УДК 621.372.852
DOI: 10.53297/18293336-2025.1-100

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ГЛУШЕНИЯ ДРОНОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДА СОВПАДАЮЩЕГО СИГНАЛА

М.Ц. Айвазян, Т.А. Григорян, Л.Г. Ниазян

Национальный политехнический университет Армении

В последние годы дроны и беспилотные летательные аппараты (БЛА) активно внедряются в самые разные сферы: от аэрофотосъёмки и мониторинга до доставки товаров и спасательных операций. Доступность и быстрое развитие технологий БЛА делают их незаменимыми помощниками, однако одновременно способствуют росту угроз для безопасности. Всё чаще отмечаются случаи несанкционированного использования дронов для проникновения на охраняемые объекты, транспортировки запрещённых грузов, сбора информации и организации диверсионных или террористических актов, особенно вблизи объектов критической инфраструктуры. В связи с этим государственные органы, а также частные охранные предприятия вынуждены уделять всё больше внимания вопросам предотвращения подобных инцидентов. Подобные инциденты вызывают серьёзную обеспокоенность у специалистов по безопасности и требуют поиска новых решений для противодействия этим угрозам, а также совершенствования уже существующих методов.

Ключевой уязвимостью дронов является их зависимость от радиочастотного дистанционного управления, что даёт возможность применять различные средства радиоэлектронного подавления. Такие системы способны блокировать или искажать управляющие сигналы, препятствуя выполнению дронами опасных задач и снижая возможный ущерб. Одним из наиболее эффективных современных методов считается метод совпадающего сигнала, при котором создаётся помеха, идентичная управляющему сигналу дрона. Это позволяет более надёжно нарушать связь между оператором и аппаратом, даже если дрон оснащён помехозащищённой связью.

Однако эффективность систем глушения зависит от множества факторов: типа аппаратуры, характеристик объекта, особенностей дронов и условий эксплуатации. Данная статья посвящена анализу эффективности применения метода совпадающего сигнала в системах радиоэлектронного подавления дронов.

Ключевые слова: дроны, дистанционное управление, радиоэлектронное подавление, метод совпадающего сигнала.

Введение. Существует множество способов борьбы с гражданскими дронами [1,2], однако с точки зрения баланса стоимости и эффективности

наиболее оптимальными являются средства радиоэлектронной борьбы или глушения. Радиоэлектронное подавление сигнала увеличивает уровень шума в целевом приёмнике, что приводит к увеличению ошибок в приёмнике. Эффективность глушения определяется соотношением мощности сигнала, передаваемого глушителем, и мощности целевого сигнала.

Среди существующих методов радиоэлектронного подавления можно выделить следующие четыре (рис.1):

а) глушение с использованием широкополосного шумового сигнала;

б) монотонное глушение;

в) глушение методом развертки;

г) глушение совпадающим сигналом.

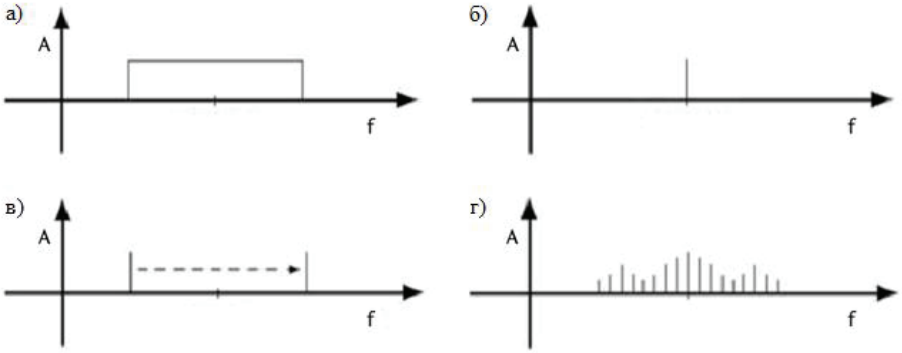

Рис. 1. Методы глушения сигнала: а- глушение с использованием широкополосного шумового сигнала; б- монотонное глушение; в- глушение методом развертки; г- глушение совпадающим сигналом

Глушение с помощью совпадающего сигнала до сих пор в основном исследовалось в беспроводных локальных сетях, построенных на основе стандартов IEEE 802.11. Результаты показали, что такой способ глушения является эффективным с точки зрения энергопотребления и низкой вероятности обнаружения [3,4].

В случае этого метода глушения необходимо заранее знать определённые параметры целевого сигнала. Такими параметрами могут быть тип модуляции, полоса излучения сигнала, несущая частота, скорость передачи данных и т.д.

Оценка эффективности метода совпадающего сигнала. Для оценки эффективности систем глушения дронов с использованием метода совпадающего сигнала была использована система обнаружения и подавления управляющих сигналов дрона, ранее представленная в [5].

Система обнаружения и подавления была построена на основе приёмопередающего устройства PXIe-5841 компании NI (National Instruments) [6].

Поскольку при реальном подавлении дрона единственным критерием качества и эффективности глушения является неуправляемость дрона, для полноценной оценки качества глушения было принято решение использовать другую приёмопередающую систему, имитирующую обмен данными между дроном и оператором. Для построения указанной системы было использовано устройство NI USRP-2954R компании National Instruments (NI) (рис.2). В приёмопередающем устройстве использовались направленные антенны. Таким образом, для проведения эксперимента по глушению антенны системы подавления управляющих сигналов дрона были направлены на систему, имитирующую обмен данными между дроном и оператором. Для реализации системы, имитирующей связь между дроном и оператором, были использованы готовые программные примеры, предназначенные для устройств NI USRP [7].

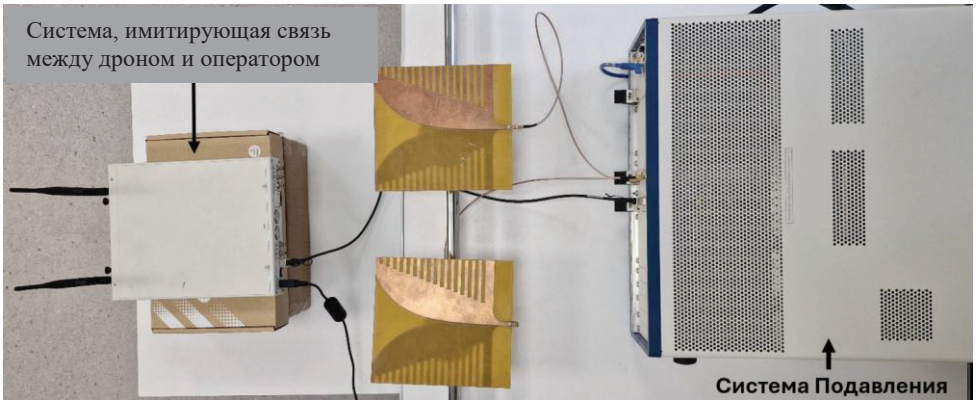

Рис.2. Тестирование системы глушения с использованием устройства, имитирующего обмен данными между дроном и оператором

Во время проведения эксперимента параметры передаваемого сигнала в обеих системах были схожими. Несущая частота сигнала составляла 2,4 *ГГц*, а частота дискретизации сигналов I и Q — 500 *кГц*.

Максимальный уровень мощности сигнала в приёмнике системы, имитирующей канал связи дрона (при отсутствии заглушающего сигнала), составлял примерно -18 *дБ*.

Для оценки эффективности метода подавления с совпадающим сигналом было проведено сопоставление данного метода с методом подавления сигнала с помощью гауссового белого шума. Основным недостатком метода подавления с гауссовым белым шумом является то, что мощность передаваe-

мого сигнала распределяется по всей ширине полосы пропускания. По этой причине такое подавление требует большей мощности передачи, чем метод подавления с совпадающим сигналом (рис.3).

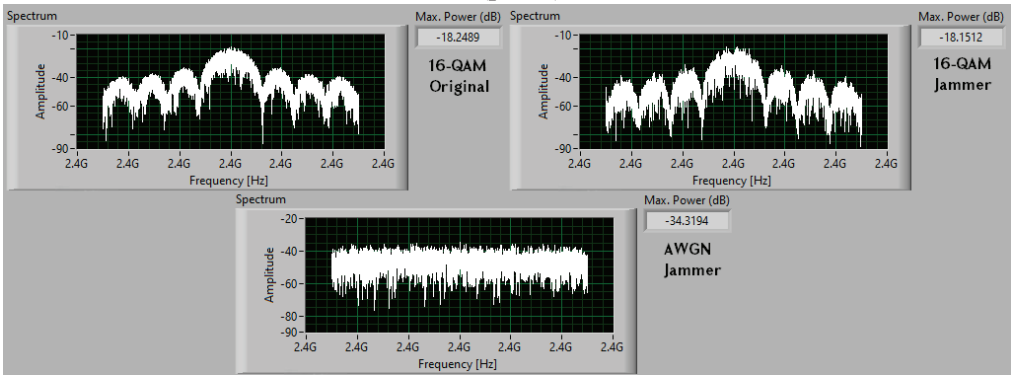

Рис.3. Спектр принятого сигнала в системе, имитирующей канал связи дрона, в случаях: отсутствия сигнала подавления, подавления сигналом 16-QAM, подавления шумовым сигналом

Во время первого эксперимента измерялся коэффициент ошибки модуляции (MER) [8]. В качестве типа модуляции сигнала здесь использовалась 16-QAM – модуляция. В приёмнике коэффициент ошибки модуляции в отсутствие подавляющего сигнала составил 30 *дБ* (рис. 4).

Максимальный уровень мощности сигнала подавления в приёмнике системы, имитирующей канал связи дрона (при отсутствии сигнала передатчика), составлял около -18 *дБ* при модуляции 16-QAM и около -34 *дБ* при использовании гауссового белого шума (рис.3).

Для оценки качества связи при подавлении вместо отношения сигнал/шум часто используют отношение мощностей информационного и подавляющего сигналов (Signal to Jamming Ratio, SJR) [9]. Таким образом, результаты проведённых экспериментов показывают, что при отношении мощностей информационного и подавляющего 16-QAM сигналов на уровне -0.3 *дБ* коэффициент ошибок модуляции в приёмнике снижается примерно до 6 *дБ*. При отношении мощностей информационного и шумового подавляющего сигналов на уровне 16 *дБ* коэффициент ошибок модуляции в приёмнике снижается примерно до 20 *дБ*. Учитывая тот факт, что для передачи 16-QAM – модуляции и шумового подавляющего сигнала использовалась одинаковая мощность, результаты эксперимента показывают, что метод подавления с

совпадающим сигналом в несколько раз эффективнее метода подавления с гауссовым белым шумом.

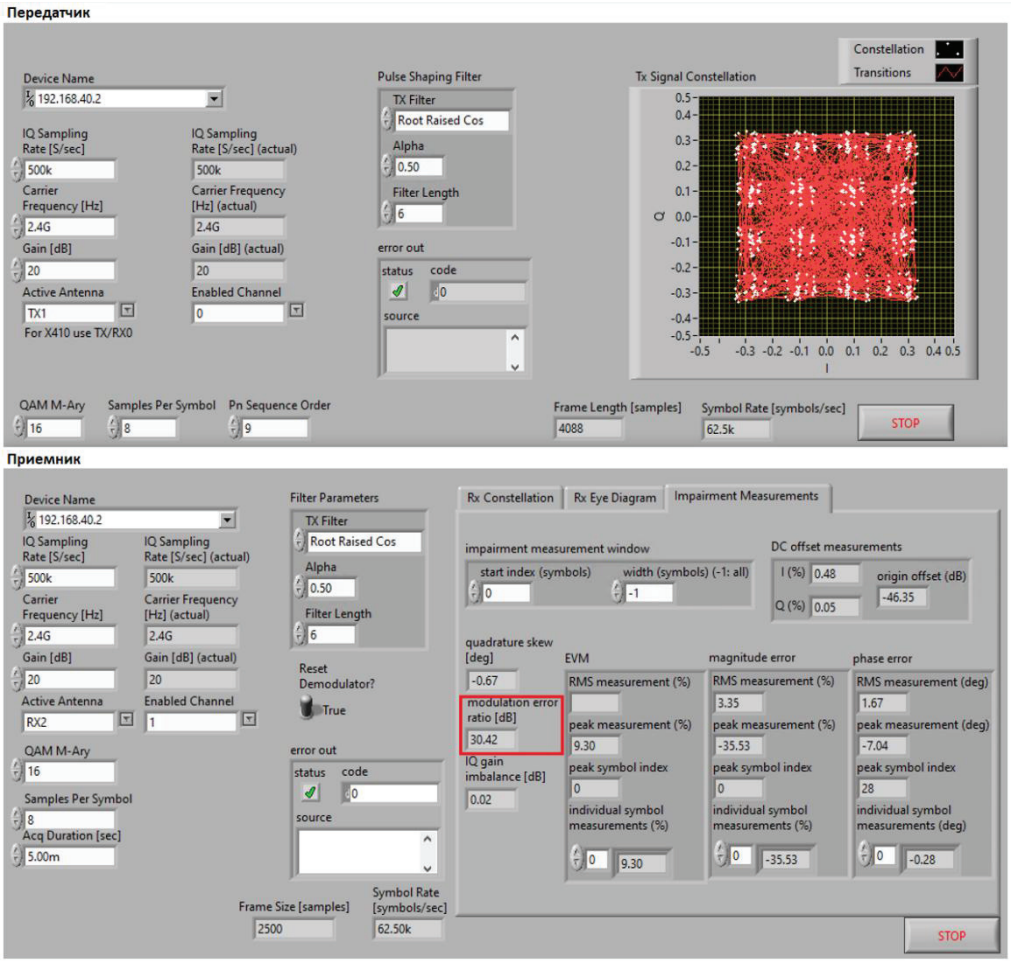

Рис.4. Лицевые панели программы измерения коэффициента ошибки модуляции в системе, имитирующей канал связи дрона

В следующем эксперименте исследовалось влияние подавляющего сигнала на восстановление передаваемых данных. Для проведения эксперимента использовались те же устройства, что и в предыдущем опыте, а для передачи и демодуляции данных в системе, имитирующей канал связи дрона, был использован другой готовый программный пример NI USRP [10]. В этом при-

мере передатчик отправляет текстовую информацию, а приёмник пытается её восстановить (рис. 5).

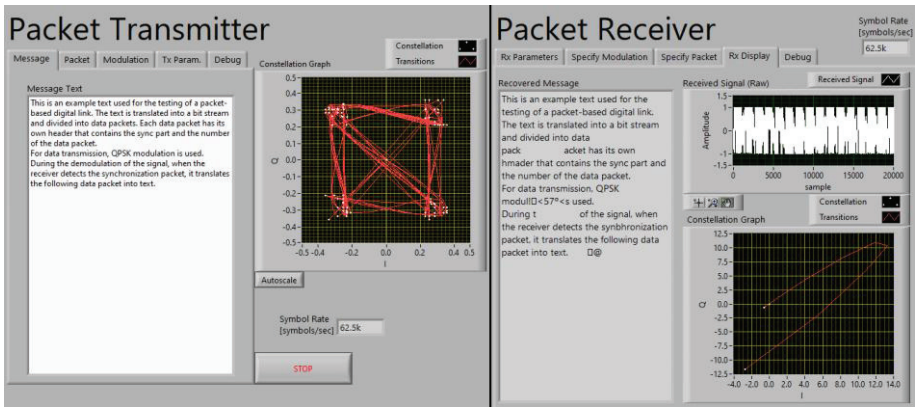

Рис.5. Лицевая панель программы для передачи и приема текстовых сообщений

Программа преобразует введённый пользователем текст в поток битов, затем разбивает его на пакеты и непрерывно передаёт в эфир.

Каждый пакет, помимо основной полезной информации, содержит номер пакета и компонент синхронизации. Приёмник после обнаружения компонента синхронизации пытается восстановить текстовую информацию и поместить её в соответствующее место по номеру пакета.

Во время проведения эксперимента несущая частота сигнала составляла 2,4 *ГГц*, частота дискретизации сигналов I и Q — 500 *кГц*, а тип модуляции — QPSK.

В условиях отсутствия подавляющего сигнала приёмник с высокой скоростью восстанавливает полный текст. Результаты экспериментов показывают, что при использовании подавляющего сигнала с модуляцией QPSK минимальное пороговое значение отношения мощностей информационного и подавляющего сигналов, при котором приёмник способен восстановить хотя бы часть текста, составляет около 7 *дБ (табл.)*. В этом случае приёмник может восстановить примерно 29,4% информации.

Таблица

Результаты экспериментов с использованием подавляющего сигнала QPSK

Сигнал/помех (*дБ*)	**Восстановленная часть (%)**	**Время восстановления (*с*)**
7	29.4%	24.3
10	83.8%	5.4
13	95.2%	2.8
15	98.4%	2.6
18	100%	2.3
21	100%	1.5
24>	100%	1.1

Заключение. Проведённые исследования подтвердили высокую эффективность метода совпадающего сигнала для радиоэлектронного подавления управляющих каналов дронов. В ходе экспериментов было показано, что данный метод, в отличие от традиционного подавления с использованием гауссового белого шума, позволяет добиться значительного снижения качества передачи управляющего сигнала при существенно меньших энергетических затратах. Это обусловлено тем, что совпадающий сигнал воздействует на целевой дрон адресно, повторяя структуру его управляющего сигнала, и тем самым существенно увеличивает вероятность разрыва связи между дроном и оператором даже при наличии помехоустойчивых средств связи на борту.

Сравнительный анализ показал, что при равных мощностях подавления коэффициент ошибок модуляции (MER) снижается гораздо быстрее при использовании метода совпадающего сигнала, чем при широкополосном шумовом подавлении.

Эксперименты по восстановлению текстовой информации также продемонстрировали, что применение совпадающего сигнала с модуляцией QPSK значительно затрудняет приём данных: уже при SJR около 7 *дБ* восстановлению было подвергнуто менее 30% информации, а при увеличении мощности подавления эффективность глушения возрастала вплоть до полной блокировки передачи.

Таким образом, метод совпадающего сигнала обладает существенными преимуществами по сравнению с традиционными методами радиоэлектронного подавления дронов: он эффективнее, требует меньших энергетических ресурсов и обеспечивает более высокий уровень адресного воздействия на целевой объект. Это делает его одним из наиболее перспективных направлений развития систем защиты от несанкционированного использования беспилотных летательных аппаратов.

Литература

1. A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones / **Castrillo V.U., Manco A., Pascarella D., et al** // Drones. – 2022. -6(3). – P. 65.
2. Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems / **H. Kang, J. Joung, J. Kim, J. Kang, et al** // IEEE Access 2020, -8. -P. 168671–168710.
3. Protocol-Aware Radio Frequency Jamming in Wi-Fi and Commercial Wireless Networks / **A. Hussain, N. A Saqib, U. Qamar, et al** // Journal of communications and networks. -2014. -16(4). P. 397–406.
4. **Thuente D. and Acharya M.** Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks // Proc. of MILCOM. - 2006. – Vol. 6. – P. 100.
5. **Григорян Т.А., Айвазян М.Ц.** Автоматическое обнаружение и распознавание цифровых модулированных сигналов с помощью нейронной сети // Известия НАН РА и НПУА. Серия технических наук. - 2024. -Т. 77, № 1. -С. 46-57.
6. https://www.ni.com/docs/en-US/bundle/pxie-5841-specs/page/specs.html
7. https://www.ni.com/docs/en-US/bundle/ni-usrp/page/ni-usrp-examples.html
8. ETSI technical report ETR 290: “Measurement Guidelines for DVB Systems” - Errata 1, May 1997.
9. **Li H.and Ye W.** A Study on the Influence of Bit Error Ratio Against Jamming Signal Ratio Under Different Channel Jamming // 2016 9th International Symposium on Computational Intelligence and Design (ISCID). -Hangzhou, China, 2016. - P. 58-61.
10. https://forums.ni.com/t5/Software-Defined-Radio/Packet-based-Digital-Link/tap/3509866

Поступила в редакцию 14.05.2025.
Принята к опубликованию 10.07.2025.

ՀԱՄԸՆԿՆՈՂ ԱԶԴԱՆՇԱՆԻ ՄԵԹՈԴԻ ԿԻՐԱՌՄԱՄԲ ԴՐՈՆՆԵՐԻ ԽԱՓԱՆՄԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ԱՐԴՅՈՒՆԱՎԵՏՈՒԹՅԱՆ ԳՆԱՀԱՏՈՒՄԸ

Մ.Ց. Այվազյան, Թ.Ա. Գրիգորյան, Լ.Գ. Նիազյան

Վերջին տարիներին անօդաչու թռչող սարքերն ակտիվորեն ներդրվել են ամենատարբեր ոլորտներում՝ սկսած օդային լուսանկարչությունից և մոնիթորինգից մինչև ապրանքների առաքում և փրկարարական գործողություններ: Դրանց մատչելիությունը և տեխնոլոգիական արագ առաջընթացը անօդաչու թռչող սարքերը դարձնում են անփոխարինելի օգնականներ, բայց, միևնույն ժամանակ, դրանք նպաստում են անվտանգության սպառնալիքների աճին: Ավելի ու ավելի հաճախ են գրանցվում անօդաչու թռչող սարքերի չարտոնված օգտագործման դեպքեր՝ պաշտպանված օբյեկտներ ներթափանցելու, արգելված ապրանքներ տեղափոխելու, տեղեկատվություն հավաքելու և դիվերսիաներ կամ ահաբեկչական գործողություններ կազմակերպելու համար, հատկապես կարևոր ենթակառուցվածքային օբյեկտների տարածքում: Այս առումով պետական մարմինները, ինչպես նաև մասնավոր անվտանգության ընկերությունները ստիպված են ավելի ու ավելի մեծ ուշադրություն դարձնել նման միջադեպերի կանխարգելման հարցերին: Նման միջադեպերը լուրջ մտահոգություններ են առաջացնում անվտանգության մասնագետների շրջանում և պահանջում են նոր լուծումների որոնում այդ սպառնալիքներին հակազդելու, ինչպես նաև առկա մեթոդների կատարելագործման համար:

Անօդաչու թռչող սարքերի հիմնական խոցելիությունը դրանց կախվածությունն է ռադիոհաճախականության հեռակառավարման համակարգից, որը հնարավորություն է տալիս օգտագործել էլեկտրոնային հակազդեցության տարբեր միջոցներ: Նման համակարգերը կարող են արգելափակել կամ աղավաղել կառավարման ազդանշանները՝ կանխելով անօդաչու թռչող սարքերի՝ վտանգավոր առաջադրանքներ կատարելը և նվազեցնելով հնարավոր վնասը: Ամենաարդյունավետ ժամանակակից մեթոդներից մեկը համարվում է համընկնող ազդանշանի մեթոդը, որը ստեղծում է անօդաչու սարքի կառավարման ազդանշանին նույնական միջամտություն: Սա թույլ է տալիս օպերատորի և սարքի միջև կապի ավելի հուսալի խափանում, նույնիսկ եթե դրոնը հագեցած է միջամտությանը դիմացկուն կապի համակարգով:

Սակայն խլացման համակարգերի արդյունավետությունը կախված է բազմաթիվ գործոններից՝ սարքավորումների տեսակից, օբյեկտի բնութագրերից, անօդաչու թռչող սարքերի առանձնահատկություններից և շահագործման պայմաններից: Այս հոդվածը

նվիրված է անօդաչու թռչող սարքերի էլեկտրոնային հակազդեցության համակարգերում համընկնող ազդանշանի մեթոդի կիրառման արդյունավետության վերլուծությանը:

Առանցքային բառեր. անօդաչու թռչող սարքեր, հեռակառավարում, էլեկտրոնային հակազդեցություններ, համընկնող ազդանշանի մեթոդ:

ASSESSING THE EFFICIENCY OF DRONE JAMMERING SYSTEMS USING THE COINCIDENCE SIGNAL METHOD

M. Ts. Ayvazyan, T. A. Grigoryan, L. G. Niazyan

In recent years, drones -unmanned aerial vehicles have been actively introduced into a variety of areas, from aerial photography and monitoring to delivery of goods and rescue operations. Their availability and rapid technological development make UAVs indispensable assistants, but at the same time contribute to the growth of security threats. There are increasingly frequent cases of unauthorized use of drones to penetrate protected facilities, transport prohibited goods, collect information, and organize sabotage or terrorist acts, especially near critical infrastructure facilities. In this regard, government agencies, as well as private security companies, are forced to pay more and more attention to the prevention of such incidents. Such incidents cause serious concern among security experts and require to search for new solutions to counter these threats, as well as the improvement of the existing methods.

The key vulnerability of drones is their dependence on radio frequency remote control, which makes it possible to use various means of electronic suppression. Such systems are capable of blocking or distorting control signals, preventing drones from performing dangerous tasks and reducing possible damage. One of the most effective modern methods is the coincidence signal method, which creates interference identical to the drone's control signal. This allows for more reliable disruption of communication between the operator and the device, even if the drone is equipped with interference-resistant communication.

However, the effectiveness of jamming systems depends on many factors: the type of equipment, the characteristics of the object, the features of the drones and the operating conditions. This article is devoted to the analysis of the effectiveness of the coincidence signal method in drone electronic suppression systems.

Keywords: drones, remote control, electronic suppression, the coincidence signal method.