

**Пальчиков Владимир Александрович**, студент,  
ФВУНЦ ВВС «ВВА», РФ, г. Челябинск  
Vladimir Palchikov, student,  
FVUNTS VVS «VVA»,  
Russia, Chelyabinsk

**Болотников Александр Сергеевич**, студент,  
ФВУНЦ ВВС «ВВА», РФ, г. Челябинск  
Alexandr Bolotnikov, student,  
FVUNTS VVS «VVA»,  
Russia, Chelyabinsk

Научный руководитель:  
**Попов Юрий Леонидович**,  
кандидат исторических наук, доцент  
ФВУНЦ ВВС «ВВА», РФ, г. Челябинск  
Yuriy Popov, scientific supervisor,  
FVUNTS VVS «VVA», Russia, Chelyabinsk

## **ДРОНЫ – КАК СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ UNMANNED AERIAL COMBAT VEHICLE AS WAY TO SECURE INFORMATION**

**Аннотация:** в данной статье представлен анализ способов защиты информации с помощью бесплотных летательных аппаратов (дронов) преимущественно в военной сфере. Выдвинуты основные преимущества и недостатки каждого из методов защиты информации. Описываются перспективы развития способов ретрансляции данных и постановки помех с помощью дронов. Делается вывод по каждому элементу воспрепятствования «утечки» данных. Выдвигается мнение о новшестве применения дронов, их универсальности, надёжности и эффективности использования в военной сфере.

**Abstract:** this article presents an analysis of protection methods information using unmanned aerial combat vehicles (drones), primarily in the military sphere. The main advantages and disadvantages of each method of information protection are put forward. The prospects for the development of methods for retransmitting data and jamming using drones are described. A conclusion is made on each element of preventing data «leakage». An opinion is put forward on the innovation of using drones, their versatility, reliability and effectiveness of use in the military sphere.

**Ключевые слова:** БпЛА, дрон, защита информации, постановка помех, ретрансляция данных, передача данных, централизованное управление, децентрализованное управление, перспективы.

**Keywords:** UACV, drones, information security, jamming, data relay, data transmission, centralized control, decentralized control, prospects.

Множественность способов разведки информации показала проблему обеспечения её сохранности имеющимися методами и необходимость более эффективного подхода к недопущению «утечки» данных.

Развитие технологий и информационной сети позволило человечеству общаться между собой на расстоянии, видеть друг друга по видеосвязи, совершать покупки, путешествовать и многое другое. Вместе с этим развиваются и способы «утечки» этой самой информации, потеря которой для каждого её владельца является проблемой.



На примере пользования информацией при ведении боевых действий, при потере передаваемых сведений противник узнаёт о местоположении, вооружении, дальнейшего хода противоборствующей стороны и т. д. и, несомненно, овладевает инициативой.

В связи с этим применение беспилотных летательных аппаратов (БПЛА), или же дронов, в целях защиты информации от несанкционированного доступа является перспективным, новым, а также передовым способом защиты информации.

БПЛА – техника, которая способна автономно перемещаться в воздухе и не требуется непосредственного пилотирования. Аппараты управляются с помощью пульта или бортового компьютера [2].

В разговорной речи применяется эквивалентное понятие – дрон, которое мы в последующем будем использовать.

Как способ защиты информации дронов можно использовать в качестве ретранслятора данных между связными дронами с возможностью перекодировки, постановки помех для воспрещения радиолокационной разведки и физическая защита информации.

Рассмотрим способ ретрансляции информации с перекодировкой.

COFDM является наиболее широко используемой технологией передачи данных между дронами, который характерен высокоскоростной передачей данных и высокой пропускной способностью, которой достаточно для передачи HD-видео. Она работает по принципу передачи данных от передающего устройства через дрон и на принимающее устройство [3].

Существует система, которая обеспечивает передачу данных на большие расстояния через связь между многими передающими дронами. Однако также существует вероятность «утечки» данных. Для обеспечения безопасности передачи информации необходимо производить шифрование данных, с этой задачей справляются программно-аппаратные комплексы, которые монтируются в дрон и обеспечивают шифрование данных.

Одним из таких комплексов выступает С-Терра – программно-аппаратный комплекс для обеспечения безопасности сети, по сути же представляет собой классический шлюз безопасности (криптошлюз, криптомаршрутизатор). Как и большинство других конвергентных устройств, устройство С-Терра, помимо функции сетевого шифрования, обеспечивает поддержку межсайтовых VPN. Её аналог модель 10G, хотя и имеет много общего, имеет другое назначение: она предназначена для защиты отдельных высокоскоростных каналов связи на режиме «точка-точка» [4].

Такая система обеспечивает быструю передачу данных на большие расстояния, включая передачу HD- видео. Имеются отрицательные стороны, например: система парализуется как только из строя выходит один из дронов. Для решения таких проблем необходимо располагать дронами на различном интервале, дальности и высоте.

В перспективе развития этого способа защиты информации создан опытный образец дрона-конвертоплана «Настасья», который имеет возможность вертикального взлёта и посадки, как квадрокоптер, и при этом оснащён самолётным крылом для повышения скорости и дальности полёта. Основное назначение «Настасьи» – ретрансляция сигнала. Радиус действия БПЛА при этом составляет 100 км [5].

Также осенью 2023-го в зоне проведения специальной военной операции завершились испытания комплекса «Воробей», который использует ретранслятор «Облачко». Дальность полёта дрона достигает 5 км, полезная нагрузка – 2,6 кг. При этом для поддержания связи между оператором и БПЛА используются нестандартные частоты [5].

Вторым способом защиты информации является использование дронов – постановщиков помех, а именно постановщиков заградительных помех, которые создают некую зону импульсных сигналов, воспрепятствующую несанкционированному доступу к информации.



Многие специалисты скептически относятся к возможности эффективной постановки заградительной помехи против разведки. Это связано прежде всего с тем, что необходимо поставить помеху в очень большом диапазоне частот, приблизительно от 20 МГц до 1 ГГц, и это значит, что постановщик помех должен иметь неприемлемо большую мощность [6].

Отсюда вытекает главный недостаток – высокие нагрузки на систему дрона и большие затраты на производство этого аппарата и внедрения в него устройства постановки помех. Тем более, необходим источник питания большой мощности, обеспечивающий непрерывную и бесперебойную работу, что увеличивает габариты дрона и повышает его заметность.

Положительной стороной заградительных помех можно выделить его варьлируемый масштаб покрываемой зоны, будь то здание, комната или участок местности.

На данный момент наиболее передовыми устройствами являются генераторы помех, предназначенные для защиты от утечки информации по каналам побочных электромагнитных излучений от электронно-вычислительной техники, один из примеров такого устройства отечественный стационарный генератор шума "Гном-3" [6].

Третьим способом защиты информации выделяется физическая защита информации, основанная на использовании дрона или же групп дронов в качестве патрульных аппаратов, исключающих видовую разведку информации, то есть наблюдения.

Централизованное и децентрализованное управление дронами позволяет в реальном масштабе времени сканировать участки местности с целью выявления способов утечки информации.

Централизованное управление – способ, при котором существует выделенный наземный центр управления, из которого оператор осуществляет контроль над группой дронов. Необходимые вычисления и обработка информации происходит в наземном центре управления. При этом, оператор может осуществлять управление полётом и обмен информацией с каждым дроном из группы [1].

Преимуществом такого управления дронов является простота реализации процессов подачи управляющих команд и обмена информацией, относительная стабильность, использование более простых алгоритмов.

Недостатком такого управления является то, что оно теряется, как только наземная станция или оператор выходят из строя или подвергаются внешнему силовому воздействию.



Рис. 1 Схема, централизованной архитектуры управления



Децентрализованное управление – это способ, при котором основной объём вычислений производится не в наземном центре управления, а в дроне. Группа соседствующих дронов образует однотипную сеть. Ближайший «ведущий» дрон связывается с инфраструктурой, связь между любыми двумя дронами в архитектуре многослойной децентрализованной сети группы не требует ретрансляции инфраструктуры [1].

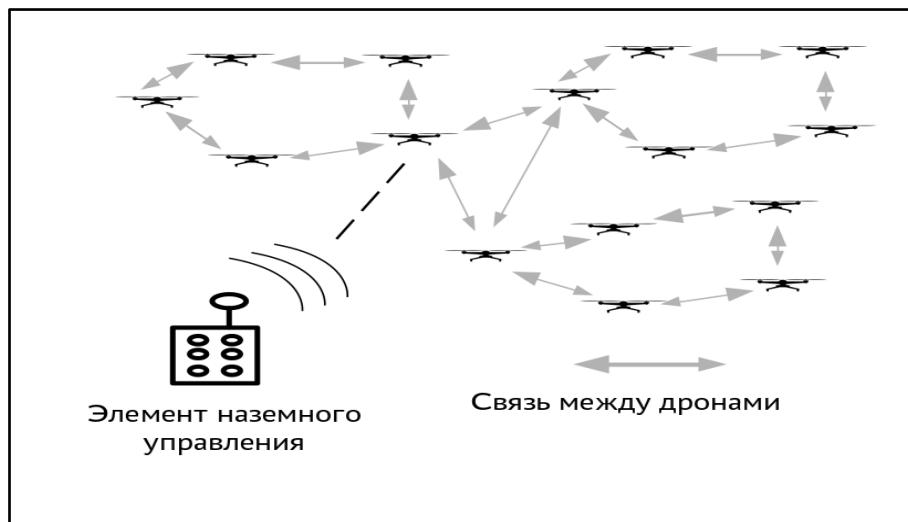


Рис. 2 Схема, мультигрупповой децентрализованной сети

Преимуществом такой децентрализованной сети является автономность работы группы.

Недостатком является то, что такие функции будут обеспечиваться более сложными алгоритмами управления и развитой аппаратной частью.

Таким образом, при выборе способа защиты информации с помощью дронов необходимо учитывать цель мероприятий по защите данных от несанкционированного доступа, при этом необходимо понимать затрачиваемые ресурсы и средства на той или иной метод защиты.

#### Список литературы:

1. А.А. АБЛЕЦ, А.Н. СТРЕБКОВ, Е.В. ЗАВГОРОДНЯЯ Опыт создания роя БПЛА в вооруженных силах иностранных государств //ВОЕННАЯ МЫСЛЬ № 6 – 2022 С. 137-146
2. Беспилотный летательный аппарат [Электронный ресурс] – Режим доступа. – URL:[https://old.bigenc.ru/technology\\_and\\_technique/text/2142467](https://old.bigenc.ru/technology_and_technique/text/2142467) (дата обращения 13.04.2025)
3. 5 лучших технологий беспроводной связи для передачи видео с дронов на большие расстояния [Электронный ресурс] – Режим доступа. – URL: <https://www.iwavecomms.com/ru/news/top-5-wireless-communication-technologies-for-long-range-drone-video-transmitting/> (дата обращения 13.04.2025)
4. Устройства постановки помех [Электронный ресурс] – Режим доступа. – URL: <https://info.wikireading.ru/238193?ysclid=m999yb4l8q312496312> (дата обращения 13.04.2025)
5. Взгляд за горизонт: как в России идёт разработка дронов-ретрансляторов [Электронный ресурс] – Режим доступа. – URL: <https://russian.rt.com/russia/article/1268863-dron-retranslyator-nastastya> (дата обращения 13.04.2025)
6. Устройства для сетевого шифрования: плюсы и минусы [Электронный ресурс] – Режим доступа. – URL: <https://systempb.ru/company/articles/shest-ustroystv-dlya-setevogo-shifrovaniya-plyusy-i-minusy/?ysclid=m99aezct7772881794> (дата обращения 13.04.2025)

