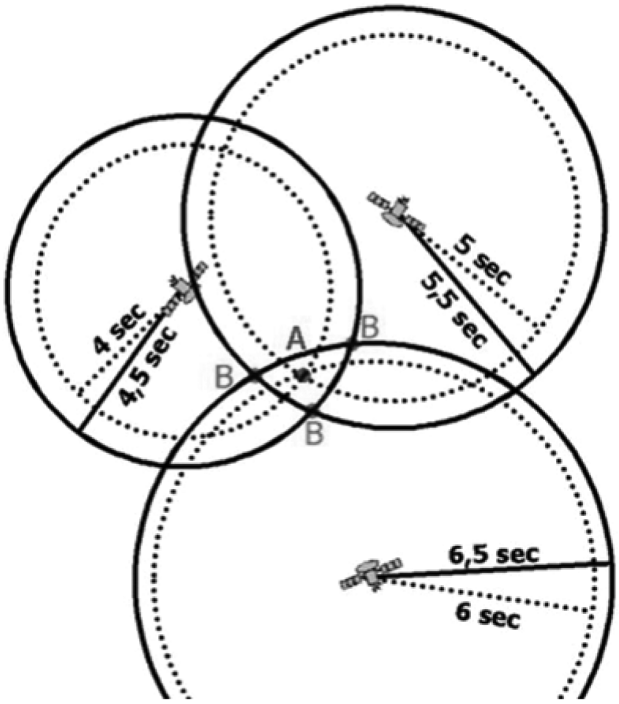
Каждый GPS-приемник имеет собственный генератор, работающий на той же частоте и модулирующий сигнал по тому же закону, что и генератор спутника. Таким образом, по времени задержки между одинаковыми участками кода, принятого со спутника и сгенерированного самостоятельно, можно вычислить время распространения сигнала, а, следовательно, и расстояние до спутника.

Основой идеи определения координат GPS-приемника является вычисление расстояния от него до нескольких спутников, расположение которых считается известным (эти данные содержатся в принятом со спутника альманахе). В геодезии метод вычисления положения объекта по измерению его удаленности от точек с заданными координатами называется трилатерацией.

Для определения координат навигационному приемнику дополнительно нужна информация о текущем местоположении НКА, а также о его бортовой шкале времени. Эта информация передается в специальных навигационных сообщениях в форме, так называемых, альманаха и эфемероидной информации.

Основным способом информационно-программного противодействия БПЛА является создание ложь-





ного радионавигационного поля, или, так называемый, GPS-spoofing. Принцип подмены радионавигационного поля заключается в том, что устанавливают относительно мощный передатчик, который излучает ложные, но структурно и технически корректные навигационные сигналы. Если мощность ложного сигнала превышает мощность сигналов от НКА, то навигационный приемник будет определять неверные координаты.

Средства интеллектуального искажения навигационного поля (ИИНП) предназначены для имитации в некоторой зоне навигационного поля, параметры которого будут отличаться от истинных. В результате этого на определённой территории будет невозможно определить истинные координаты объектов. Вне зоны действия средства ИИНП навигационное поле остаётся легитимным.

Рассмотрим следующий пример, предположим, что необходимо у зданий номер 2 и 3 (рис. 1) подменить координаты на близкие, но неверные, сохранив при этом истинные координаты здания номер 1. При отсутствии подмены навигационного поля каждое из этих строений имеет свои координаты. После включения ИИНП в зоне действия средства все навигационные приёмники будут показывать координаты, заданные оператором ИИНП. Все приёмники сигналов навигации, находящиеся в зоне действия ИИНП, будут работать корректно, но будут показывать ложные (заданные оператором) координаты (рис. 2).

Данный способ может быть использован при борьбе с БПЛА, которые ориентируются в пространстве по сигналам спутниковой навигации. Однако его следует с осторожностью применять к коммерческим БПЛА в связи с тем, что из-за их простых и дешевых систем навигационного управления при значительном изменении текущих координат происходит «зависание» системы навигационного управления и неуправляемое падение коммерческого БПЛА. Учитывая массу коммерческих

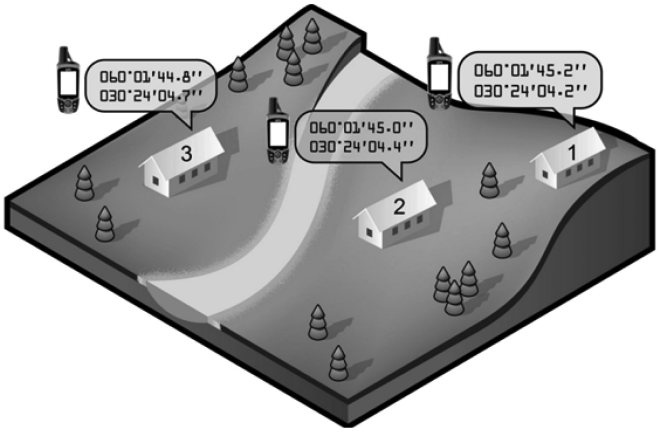


Рис. 1. Пример подмены координат объекта до искажения поля

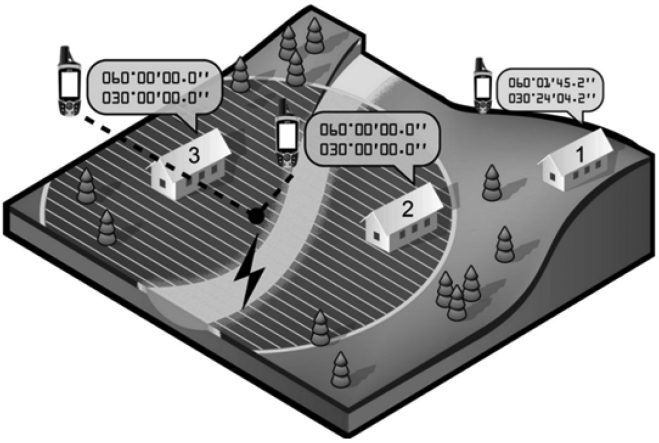


Рис. 2. Пример подмены координат объекта после искажения поля

БПЛА, их падение с высоты нескольких сотен метров может причинить ущерб имуществу охраняемого объекта и существенный вред здоровью (вплоть до летального исхода) людям, находящимся на объекте.

К основным способам противодействия БПЛА, нацеленным на прекращение перемещения БПЛА, срыв выполнения ими задач, а также их физическое уничтожение или захват, относятся[7]:

— радиоэлектронное воздействие (блокирование, подавление);
— информационно-программное воздействие (перехват, спуффинг, ddos-атаки);
— микроволновое воздействие (электромагнитное воздействие);
— оптоэлектронное воздействие (лазерное воздействие);
— механическое воздействие (ловля специальными сетями, огневое и кинетическое воздействие).

Радиоэлектронное подавление (РЭП) заключается в излучение помеховых сигналов, приводящих к затруднению или срыву функционирования различных систем БПЛА:

— подавление радиолиний управления БПЛА;
— подавление средств спутниковой радионавигации (GPS/ГЛОНАСС и других космических радионавигационных систем);
— комбинированные воздействия.

Радиоэлектронное подавление БПЛА является одним из основных способов борьбы с управляемыми БПЛА. Наиболее часто используется заградительная шумовая помеха, перекрывающая полосу пропускания радиоприемного тракта и превышающая по мощности управляющий сигнал.

Борьба с квадрокоптерами или радиоэлектронное подавление БПЛА обладает целым рядом достоинств, по сравнению с другими способами противодействия, например, механическим воздействием:

— радиоэлектронное подавление может осуществляться сразу на несколько БПЛА. Теоретически количество подавляемых целей не ограничено, условием подавления является лишь превышение уровня помехи над уровнем полезного сигнала. Причем это относится как к подавлению каналов управления, так и к подавлению средств радионавигации;
— радиоэлектронное подавление экономически более выгодно, так как в ходе функционирования расходуется только электроэнергия;
— радиоэлектронное подавление обладает большой гибкостью применения. Можно использовать различные режимы работы, избирательно подавлять заданные БПЛА и/или выбранные бортовые системы, применять различные сценарии функционирования комплекса противодействия, адаптируясь к внешним условиям.

Однако кроме достоинств радиоэлектронное подавление обладает и некоторыми недостатками:

— при функционировании средств радиоэлектронного подавления должны выполняться экологические требования, а также требования по электромагнитной совместимости с другими радиоэлектронными средствами;
— радиоэлектронное подавление радиолиний управления невозможно в случае функционирования БПЛА в режиме «радиомолчания», когда его полет осуществляется автономно по заранее загруженной программе;
— использование заградительных помех приводит к необходимости применения мощного помехового радиоизлучения, особенно для широкополосных сигналов БПЛА. Для использования прицельных помех требуется предварительный этап обнаружения и технического анализа сигналов БПЛА.

Современные средства радиоэлектронного подавления можно разделить на следующие типы:

— военные средства РЭП — имеют большую излучаемую мощность, и, как следствие, обладают большой дальностью подавления;
— «коммерческие» средства РЭП — имеют среднюю излучаемую мощность и ограниченную дальность подавления. Используются для прикрытия важных государственных, промышленных и социальных объектов от «коммерческих» беспилотных летательных аппаратов;
— малогабаритные средства РЭП — имеют невысокую излучаемую мощность и малую дальность подавления. Как правило, выполнены в виде носимого радиоэлектронного «ружья».

Существуют несколько основных способов информационно-технического воздействия на БПЛА:

— воздействие путем нарушения радиообмена между БПЛА и наземным пунктом управления (НПУ);
— воздействие путем нарушения информационного обмена между БПЛА и наземным пунктом управления (НПУ);
— воздействие путем нарушения специального программного обеспечения на БПЛА и/или НПУ.

Для осуществления указанных воздействий средства противодействия должны получить информацию о формате и структуре используемых протоколов управления

[7] Плотников, Г.Г. О модели оценки противодействия беспилотным системам / Г.Г. Плотников // Информационные технологии в деятельности органов внутренних дел: Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. — Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2024. — С. 214–215. — EDN CIMEGA.

и обмена данными. Тогда появляется возможность передачи ложных команд управления или ложных параметров на БПЛА.

Для реализации указанных воздействий средства противодействия могут использовать следующие уязвимости используемых в каналах управления БПЛА технологий беспроводного доступа и/или сотовой связи:

— уничтожение или подмена параметров аутентификации и/или авторизации в ходе установления или поддержания соединения между БПЛА и НПУ;
— использование в каналах управления протоколов шифрования со слабой криптографической стойкостью.

Если удается получить доступ к форматам используемых протоколов обмена информации, то становится возможным установить:

— тип БПЛА;
— координаты БПЛА по информации от бортовой навигационной аппаратуры;
— статус (состояние) систем беспилотного летательного аппарата;
— заданную последовательность управляющих команд;
— параметры и настройки программного обеспечения.

К информационно-техническим воздействиям (ИТВ), основанным на нарушении радиообмена между беспилотным летательным аппаратом и наземным пунктом управления, можно отнести следующие:

— срыв синхронизации и/или процедуры установления связи;
— внесение нарушений в канальные или сетевые протоколы радиосети;
— переполнение входного буфера путем DOS или DDOS-атак;
— нарушение функционирования программного обеспечения микроконтроллера управления средствами радиообмена.

К информационно-техническим воздействиям (ИТВ), основанным на нарушении информационного обмена между беспилотным летательным аппаратом и наземным пунктом управления, можно отнести следующие:

— перехват управления БПЛА путем создания ложного виртуального НПУ;
— перевод БПЛА в ложный аэродинамически некорректный режим полета;
— подача на БПЛА команд на выключение или на снижение;
— подача управляющих команд на выключение бортовой полезной нагрузки;
— имитация на НПУ виртуального БПЛА.

К информационно-техническим воздействиям (ИТВ), основанным на нарушении специального программного обеспечения на БПЛА и/или НПУ можно отнести следующие:

— установка в специальное программное обеспечение компьютерных вирусов, для перехвата управления беспилотным летательным аппаратом;
— установка в БПЛА программных закладок, обеспечивающих перехват управления с помощью ложного НПУ.

ЛИТЕРАТУРА

1. Макаренко С.И., Тимошенко А.В., Васильченко А.С. Анализ средств и способов противодействия беспилотным летательным аппаратам//Системы управления, связи и безопасности. — №1, 2020. — С. 109–146. — DOI: 10.24411/2410-9916-2020-10105
2. Беспилотник упал в Минске — посмотрели, что сейчас на месте крушения// https://tochka.by/articles/incidents/bespilotnik_upal_v_minske_posmotreli_chto_seychas_na_meste_krusheniya/
3. Жарова, А.К. О возможности совершения компьютерных атак по типу man in the Middle attack с применением генеративного искусственного интеллекта /А.К. Жарова//Актуальные проблемы расследования преступлений в сфере компьютерной информации или с применением компьютерных технологий в условиях цифровизации экономики и государственного управления: Материалы Межвузовского круглого стола, Москва, 28 ноября 2024 года. — Москва: Российский экономический университет им. Г.В. Плеханова, ООО «РУСАЙНС», 2025. — С. 45–51. — EDN WLWCKL.
4. Федеральный закон от 04.08.2023 г. № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»// http://www.kremlin.ru/acts/bank/49674
5. Приказ МВД России от 30 апреля 2020 г. № 252 «Об утверждении Порядка принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях защиты жизни, здоровья и имущества граждан над местом проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-разыскных мероприятий и Перечня должностных лиц, уполномоченных на принятие такого решения».
6. Боев Н.М., Шаршавин П.В., Нигруца И.В. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния//https://uav-siberia.com/news/postroenie-sistem-svyazi-bespilotnykh-letatelnykh-apparatov-dlya-peredachi-informatsii-na-bolshie-ra/
7. Плотников, Г.Г. О модели оценки противодействия беспилотным системам /Г.Г. Плотников//Информационные технологии в деятельности органов внутренних дел: Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. — Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2024. — С. 214–215. — EDN CIMEGA.

© Плотников Герман Геннадьевич (gr175@mail.ru); Елин Владимир Михайлович (elin_vm@mail.ru);
Царегородцев Анатолий Валерьевич (tsaregorodtsev_av@pfur.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»