



Противодействие

беспилотным системам

семинар в НИУ «МЭИ» 31 марта 2025 г.

Участники:

- 1) представитель «Кристофор и Никас»;
- 2) представитель КБ «Чистое небо»;
- 3) представитель МО;
- 4) представитель Департамента региональной безопасности и противодействия коррупции города Москвы;
- 5) представитель ВУЦ МЭИ;
- 6) представитель АО ДПО Луис+;

- 7) представитель ООО «СТЭК КОМ»;
- 8) представитель НПО «Алмаз»;
- 9) представитель Фонда Национальной Технологической Инициативы (Фонд НТИ);
- 10) представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ;
- 11) представитель ФГАОУ ВО КФУ;
- 12) представитель НИУ «МЭИ»;
- 13) представитель НИУ «МЭИ»;
- 14) представитель НИУ «МЭИ»;
- 15) представитель НИУ «МЭИ».

Повестка:

О возможности перехвата каналов управления БЛА.

Предложения по итогам:

1. Принять к сведению информацию материалов докладов.

Стенограмма семинара (2 часа 30 минут)

Представитель НИУ «МЭИ»

Здравствуйте, уважаемые коллеги, товарищи. Мы начинаем очередной семинар по противодействию беспилотным системам. Сегодня у нас 31 марта. Мы, как обычно, проводим семинар. Напоминаю, что семинар является ме-

роприятием открытым. Здесь не надо упоминать ничего, что является информацией ограниченного доступа. Наша беседа записывается, как вы видите, на аудионоситель. Потом расшифровываем в стенограмму и выкладываем на общее пользование. Когда мы все выключим можно будет там, если нужно, кому-то обсудить какие-то более тонкие вопросы, но обращаю внимание - только открытая информация. На семинаре мы выработали такой базовый подход, что у нас участники представляют одну из трех возможных ипостасей, а именно: либо это заказчик решений, потребитель, либо это носитель компетенций, который готов какие-то запросы отрабатывать в силу своей компетенции, объединяясь с другими, либо третья ипостась это проводник к ресурсам или владелец ресурсов для проведения тех или иных разработок или других мероприятий. Мы сейчас представимся и каждый из нас сам скажет, в какой ипостаси он выступает, чтобы остальные участники семинара это понимали отчетливо.

У нас есть часть участников, которые не первый раз, есть те, кто участвует впервые, поэтому мы всегда представляемся по очереди, чтобы все знали - с кем имеют дело. Начнем, как всегда, с меня.

Я представляю Институт радиотехники и электроники МЭИ. И представляю группу носителей компетенции.

Напоминаю, мы в стенограмме имя, отчество, должность уберем, оставим только привязку к организации.

Представитель НИУ «МЭИ»

Я представляю Московский Энергетический Институт, являюсь носителем компетенций.

Представитель НИУ «МЭИ»

Я представляю кафедру формирования и обработки радиосигналов МЭИ, и представляю группу носителей компетенций.

Представитель «Кристофор и Никас»

Я, представляю «Кристофор и Никас». Те технологии, которые нам понадобятся.

Представитель КБ «Чистое небо»

Я представляю КБ «Чистое небо». Представляю компетенции.

Представитель МО

Я представляю МО. Выступаю в роли заказчика.

*Представитель Департамента безопасности и противодействия коррупции
Правительства Москвы*

Я представляю Департамент безопасности и противодействия коррупции
Правительства Москвы. Здесь выступаю в роли проводника к ресурсам.

Представитель ВУЦ МЭИ

Я представляю ВУЦ МЭИ. Выступаю в роли заказчика и носителя компетенций.

Представитель АНО ДПО Луис+

Я представляю компанию Луис+. Выступаю в роли заказчика.

Представитель ООО «СТЭК КОМ»

Я представляю ООО «СТЭК КОМ». Выступаю в роли носителя компетенций.

Представитель НПО «Алмаз»

Я представляю НПО «Алмаз». Выступаю в роли носителя компетенций.

Представитель Фонда национально-технологической инициативы

Я представляю Фонд Национальной Технологической Инициативы. Исполняю роль проводника.

Представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ

Я представляю ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ.

Представитель НИУ «МЭИ»

Представьтесь, пожалуйста, чтобы коллеги Вас услышали.

Да, поэтому мы сделали исключение для вас, мы обычно по ВКС никого не подключаем. Итак, мы все представились. Сегодня основная тема нашего семинара — это вопросы технологических возможностей по перехвату канала управления БЛА.

У нас есть ряд сообщений на эту тему. С кого мы начинаем? Первым докладывает наш коллега.

Для подключившихся по ВКС презентацию мы сейчас скинем. И давайте тогда начинать.

Представитель НИУ «МЭИ»

Добрый день, уважаемые участники семинара, мой доклад является стартовым, по сути, затравочным. Я приведу небольшой обзор. Была поставлена задача сделать определенный обзор по теме нашего семинара, прошу воспринимать его не как истину в последней инстанции, а как пищу для размышлений. Определенные выводы я сделал, соответственно они будут представлены, но это будет как раз-таки предметом для дискуссии.

Как вы видите, в названии темы я ограничился тактическими беспилотными летательными аппаратами. Почему я это сделал? Потому, что если мы начнем рассматривать вообще тему любых беспилотных летательных аппаратов, то мы, конечно же, сразу же упрёмся в терминологию, и в классификацию.

Классификация самая разнообразная. Есть принятые в России, есть принятые, например, в странах НАТО. В принципе, плюс-минус она одинаковая. Но конкретно для нашего семинара я хотел бы конкретизироваться на классе малых тактических БЛА.

Для того, чтобы раскрыть, что такое малые тактические БЛА. Я буду называть этими аппаратами беспилотные летательные аппараты коптерного типа: квадрокоптеры, мультикоптеры, и беспилотные летательные аппараты самолетного типа, которая подходит под определенные критерии. Взлетная масса до 30 килограмм, конечно, я сразу отсекаю всякие тяжелые мультикоптерные системы типа «Баба-Яга», которые управляются по Starlink.

Starlink я в данном докладе трогать не буду. Так как это все-таки неподъемная тема с точки зрения анализа противодействия. И сравнительно неболь-

шая дальность полета. Под эти критерии подпадают дроны-камикадзе, которых на ЛБС большинство. Поэтому эта тема нас больше всего сейчас интересует в плане противодействия им. Ну и, также я здесь затрагиваю класс коммерческих беспилотных аппаратов. Это DJI, Autel, которые используются для разведывательных целей и в качестве легких бомбардировщиков, так скажем, так как они оборудуются системами сброса.

У таких БЛА в качестве двигателя используются обычные электрические двигатели. Питание осуществляется за счет электрической батареи, то есть никаких там двигателей внутреннего сгорания, мини реактивных двигателей, всякой экзотики, мы это не трогаем.

Задачи, выполняемые этими аппаратами, тоже известны. В первую очередь это ударные задачи и разведывательные. Кроме того, сейчас они выполняют задачи транспортные, ретрансляционные по обеспечению радиосвязи, в том числе для увеличения дальности действия самих этих беспилотных аппаратов.

Как мы знаем, уже практически год развивается направление управления дронами по оптоволокну. Но мне кажется, все равно никогда оптоволокну не заменит радиоуправление. Оптоволоконные дроны займут свою нишу, так скажем, небольшую долю, но большинство тактических дронов будут, скорее, всего на радиоуправлении.

Здесь приведена некоторая схема, она достаточно известная. Ну, значит, в базовом варианте, радиолюбительском, для организации управления дроном достаточно пульта управления и самого дрона. Но когда мы сталкиваемся со специальным применением беспилотных аппаратов, то мы должны обеспечить не только, так скажем, обычную радиосвязь, но у нас накладываются определенные требования по обеспечению дальности и помехозащищенности. Соответственно, управляя с Земли, добиться большой дальности радиосвязи невозможно. Нужно использовать либо воздушные ретрансляторы, либо размещаемые на каких-то высотных зданиях.

Это один момент. Второй момент — это безопасность расчета. Должна быть система выноса. Она организуется посредством включения некоторых модулей дополнительных к пульту, это так называемые, JR-модули. Дальше, здесь не приведено на схеме устройство, это сумматор, который объединяет сигнал очков, управления, и телеметрии.

Затем по витой паре это все подается на выход, так скажем. Либо, как я сказал до этого, организуется ретрансляция по воздуху. Дальше, соответственно, на самом Дроне-камикадзе присутствует мощный видеопередатчик.

И, как раз, все современные системы обнаружения, построены сейчас на анализе и демодуляции такого сигнала. Так как это нешифрованный аналоговый канал, аналогового видеопередатчика. Но то, что нас будет интересовать сейчас, это маленький приемник на чипе LoRa. Здесь приведены две антенны, это так называемый диверсити-приемник. В моем обзоре я ограничиваюсь только передатчиком и приемником радиуправления, то есть видео я затрагивать не буду.

Небольшая ремарка про телеметрию. В принципе, есть разработки, где передается телеметрия, но этот канал достаточно сильно разнесен от канала управления, для того чтобы не демаскировать сам канал управления. Потому, что если, кроме видеопередатчика, дрон еще будет излучать с меньшей мощностью сигнал дополнительной телеметрии, в диапазоне близком к сигналу управления, то это будет как раз-таки очень хорошей подсказкой, так скажем. И поэтому все пользуются on-screen display (OSD), то есть выводят всю телеметрию на картинку и по видео передают.

Все, тогда идем дальше. Протоколы радиуправления БПЛА. Есть протоколы классические, которые еще известны с радиолюбительских времен, это FrSky, допустим, или там Spectrum. Это древние протоколы, соответственно, они абсолютно не годятся для специальной задачи.

И поэтому, я предлагаю рассмотреть три основных протокола: это, во-первых, DJI Ocusync. Ввиду того, что продукция DJI, по сути, доминирующая сейчас в коммерческих дронах, будет интересно с ней познакомиться. И два протокола, которые касаются FPV -дронов-камикадзе, кустарных, изготавливаемых полупромышленным способом.

TBS Crossfire, это закрытый, проприетарный протокол с более дорогим оборудованием, чем ExpressLRS. ExpressLRS, соответственно, открытый протокол, он кастомизируется, модернизируется, добавляются дополнительные ответвления. Мы немножечко коснемся их. Ну вот, как раз-таки, я их ввел в группу сторонних протоколов, так называемых кастомных.

Это вот Гермес, Кузнечик, украинский MILELRS и есть PrivacyLRS. Я о них расскажу с точки зрения безопасности самого ELRS. То, что нас, по сути, интересует в этом семинаре. Начну с DJI. Раньше, как только DJI вышел на рынок, он использовал, по сути, Wi-Fi. Конечно же, им хотелось иметь

свой собственный защищенный протокол, но, если так проанализировать, ту продукцию, которую они сейчас поставляют, есть протокол Ocusync, но он очень похож на Wi-Fi подобный, даже, может быть, не Wi-Fi - подобный, а OFDM - подобный. OFDM это такой специальный тип сигнала, сложный, композитный радиосигнал, который состоит из множества поднесущих. Такой сигнал обеспечивает большую скорость передачи данных, что и требуется для этого протокола. Потому, что Ocusync, по сути, это гибридный протокол, который неразрывно в самом протоколе передает и управление, и видео, и телеметрию. То есть, отдельного протокола для передачи сигналов управления в DJI нет. Он как раз-таки в Ocusync тоже интегрирован, получается. То есть, примером является LTE. Если вскрыть DJI, такие работы проводились. Проводился реверс-инжиниринг DJI не на уровне прошивок, а на уровне, который позволяет воспроизвести радиопrotocol. Там используются доступные чипы LTE, только с прошивкой, которая является собственностью фирмы DJI. Те, кто используют дроны DJI, знают, что была большая уязвимость на начальном этапе СВО. Эти дроны можно было с помощью так называемого «Аэроскопа», производства DJI, легко найти. «Аэроскоп» это аппаратный комплекс. Он есть стационарный, был портативный носимый. На него цены с начала войны взлетели до небес. DJI, так как она выполняет все нормы законодательства в США, в России, в Китае, соответственно он в нешифрованном виде передает координаты, причем не только дрона, но и оператора, и поэтому «Аэроскопы» на начальном этапе войны использовались для выявления расчетов. Потом появилась прошивка 1001, которая как раз-таки эту функцию DroneID отключила.

Причем не только DroneID, а всякие запреты на полеты, безопасные зоны и так далее. То есть основная уязвимость, была решена, по сути, народными умельцами, программистами. С нашей стороны, со стороны противника, уже проблемы DroneID нету. Значит, по поводу самого трафика. На текущий момент нет никаких работ по выявлению, и по декодированию трафика DroneID DJI. Он может только спуфиться по каналу навигации. Опять-таки, сейчас есть различные приспособления, которые отключают навигацию на этом дроне и, соответственно, есть прошивки, которые полностью переделывают прошивки коммерческих беспилотных аппаратов под боевые задачи.

По Autel ничего не могу сказать, доля маленькая. Есть, соответственно, преимущество Autel за счет того, что есть диапазон 900 МГц. Но этим, по сути, преимущество и заканчивается. Ввиду того, что все научились работать с большой номенклатурой линейкой, в принципе, все их используют.

Соответственно, подмену каналов управления осуществить очень сложно. Причина простая, это - криптографический канал, то есть там встроено шифрование.

В отличие от DJI, у них самая печальная, самая страшная птичка. Технически она может поддерживать 15 диапазонов. Прошивки под Autel тоже есть. Проблема заключается в том, что у них открытая архитектура. Если эта птичка с прошивкой попадает к противнику, то противник попадает с прошивкой. Поэтому они удешевляются именно с этой целью. Но 15 диапазонов, учитывая, что это все растет, это очень серьезная угроза. То есть подавить дрон, который летает на 15-ти диапазонах частот, вы не сможете. Можно подавить обычный DJI на 2.4, 5.8. с фаршировкой или без фаршировки.

Ну, и по поводу DJI, все-таки его же научили перестраивать и на 2.3, и на 2.6.

Ну, и помимо всего этого, в продаже появились, например, All-Inter.

Представитель НИУ «МЭИ»

Есть предложение, дискуссию на эту тему провести чуть позже, давайте дослушаем выступление докладчика. Это содержательное замечание, но просто иначе мы сейчас уйдем в сторону.

Как я уже сказал, я же не претендую на то, что вся приводимая мною информация окончательная и не подлежит дальнейшему развитию, мы проводим семинары, чтобы обмениваться мнениями. Я не работаю в сфере дронов, это все, по сути, хобби. Давайте я тогда, может быть, перейду к следующему пункту. Это TBS Crossfire. Система начала массово применяться в FPV-дронах, за счет того, что не нужно ничего настраивать. Купили, из коробки все присутствует, то есть поставили, и полетели. Поэтому TBS Crossfire приобрел популярность. Минусом, является дороговизна оборудования, потому что за JR-модуль, вот он слева показан, нужно заплатить сейчас от 25 тысяч рублей, что, конечно, не идет ни в какое сравнение с ELRS, тем же самым.

Что здесь? Здесь уязвимость будет, как и с ExpressLRS. Во-первых, на уровне физического формирования сигнала это протокол, который работает на модуляции LoRa, т.е. он использует чипы Semtech, монополизатор рынка чипов LoRa. Потому, что это их технологии, они в 2014 году ее запатентовали, и она, кстати, закрытая, то есть все статьи, касаемые LoRa, это реверс инжиниринг.

То есть люди, используя опыт работы с LoRa, пишут статьи, пытаются воспроизвести, но, соответственно, это лицензионная технология. То есть, конкурентов у Semtech нет. Это единственный производитель. В этом кроется минус как нашей радиосвязи, так и радиосвязи противника.

Даже если взять Гермес, который считается «продвинутым», он тоже строится на чипах LoRa. Просто немножко других, так скажем. Значит, во-первых, тип модуляции известен, да, там есть некоторые параметры, которые можно изменять, по сути, а дальше - прошивка. Но изначально, так как TBS Crossfire я прошу прощения, не сказал один момент про LoRa. Почему LoRa? Да, потому что LoRa обеспечивает минимальный бюджет радиоканала среди известных типов модуляции.

Если мы сравним LoRa с FSK, то есть с частотной модуляцией, с фазовой модуляцией, то LoRa за счёт линейной частотной модуляции обеспечивает очень высокую помехозащищённость. Плюс, дополнительно, используется режим ППРЧ. ППРЧ, как может многим показаться, нужно для того, чтобы снизить воздействие РЭБ. Но в изначальном варианте этого протокола там достаточно узкополосная ППРЧ, и она необходима не для того, чтобы минимизировать воздействие РЭБ, а для того, чтобы однотипные приемники-

передатчики между собой не конфликтовали. У разработчиков на начальном этапе не было никакого шифрования трафика. Почему? Потому что для войны этот протокол специально не готовился. Он появился до войны, появился для радиолюбителей и не предполагал никакого шифрования. Так как шифрование ставит запрет на легальную продажу технологии, например, в России. Потому, что нужны сертификаты соответствующих органов, если у вас используется шифрование, трафика и так далее. Соответственно, как только началось применение их для боевых дронов, был введен режим шифрования. Он вводится на уровне прошивки, требуется кое-что дописать и поставить галочку, условно в конфигураторе. Не все это знают, и часто те пользователи, которым приходят эти модули в виде помощи от волонтеров, это не делают. Этот ТПС ничем не отличается от открытого ELRS, в таком случае. И там будет крыться уязвимость, о которой я буду говорить на примере ELRS. Значит, если вы ставите модуль инкрипшен, то в конфигураторе, TBS нельзя никак подменить и воспроизвести. То есть послать дизарма на дрон вы не сможете. Для этого вам нужно знать криптографический ключ, а это в современных условиях невозможно выявить, если вы только не обладатель этой аппаратуры.

ELRS - это абсолютное большинство протоколов, он используется в чистом виде, под него очень большая поддержка. Если вы зайдете непосредственно на сайт ELRS, есть, кстати, русскоязычный сайт, там есть все - вплоть до печатных плат, до исходного кода прошивок печатной платы со всеми спецификациями компонентов. Берите сами паяйте и запускайте. Соответственно, открытая система - она с одной стороны позволяет, если есть команда разработчиков, знающих как его модифицировать, превратить его в настоящую защищенную радиосвязь. Что, в принципе, команды у нас и на той стороне делают вполне успешно. Но если использовать ELRS из коробки, то мы получаем серьезные уязвимости. В первую очередь, это касается любых протоколов, которые там работают, в том числе на ППРЧ. Дело в том, что приемники и передатчики должны синхронно переключать частоты. Для начала, они же должны договориться каким-то образом. Они договариваются вначале, при привязке дрона к пульту. Это так называемый бинд, то есть привязка происходит через бинд-фразы, и соответственно, если вы используете ELRS из коробки, то набор этих бинд-фраз он стандартный и, соответственно, у вас, по сути, протокол будет не защищён в таком случае.

То есть противник,... давайте я не буду забегать, я там в следующий слайд покажу уже разработку украинцев на эту тему, эксплуатирующие эту уяз-

вимость. Значит, соответственно, используется очень примитивный протокол MD5 для вычисления хэш-функции, для вычисления последовательности частот. Эта хэш-функция и этот протокол известны. То есть MD5 криптографически не является стойким. Соответственно, большого труда не требуется для того, чтобы, зная бинд-фразу, зная этот протокол хэш-функции, внедриться в протокол радиосвязи. Еще один момент. Это пакеты синхронизации, которые тоже привязаны к этому UID, который вычисляется по бинд-фразе. И, соответственно, если противник знает бинд-фразу или знает синхропакеты нешифрованные, хотя бы какую-то информацию о радиоканале, знает packet rate, то есть темп выдачи пакетов.

Я здесь привел эту таблицу с чипами Semtech, семейства SX128x, SX127x, и в ней приведены типы модуляции и packet rate 200 Гц, 100 Гц. Соответственно, если мы используем диапазон 900 МГц и ниже, то есть чипы SX1276, самые популярные, то у нас, по сути, packet rate это 250-500-100-200. Всего 4 набора пакет рейта, а тип модуляции известен. В таком случае ExpressLRS, который не обладает шифрованием и построен на вот этих чипах в нижнем диапазоне частот, он уязвим.

И следующий слайд, это разработка украинцев, там шильдик фирмы Мудро. На самом деле, больше об этой фирме ничего не известно, то есть это какой-то украинский стартап, там у них на сайте минимум информации, но они заявляют, что они изготавливают умные комплексы РЭБ и комплексы РЭР. По-моему, этот комплекс называется «Отпор». Там по-украински у них свое название, но эту информацию нужно проверять, потому что эта информация почерпнута из телеграм-каналов. Первичный осмотр, по сути, единственное, что удалось найти, - это вот эти три фотографии.

Внешне, как мы видим, три блока, на них написано «направление к врагу», да, куда направлять эти модули, и внутренка. Если мы проанализируем внутренности, то мы увидим, что это стандартные чипы LoRa. По длине антенн можно заметить, что это диапазон 900, то есть это 4 модуля на диапазон 900.

Я не вижу здесь никаких усилителей мощности, которые обычно встречаются в JR-модулях. Там же должен стоять вентилятор, его сразу было бы видно, внешний вентилятор. Соответственно, мощность у самих этих модулей небольшая. Как их можно использовать на фронте? Можно использовать этот комплекс для выдачи команд джарма на дроны, с нешифрованным ELRS. Анализирует ли это устройство обстановку, непонятно, в принципе. Если бы я не знал, что это умный комплекс РЭБ, ближнего радиуса

действия, я бы подумал, что это, ну, даже не пеленгатор, это просто сканирующее устройство. Он сканирует определенным образом эфир, находит LoRa-подобные сигналы, а дальше, соответственно, на каком-то пункте эта информация обрабатывается, принимается какое-то решение. По сути, это специализированный комплекс радиоэлектронной разведки. Но я бы не назвал его даже пеленгатором потому, что здесь нет антенной решетки и, соответственно, количество одновременно отслеживаемых устройств невелико. Ну, это уже мои домыслы. Единственное, что можно утверждать, что эта коробка, - это именно комплекс умного подавления. Радиус его действия небольшой, скорее всего, устройство направлено на то, чтобы влиять на дроны, которые подлетают, ну находятся в прямой видимости с этим блоком, а непосредственно, на взлёте он дроны не дизармит. Для того, чтобы произошел дизарм прямо у вас в окопе, прямо на позиции, нужно комплекс поднять всё-таки наверх, да, и использовать уже усилители мощности для того, чтобы добивать до позиции противника. Значит, можно было бы прийти к выводу, что на этом, нам конец, то есть, от ELRS мы должны отказываться. Но нет. Дело в том, что разработчики ELRS категорически отказываются добавлять шифрование. Они говорят, что они не участвуют в никаких военных действиях. Хотите, внедряйте свою радиосвязь, внедряйте шифрование, но сами. И поэтому есть так называемый форк, ответвление ExpressLRS, называется PrivacyLRS. И вот как раз PrivacyLRS, это была отправная точка для большинства современных помехозащищенных протоколов управления.

Конечно же, я должен был бы рассказать, как перехватывать дроны, а в конечном итоге рассказывал про то, как мы привыкли с этим бороться. Но в последний момент я пришел к выводу, об этом будет следующий слайд, уже последний, заключительный.

А пока, расскажу про PrivacyLRS. Энтузиасты не согласились с позицией компании и сразу же сделали отдельное ответвление с шифрованием. Т.е. добавили AES-128, по-моему. Главная задача была: при добавлении шифрования не убить задержку, потому что ELRS это система управления с очень низкой задержкой, т.е. буквально 6 мс. Т.е., для FPV - это прекрасная система. Соответственно, они добавили шифрование, по сути, оставив задержку на почти таком же уровне, практически. Как им это удалось, ну это надо изучить в прошивке, значит, вот это уже при выводе ELRS не страдает той проблемой, зато на неё уже не получится подать дизарм вот в открытом виде. На базе этой прошивки появился, как я понимаю, Кузнечик у нас и появился MILELRS у Украины. Дальше, там уже фантазия бесконечная, как

его модернизировать, то есть я думаю, что ELRS будет дальше модернизироваться. Я бы тут привел еще дополнительный Гермес, потому что Гермес, они заявляют, что это не форк ELRS. Но если взглянуть на сами модули, то это LoRa, всё та же самая LoRa, абсолютно. В любом случае, Гермес относится к системам помехозащищённой радиосвязи, с очень широкой ППРЧ, которая неподвластна стандартному ELRS и, соответственно, большая поддержка диапазонов частот. Как мы знаем, эти SX1276 поддерживают частоту от 137 МГц. У них в конфигураторе можно выставить, главное, чтобы у вас была подходящая антенна и радиочастотное оборудование, усилители мощности, МШУ на эти диапазоны частот. По итогам анализа, я пришел к выводу, что все-таки задача перехвата управления достаточно сложная. Есть, конечно, разработчики, там, израильские, которые заявляют, что мы там всех победим и вот это шифрование сломаем, я не верю в это. То есть, добавление просто AES-а примитивного, да, сразу же, моментально, или просто, если сказать, расчёту, регулярно менять бинд-фразу, не делать её, там, короткой, делать её длинной, там. Не делать мульти бинд, когда мы понимаем, что боевые задачи требуют запуска большого количества дронов в единицу времени. Поэтому у расчета просто не хватает времени постоянно перепрошивать, менять бинд-фразы, и поэтому какая-то группа дронов будет лететь с одним пультом, - это минус.

То есть, всё-таки нужно стараться не давать противнику, даже если они перехватят какие-то пакеты, пытаются их там расшифровать с помощью каких-то способов, чтобы не дать им возможности скомплементировать наш радиоканал управления.

Соответственно, организационно, тут я во второй абзац, он такой условный, так скажем, поместил. Поднимется вопрос по недостатку материальной части. Я как раз говорю, что поставляются модули без шифрования и, соответственно, расчетом FPV-дронов, соответственно, не объясняются угрозы и последствия, к которым может привести использование нешифрованного ELRS.

Значит, как я сказал, в TBS нужно поставить в конфигураторе одну галочку. Эта галочка может стоить жизни расчета, фактически. Если мы говорим про DJI, Autel, они останутся, потому что отечественных аналогов не предвидится. Это долгосрочная перспектива. То же самое касается и собственных чипов. На самом деле можно вообще не устраивать никакого шифрования, а просто производить свои LoRa чипы, например, с абсолютно другим Spread Factor.

В LoRa есть параметры модуляции, если мы используем Spread Factor 13, а такого Semtech не производит, допустим, или какой-то экзотический параметр, или полосу этой LoRa сделать не 200 кГц, а, допустим, 220 кГц, соответственно, - все вот эти методы разведки, они полностью ломаются. Потому, что РЭР анализирует стандартные сигналы LoRa, которые никак нельзя поменять, потому что это - проприетарная технология и, соответственно, ни на той стороне, ни на нашей стороне чипов таких вот дальнобойных нет. Значит, про управление по оптоволокну. Свою ремарку я уже сказал в начале: оно не заменит радиоуправление. Уже из моего выступления, я думаю, у вас может сложиться впечатление, что радио — это бесконечная тема, то есть дальше всё будет развиваться, будут добавляться новые режимы. Я знаю, что сейчас появилось третье поколение чипов LoRa LR1121, где появилась поддержка мультибенд, то есть двух диапазонов сразу, и 900, и 2.4, сразу на одном чипе. Да, и появился новый тип модуляции, это FLRC, Fast Long Range Communication. Это не LoRa, это - модуляция GMSK, значит, она найдет свое применение тоже, я думаю, на СВО, в том плане, что ее можно использовать для FLRC. Чем он хорош? Это еще меньшая задержка по сравнению с LoRa, то есть там задержки буквально уже 2–3 миллисекунды, даже, может быть, меньше. Есть минус этого всего, он заключается в небольшой дальности. Но ничто не мешает вначале запускать дрон на FLRC, и тем самым избегать всех этих проблем, а дальше переходить на стандартную LoRa, чтобы добивать на 10, 15, 20 километров и так далее.

Соответственно, вот это комбинирование скрывает сам расчет от комплексов радиоэлектронной разведки. К этому нужно быть готовым, потому что в дополнение к динамическому изменению мощности, то есть сначала пилоты взлетают на малой мощности, на милливаттах, а потом, по постепенному отдалению от позиции они уже начинают раскочегаривать. Соответственно, безопасность расчета будет на первом месте. Вот и в принципе на этом мой доклад окончен. Спасибо за внимание.

Представитель НИУ «МЭИ»

Спасибо. Сейчас у нас еще второй доклад есть. Коллеги я боюсь, что если мы сейчас начнем обсуждать, то у нас не останется времени ни на что другое. Давайте вы выступите, а потом по результатам двух сообщений будет возможность тем, кто хочет высказываться.

Представитель АНО ДПО Луис+

Правильно ли я понимаю, что подавление сейчас является более перспективным и простым решением, чем перехват управления?

Представитель НИУ «МЭИ»

Ну, я бы так сказал. Радиоэлектронная разведка, она перспективнее на тактическом уровне. То есть, я считаю, что мы должны насыщать передовую тактическим РЭРом. И тогда сразу станет понятно, что давить и как давить. Бесконтрольное использование РЭБа — это не панацея.

Представитель АНО ДПО Луис+

И свои, и чужие.

Представитель НИУ «МЭИ»

Бесконтрольное использование РЭБа и прочих помех — это стрельба себе в ногу.

Представитель Фонда НТИ

Что вы подразумеваете под тактическим РЭБом? На каком уровне его использовать?

Представитель НИУ «МЭИ»

Смотрите, у нас был семинар, когда к нам приезжали с фирмы ИРКОС. Они делают хорошие пеленгаторы, очень дорогие, multifunctional. Эти пеленгаторы далеко видят, имеют прекрасную аппаратную часть и обладают хорошей чувствительностью, но мне сказали, что вот на Белгородском направлении мало таких пеленгаторов, они не перекрывают зону ответственности, то есть они, по сути, бесполезны в малом количестве. Да вот буквально вчера я видел разработку, к сожалению, не нашу. Это беспилотный летательный аппарат у на борту стоит примитивнейший пеленгатор из двух антенн, который показывает на экране, куда лететь, где направление на источник излучения.

Давным-давно, еще три года назад, запустили то же самое, если было бы нормальное шифрованное средство связи. Или хотя бы спутниковая связь. Спутниковая связь решила бы все проблемы.

Представитель НИУ «МЭИ»

Конечно.

У нас нет ни спутниковой группировки, ни связи нормальной, т.е. там те же самые Азарты, да? Тракт расшифровывают, как будто шифрование отсутствует. Опять-таки, вопросы надежности дешифрования решаются наличием вычислительных мощностей. Если мы находимся в поле, какое у нас подразделение обладает вычислительными мощностями? Вот, никакого соединения. А если бы у нас была спутниковая связь, мы могли бы новый перехваченный сигнал, отправить через сеть, на сеть распределенных ядер, если бы у нас был такой. Любой компьютер под управлением Windows является системой дешифровки.

Представитель НИУ «МЭИ»

Ну, да если ИРСИ-40, то это буквально минуты, там если примитивная протокольность...

Да, 6-значный, 8-значный код, это все на лету. Вопрос в том, что у нас, например, есть передовые датчики, распределенной системы обнаружения радиоизлучения. Это примитивные средства радиоразведки. Но как получить данные с них? У нас тысяча километров фронта. У нас была бы просто потрясающая информация о радио обстановке на всей тысяче километров. У нас нет дата-центра, у нас нет средств связи, чтобы передавать эти массивы данных. Представляете, какие там массивы данных? Один спектроанализатор, отслеживая диапазон частот шириной в 500 МГц, плодит за минуту терабайт информации. Терабайт! Всё. Чем это передать? Каким средством связи? Полтергейстом?

Представитель НИУ «МЭИ»

Ну, давайте я расскажу.

Представитель Фонда национально-технологической инициативы

Просто вы, когда сказали на тактическом уровне, вы не сказали о взводе.

Представитель НИУ «МЭИ»

Да, да.

Представитель Фонда национально-технологической инициативы

Взвод, я не представляю, что такое взвод с установкой РЭР.

Представитель НИУ «МЭИ»

Я сформулирую. Дело в том, что количество дронов растет. Та сторона уже перешла на цифровые линии видео. Соответственно, дальше системы типа «совы», которая позволяет просматривать видео, что в тебя летит дрон, они перестанут работать абсолютно.

Я к чему веду? Что количество беспилотников растет, и первоочередной задачей должна быть борьба именно с операторами, борьба с ретрансляторами, да и борьба с антеннами, ну потому, что они сейчас все сидят на выносе, то есть нужно пеленговать каналы управления. То есть не дизармить дроны, не пытаться там что-то ломать, нужно выявлять эти антенны и просто туда пакет от Града направить и так далее. То есть уничтожать ретрансляторы, глаза Мавика.

Представитель НИУ «МЭИ»

Хорошо.

Второй докладчик.

Представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ

Коллеги, еще раз поблагодарю. У меня тоже особый доклад, касающийся тематики применяемых нашим противником уже не просто технологий, а конечных решений, против которых нам бы как раз и хотелось выработать свои элементы защиты. Причем, эти технологии для применения как на передовой, так и в тылу, при защите от противоправного применения беспилотных систем.

Хотелось остановиться на нескольких выявленных в последнее время системах и решениях, которые, к сожалению, до сегодняшнего дня кратно превосходят возможности по противодействию им.

И это связано, во многом, не столько с тем, что у нас нет конечных решений или мы не пытаемся противодействовать, насколько с самим подходом к организации противодействия. У нас фактически отсутствует системный подход. И занимаясь кустарными средствами противодействия, особенно на ЛБС, к сожалению, мы не решаем проблему в целом.

Также мы, к сожалению, как известно, находимся в зависимости от компонентной базы, у нас есть ключевые проблемы с критическими компонентами, такими как процессоры, микроконтроллеры. Это дает преимущество нашим противникам. Но я хотел бы рассказать о следующем. Есть такая американская компания как SILVUS Technologies. Она еще в 2014 году уже получала гранты Министерства обороны США и фактически разработала систему, которая позволяет создавать самоустанавливающиеся, самоформирующиеся объединяющие несколько объектов, в данном случае до 550, подключаемых одновременно, устройств сети. Это позволяет проводить мультидоменные операции. Это значит, что вы используете сигналы из различных сред. Авиационные, наземные и даже подводные. Технология показала и возможность принимать и передавать данные на глубине до 70 метров. Плюс, он работает в шахтах, это архитектура системы на чипе, не используя чип Wi-Fi, то, о чем говорилось в предыдущей части. Задача системы — это изменение формы сигнала, это обнаружение наличия факторов подавления и отстраивания от этих факторов. На следующем слайде есть диаграммы, того, как перестраивается сигнал передачи в зависимости от то-

го, какие на него воздействуют помехи. Вот 3 сверху это показатель в зависимости от наличия шума. Это скриншот с экрана оператора. Второй слайд диаграмма подстройки в зависимости, от тех шумов, которые идентифицируются системой. Она начинает перестраивать собственный канал передачи данных.

Эта как данная система работает. Система предполагает низкую вероятность перехвата. Используя технологию скрытой связи, при которой информация скрывается под шумами или в бесполезных сигналах, с помощью эффективной модуляции.

У системы очень высокая пропускная способность: до 100 Мбит в секунду. Высокая устойчивость к сигналам помех, которая предоставляет детали сигналов помех, и происходит перестроение за несколько миллисекунд для игнорирования сильных помех и переход на новые электронные защиты. Существует контроль мощности сигнала.

Система позволяет минимизировать мощность радиостанции, динамически уменьшая ее до минимума и увеличивая ее в зависимости от дальности БПЛА, что, по сути, долгое время сохраняет скрытность передачи информации и позволяет скрывать и оператора, и всю систему.

Надо понимать, что она включает в себя не только бортовые модули, которые стоят на беспилотниках, это система наземного управления и радиостанции, то есть все участники этой сети, они видят и идентифицируют и себя в пространстве, и понимают, где находятся элементы системы в данный момент, позволяя более эффективно управлять миссиями.

Соответственно, происходит применение внутриимпульсной модуляции. Для модуляции сигнала может использоваться фазовая или частотная модуляция, а также псевдослучайная шумоподобная модуляция.

Как я уже сказал, есть специальный модуль, который контролирует мощность, который регулирует ее причем как в автоматическом режиме, так и позволяет оператору делать это в ручном режиме. Возможность работы с другими технологиями, и вообще надо говорить о том, что наш противник работает с системами на открытой архитектуре. А основным критерием выбора таких систем и постановки их на вооружение, становится критерий возможности интеграции. Это, к сожалению, в пике нашим военным системам, которые абсолютно закрыты, плохо взаимодействуют между собой. И процесс их интеграции в систему управления занимает безумное количество времени, а еще хуже того - сопротивление самих же разработчиков.

Страны же НАТО этот критерий выставляют как основной. Если система является закрытой, она никогда не встанет на вооружение. Используют сигналы отличной техники, которая настроена разведывать их приемники, что ускоряет само их обнаружение. И это как раз дает преимущество и во времени, и возможность скрывать операторов. То, что коллега правильно сказал, задача воздействовать не непосредственно на сам объект, а задача воздействовать на операторов и на центры управления. Соответственно, в данной системе возможность его обнаружения для нас сильно ограничена. Протокол у них запатентован, они запатентовали даже саму форму волны, на которой он работает. При этом коммуникационное решение позволяет передавать и видео с высокой пропускной способностью, и данные управления С2. Данные состояния самодиагностики системы и все данные телеметрии.

Наша цель - выработать для себя элементы защиты.

Поэтому результаты сегодняшнего семинара — это не просто говорить о проблеме. Нужно сформировать, во-первых, технологический слепок, который мы могли бы сейчас использовать уже из наработок наших прикладной и фундаментальной науки. Это предприятия промышленности, находящиеся в контуре, способные разработать и применить уже действующие системы.

Нужно собрать кооперацию и в ближайшем проекте, в рамках федерального проекта, подготовить техническое задание и совместно выйти на разработку ТЗ и создание данной технологии. Организовать ее воспроизведение. Это может быть как реинжиниринг, так и, возможно, разработка чего-то более лучшего, но о котором мы, к сожалению, пока не знаем, или, хуже того, оно не идет в коммерциализацию по разным причинам.

Дороговизна компонентной базы. Прекрасные пеленгаторы очень дорогие. Надо понимать, что вообще все системы подобного рода, они еще грешат тем, что сроки их производства занимают 8–12 и более месяцев. Понятно, что в режиме войны это не допустимо. Все это происходит ровно потому, что надо заказать комплектующие, они изготавливаются, а это все, как всегда, с проблемами и ограничениями, как в закупке, так и в доставке, плюс понятно, что наши партнеры, которые эти комплектующие поставляют, не очень-то нам партнеры, на самом деле. Кто-то манипулирует и ценами, и сроками и так далее.

Поэтому, задача - создать эту кооперацию и выйти на разработку этой технологии уже в этом году. Я бы как раз попросил дать слово моему коллеге. Он тот, кто работает на фронт и работает на ЛБС, его продуктами пользуются и считают их наиболее эффективно применяемыми.

Я бы хотел, для скорейшего решения озвученной мною проблемы, а к сожалению, за четыре года, несмотря на то что эта технология уже активно применяется НАТО, мы вообще практически не шевелимся. Я попросил бы комментировать, какие на ваш взгляд есть ключевые проблемы, на которые нам надо при создании такой системы обратить внимание.

Представитель КБ «Чистое Небо»

Коротко, по поводу сигнала. Сейчас схему прямо на экран повешу.

Это с левой стороны у нас 200 МГц, крайний правый угол 6000 МГц. Значит, симптомы обеспечивают непрерывную связь на всем диапазоне от 200 МГц до 6000 МГц. Это означает, что нам нужно передавать данные, можно создавать абонентские сети. Это идеальная мечта военного. Маленькая железенькая коробочка такого размера, с которой можно сделать станцию абонентскую, то есть ретранслятор, базовую станцию, завязать на нее все каналы связи, она будет прекрасно вытягивать в любом диапазоне. Передавайте даты, карты, текстовые сообщения, короткие сообщения, причем обнаружить передачу данного передатчика можно только при помощи спектроанализатора реального времени, что реально увеличивает стоимость оборудования для радиоразведки. То есть, спектроанализатор реального времени, это стоимость миллионов, десятков миллионов и выше. Чтобы заставить по связи, представьте себе, какого размера должен быть эшелон машин в модульном исполнении, если на каждые 100 МГц использовать хотя бы по одному модулю. Реально это два КАМАЗа оборудования. Два КАМАЗа оборудования противнику со спутника будут видны тут же, моментально. То есть, поработает это дело 5 минут, дальше всю эту штуку уничтожат. Мало того, наш РЭБ, которым мы будем противодействовать на столь широком диапазоне, сам себе заглушит всё, что у нас есть. Всю нашу связь, всю нашу передачу данных, всё-всё-всё. Мы останемся слепы, глухи и ещё получим радарные травмы. То, с чем мы боролись до этого, вот это все детский сад, поделки детей, это вот верхняя часть таблицы, где красные пятна, это каналы управления, только по одним детекторам мы отстроили у себя детектор, - максимум детектирует 5 диапазонов. Посмотрите, сколько дыр вообще остается в работе. За три года даже самые непробиваемые люди

пришли к тому выводу, что чтобы противостоять угрозе дистанционно управляемому аппарату, управляемому, я имею в виду по радиоканалу. Просто какого-то одного чудо-устройства, персонального детектора или блока радиоэлектронной борьбы уже недостаточно, нужна система, нужен системный подход.

Как делают американцы? У них разработана стратегия ведения радиоэлектронной войны, в основе которой лежит контроль спектра. То есть всё, что мы видим, это всё спектр, спектр всевозможных излучений, в данном случае в радиодиапазоне. А еще есть спектры, не только электромагнитные, но и другие, вплоть до спектров далеких светил и электронных звезд. Но даже на уровне обыкновенного контроля радиоэфира, который в принципе должен осуществляться в любом населенном пункте, я имею в виду работу радиочастотных центров, которые обязаны выявлять нарушителей, которые пользуются радиооборудованием на изолированных каналах. Но мы этого не делаем, у нас этого нет. Обнаружить этот вот американский сильный источник излучения достаточно сложно.

А теперь посмотрите на израильтян. Почему они так хвастаются, что мы можем убить всех и пролететь где хотим? Вообще все забито, а еще есть то, что отсутствует в этой таблице, то есть от 6 до 40 ГГц. Это спутниковые системы, — все это должно работать в тандеме. Просто так, значит, взломать все и пролететь на TBS или ExpressLRS и в эфир, значит, выпускать одну команду, теперь мы этим не отделаемся. Это все прошлый век, это закончилось два года назад.

Сейчас, серьезная угроза это не только маленькие аппараты. С маленьким аппаратом еще кое-как можно бороться. Но то, что мы наблюдаем последние недели, последние месяцы. Прилеты БЛА самолетного типа под названием «Лютый» КБ Антонова, «Летучая Лисица» (Аэропракт А-22). Кто-нибудь ездил, смотрел живьем на этот самолет? Что это за радиооборудование там стоит? Никто не заметил там радиокompас? Эта штука снабжена радиокompасом, таким же, как на В-52 стоял. То есть практически тысячу километров он может лететь без GPS. И спуфинг вам не поможет, он достаточно точно прилетает. Системы связи, как правило, там есть модуль Silvus, который обеспечивает связь и со спутником, и с наземной станцией, и с любым радиооборудованием нашей мобильной связи. Смотрите, как пересекаются частоты с тем же самым стандартом LTE. Серенькая вот эта вот, это LTE, мобильный диапазон. Все вражеское оборудование может спокойно работать с нашими базовыми станциями ретрансляторов и так далее. Чипы,

микросхемы, которые мы покупаем в Китае. За три года я столкнулся с тем, что все работают с китайскими компонентами, которые мы закупаем в Китае. Китайцы, в итоге, сказали, а что вы там делаете? Вы так много уже стали покупать, давайте мы будем делать. Ну, а если что-то начинают делать китайцы, они начинают это продавать. Кому? Только вам? Они начинают продавать это всем. Всем подряд. Врагам, друзьям, всем разным. Всем, кто заплатит денег. Поэтому, пока у нас не появится своей национальной собственной элементной базы, даже вопросы простейшего контроля спектра просто будут недоступны. Даже имея достаточно большое количество датчиков дешевых для первичной радиоразведки, мы не сможем обеспечить передачу такого количества данных, ее унификацию, ее обработку, потому что просто нет технических средств для того, чтобы обеспечивать передачу информации. Вот возьмите город, какой-нибудь важный стратегический объект находится обязательно где-нибудь в центре города. Или где-нибудь в жилой зоне. Как мы его защитим? Давайте быстро во всех городах ставить выжигатели мозгов, чтобы у людей как можно больше рака появилось. По-больше ватт: 100 ватт, 200 ватт, 300 ватт. Но, читаем сноску. Радарная травма. Что это означает? Мы будем, значит, своих собственных граждан травить радиоволнами и мощностями? Без эффектов?

Представитель НИУ «МЭИ»

А что Вы предлагаете?

Представитель КБ «Чистое Небо»

Для начала разработать собственную отечественную ПЛИС-микросхему. И на ней уже мы какие угодно можем системы построить. У нас нет своей собственной электроники.

На технические вопросы, я сейчас отвечать не буду. Тут важен принцип. У нас нет микрочипов, на которых мы могли бы строить широкополосную связь, нормальную, какая она должна быть в 21 веке.

Представитель НИУ «МЭИ»

У нас этого не будет еще долго.

Представитель НИУ «МЭИ»

Вопрос можно? Вы уже закончили? С какой скоростью вы хотели просматривать диапазон от 200 МГц до хотя бы 6 ГГц. В идеале, моментально, - это не радиотехнический термин. Моментально ничего не бывает, ну сколько, миллисекунды, секунды?

Представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ

Еще раз, он говорит про анализатор спектра в режиме реального времени.

Представитель ВУЦ МЭИ

Он обзор делает, не любого технического устройства. За сколько вы хотите просмотреть этот спектр?

Представитель КБ «Чистое Небо»

Естественно, мы весь спектр, единомоментно просмотреть не можем, для этого нам нужен некий комплекс.

Представитель НИУ «МЭИ»

Нет, вопрос конкретный. Как часто вы хотите иметь обновленную информацию о наличии сигнала в диапазоне от 200 МГц до 6 ГГц?

Представитель КБ «Чистое Небо»

8 ГГц в секунду, это было бы приятно.

Представитель НИУ «МЭИ»

Вот в известном городе Ярославле, в госуниверситете, есть устройства, которые сканируют диапазон от 200 МГц до 25 ГГц 3 раза в секунду. Прекрасно. Сколько он стоит? Ну, может быть миллион, может быть 200 тысяч, может 300, в зависимости от партии. Почему этого нет в армии?

Представитель НИУ «МЭИ»

Это вопрос к армии. Странно, у нас вообще нет системы работы со спектром. Системы контроля спектра.

Представитель НИУ «МЭИ»

Мы уже второй доклад слушаем. Все говорят, надо сделать. Мы-то, что можем сделать конкретно? Я сейчас выступаю не как военный. Я уже 4 года в запасе. Потому, что мы тут все что-то говорим, есть какие-то картинки, у нас есть компетенции. Давайте конкретно, предложения какие?

Представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ

Но толку от этих приемных устройств, если мы не можем обеспечить между ними передачу данных?

Представитель НИУ «МЭИ»

Давайте обеспечим, но конкретно, что надо сделать? Дата-центр как минимум. Да, это слишком глобально для нас. Вот, например, мы сейчас пытались разговаривать о постановке помех каналов управления. Просто мы много говорим, а вот какой вывод из всего этого? Что нам конкретно делать?

Представитель НИУ «МЭИ»

Но когда я смотрю на эту картинку, вот третью сверху, я ничего не понимаю. Мне рассказывают о каких-то вещах, а я смотрю на эту картинку, пытаюсь понять, я не понимаю, что это за окружности, которые смещены, что это за созвездие, что это, ну просто, понимаете, давайте конкретнее.

Представитель КБ «Чистое Небо»

Это, скорее всего, визуализация и поляризация отраженных сигналов. Скорее всего, это, опять же, вопрос не конкретный.

Представитель НИУ «МЭИ»

Нужно конкретно. Ось времени, ось амплитуд, ось частот, ось фаз, чтобы это была информация, а не картина. На сайте изделия очень подробно все описывается.

Представитель НИУ «МЭИ»

Давайте вернемся немножко к конструктиву. Семинар, как форма деятельности, подразумевает, что задается тема. Поэтому давайте, у нас тема сегодня была заявлена, это технические возможности перехвата или воздействия на каналы управления. Она сейчас начинает расширяться в принципе в очень, очень общие вопросы, наподобие отечественной микроэлектроники. Конечно, эту вещь можно бесконечно обсуждать. Как Марианскую впадину по глубине исследовать, но мы-то здесь все-таки, не для того собрались. Нет у нас задачи поплакать. Прямой вопрос, чем мы противодействуем? Вот есть какая-то схема.

Представитель КБ «Чистое Небо»

Вот смотрите, с чем мы столкнулись, сейчас мы разрабатываем собственный спектроанализатор. Опять-таки, на китайских компонентах, потому что других нет, а хотелось бы свои собственные. Я уверен, что через какое-то время китайцы скажут, что у нас все поменялось, давайте мы будем делать так, а то у вас ничего не получится. Вопрос не в этом. Предположим, у нас есть датчики, которыми мы можем организовать контроль спектра, появляется какой-то новый сигнал. Я не зря привел в качестве примера эту картину. Здесь достаточно широкий спектр, который нужно наблюдать, и очень мало специалистов, которые разбираются в этих спектрах. Лучше, конечно, автоматизировать этот процесс. Чтобы его автоматизировать, надо работать с данными. Эти данные надо собирать, архивировать, анализировать. И если у нас не будет широкополосной, шифрованной своей собственной системы связи, у которой нет никаких барьеров. Так не бывает. Непонятно, что такое. Это возможность взлома. Любой разработчик оставляет в своем изделии возможность, так скажем, контролировать эту машину. Потому что что-то может пойти не так, чисто из-за человеческих факторов. Забыл, как она шифрует, расшифровывает. Мастер-ключ. Существует такое понятие. Существуют закладки всевозможные для разработчика. На этапе отладки устройства, создаются контрольные точки, через которые можно это устройство сломать и обойти, так скажем, систему защиты. Но мы сейчас не об этом. Это уже, так скажем, комбинированные средства противодействия. Это то, с чем мы столкнемся в настоящей нормальной взрослой войне, не той детской, которая сейчас идет. Это вот все, детский сад. Да, опасно, да, страшно, но слушайте, как только первый человек схватил палку, он стал страшным и опасным. Дальше появился второй человек, который тоже притащил палку. Разницы никакой нет. Но то, что у нас нет сегодня широкополосной шифрованной радиосвязи, которая бы позволила контролировать

спектр. Огромные объемы данных позволила бы передавать. Перехватывать видеосигналы опять-таки. Ну, вы поняли.

Представитель НИУ «МЭИ»

Вопрос, вот эти изделия Silvus, они на практике сейчас насколько часто встречаются? Они, я так понимаю, не самые дешевые?

Представитель КБ «Чистое Небо»

Учитывая, что, в основном, они используются на дорогих устройствах, которые несут, так скажем, разведывательную функцию, они попадаются достаточно редко, но попадаются. По крайней мере, на моей памяти, трижды был сбит самолет, с одного мы сняли модуль. Где-то, наверное, существуют еще такие сбитые беспилотники.

Просто из сферы личной безопасности это перешло в некую коллективную ответственность. Если раньше подразделение достаточно комфортно пользовалось своим персональным каким-то оборудованием для определения точек взлёта, для определения угроз, какими-то детекторами для обнаружения пролётов уже с пост-фактором, да? То сейчас этого уже недостаточно.

Просто, может быть, некоторые вещи придётся показать на графике. Здесь всё предельно просто. Красный канал управления, фиолетовое видео.

Представитель НИУ «МЭИ»

Правильно я понимаю, что изделия фирмы «Silvus» это хорошие, эффективные программно-аппаратные радио модули?

Представитель КБ «Чистое Небо»

Фактически это и спутниковая связь, и гражданская связь, и специальная связь в одном. Это конструктор, из которого можно собрать...

Представитель НИУ «МЭИ»

Я не очень понимаю, как в таком размере можно все эти диапазоны сочетать.

Представитель НИУ «МЭИ»

Нет, до 6 ГГц без проблем. Как я уже говорил, а дальше, может, 3,63...

Представитель НИУ «МЭИ»

Но вы знаете, что если развести ее на fr4, у нее после 3 гигов вообще никакой четвертности не будет.

Представитель НИУ «МЭИ»

Я все понимаю, но вопрос в том, что по мощности, насколько это будет вытягивать.

Представитель НИУ «МЭИ»

Нет, вы аналоговый видеопередатчик к ней поднесете, она его не увидит уже на 5,8, то есть вы не сможете сделать виртуальное устройство.

Представитель НИУ «МЭИ»

Хорошая мощная ПЛИС, наверное, с большим объемом прошивок, это классная вещь, ну и явно, что там радиус частотной части больше.

Ну, либо тут два канала разбросаны на...

Представитель НИУ «МЭИ»

Ну, любой, в принципе, скажет, что после 4 гигов СВЧ уже другие материалы нужно использовать.

Представитель НИУ «МЭИ»

Нет, опять же, можно на том же плане развести её, а низ, нужно же пробросить её просто... Ну, это так же, как с антеннами.

Представитель НИУ «МЭИ»

То есть, если я правильно понял тезис, то противник все чаще переходит на некое типовое SDR, программно-определяемое решение, потому, что так

удобнее адаптироваться к узкому спектру, тогда идем, значит, в правильном направлении.

Представитель КБ «Чистое Небо»

По нему - устойчивость, адаптация, передача данных и передача текста.

Представитель НИУ «МЭИ»

Но потом дальше, значит, передача файлов, передача потока, совершенно разные задачи связи. Совершенно по-разному решают эти задачи.

Представитель КБ «Чистое Небо»

А потребителю это должно быть интересно вообще?

Представитель НИУ «МЭИ»

А мы сейчас не как потребители, мы сейчас здесь обсуждаем как специалисты. Это технические возможности перехвата каналов управления. Если мы говорим про сообщение, которое было вторым, то техническое средство, на котором должен реализовываться тот или иной протокол управления беспилотником.

Представитель КБ «Чистое Небо»

Ну, нам надо сначала считать, что это программное решение.

Представитель НИУ «МЭИ»

Ну, например, протокол LoRa. Ведь без этого протокола организовать сегодня связь с беспилотником невозможно. Вот значит, этот протокол и нужно анализировать в первую очередь с помощью спектроанализатора.

Представитель КБ «Чистое Небо»

Спектроанализатор реального времени, SDR-приемник спокойно считает все, по битам, все, что она передает.

Представитель НИУ «МЭИ»

Есть определенный тезис. Дело в том, что я SDR-ом занимался и занимаюсь. Все-таки SDR — это лабораторное оборудование.

Представитель ПАО НПО «Алмаз»

Все когда-то было лабораторным оборудованием.

Представитель НИУ «МЭИ»

Погодите, я сказал, что SDR, оно прекрасно, когда вы что-то прототипируете, проверяете что-то, какие-то технологии. Но когда вы выходите на рынок, то лучшим решением будет, когда радиочастотный тракт согласован с вашим сигналом. А когда у вас сигналы непонятно какие, у вас устройство по размерам превратится в КАМАЗ. Соответственно, что будет лучше, прием SDR или прием LoRa? Просто таким же чипом LoRa, просто я их запрограммирую, в нужном диапазоне поставлю, подберу нужную антенну и заставлю ее сканировать и принимать сигнал, потому что тракт LoRa уже построен под LoRa. Он заточен, чтобы принимать сигналы значительно ниже шума. А SDR не примет никогда сигнал на 20 дБ ниже уровня шума. А LoRa чип примет, потому что он знает, этот сигнал. Это техническое решение.

Представитель ООО «СТЭК КОМ»

Например, если мы озаботимся перехватом аналогового видео, либо мы можем строить огромный чемодан с 1000 приемников, каждый на свою частоту, либо все это организовать через смеситель с управлением с того же самого SDR-приемника, в данном случае передатчика SDR-приемника, чтобы модулировать несущую волну и не связываться с огромным количеством приемников. Мы сможем сделать всеядные видеоприёмы.

Представитель НИУ «МЭИ»

Я тоже большое количество времени занимался защищённой связью, точнее её называют стеганостойкой. Есть криптография и стеганография. Стеганография — это про то, как вообще вскрыть факт передачи. И, соответственно, там проблема в том, что есть формы сигналов, которые позволяют действительно записать сигнал на уровень шумов, даже ниже уровня шумов приемника. И, соответственно, ни один разведывательный приемник эту

связь не заметит. Да, но вопрос цены. То есть, для обычного бойца это будет стоить, ну крайне дорого.

Представитель ПАО НПО «Алмаз»

Ну, специалисты работают над этим.

Представитель НИУ «МЭИ»

Там можно передавать гигантские объемы данных под шумом. Но на выходе мы имеем пока только LoRa. Она лучше, чем узкополосные виды модуляции. Амплитудный, частотный, базовый, еще раз повторюсь. Вы хотите создать какую-то коммерческую систему, но она все равно будет стоить гигантские деньги.

Представитель НИУ «МЭИ»

Вопрос. Тезис, что LoRa уходит, а появляются мощные и так далее протоколы. Насколько спорный этот тезис, что сейчас действительно фокус с LoRa-подобных каналов управления переключится на протоколы с новым программным управлением?

Представитель ООО «СТЭК КОМ»

В этом скачкообразном развитии, которое мы видим сейчас, всех этих дистанционно управляемых вещей, возникают достаточно большие окна возможностей. Пока идет перестройка, с одной системы на другую, в любом случае единого проверенного опытом эксплуатации решения нет. Как действует противник, как он употребляет оптоволокно сейчас? Оптоволокно он употребляет там, где не может пролететь на радиоканалах. Для того, чтобы на стандарте можно было наносить удары. А это подразумевает хотя бы какую-то примитивную радиоразведку. Не в глубоком смысле этого слова, что мы перехватили сигнал, управление дроном, направили его обратно. Это сейчас космос далекий, так скажем, для нас вообще, в принципе. Для того, чтобы это эффективно работало, нужна система. Система сбора данных, система контроля вообще, радиус передачи данных.

Представитель НИУ «МЭИ»

Почему LoRa не уйдет? Есть проект беспроводного HDMI. Задача заменить все кабели на беспроводной интерфейс, но через HDMI такие потоки данных проходят. Чтобы сделать портативное устройство беспроводное, оно будет стоить сотни тысяч рублей вместо того, чтобы купить кабель за 500 рублей. Тоже самое с LoRa.

Представитель МО

Он летает на тактических беспилотниках, на Silvus.

Представитель НИУ «МЭИ»

Сам носитель стоит 30 тысяч рублей, а связь для него будет стоить сотни.

Представитель КБ «Чистое Небо»

Наглядный пример для нищих, как противники, не имея в большом количестве сил, устанавливает гражданские LTE. Например, та же самая Толтоника. Внешняя широкополосная связь в стандарте Украины всеядна, она работает со спутниковыми антеннами, с GSM антеннами, с LTE антеннами. Вот этот нижний самый серенький кусочек кубиков, на схеме, - это LTE. Что тоже позволяет скрыть канал передачи управления? Попробуйте отличить дронное LTE, летящий, передающий канал управления, видео, от других источников сигнала.

Представитель НИУ «МЭИ»

Ну, вы знаете, LTE — это 20 километров и уже нет.

Представитель КБ «Чистое Небо»

Через 20 километров еще одна башня будет, а дальше еще одна башня.

Представитель НИУ «МЭИ»

Но мы выезжаем из Москвы, и уже LTE нету. А мы на воздухе. На ЛБС тем более ничего не будет.

Представитель НИУ «МЭИ»

Вдоль шоссе и в городах все-таки есть, а между городами и между шоссе, действительно, нет.

Представитель НИУ «МЭИ»

Мы же говорим, GSM - он везде есть. А LTE нет. А БЛА летит.

Представитель КБ «Чистое Небо»

Он летит, да. В воздухе, так скажем, радиообстановка отличается от радиообстановки на земле, тем более между посадкой и выяснением дороги.

Представитель НИУ «МЭИ»

Вот, и по поводу спутников, на спутниках LTE не будет никогда.

Представитель НИУ «МЭИ»

Так, тут тезис в обсуждении, о том, уйдет ли LoRa в принципе или останется?

Представитель КБ «Чистое Небо»

Нет, они никуда не уйдут, там еще задел для развития огромный на этих чипах имеется.

Представитель НИУ «МЭИ»

Соответственно, вопрос о целесообразности рассмотрения того, что можно ли технически перехватывать каналы управления? Наш коллега в первом докладе сказал, что если использовать не хорошо защищенные каналы и безалаберность операторов, то есть некоторые возможности вскрывать каналы управления, но если используются защищенные каналы, то, по его мнению, это не взламывается техническими средствами.

Представитель НИУ «МЭИ»

Смотрите, на той стороне повсеместно используется вот этот ELRS и его там всякие ответвления. Это вот украинский протокол на основе ELRS. Дело в том, что он затрофеен. Прошивку вы можете изучить, но вы не сможете на неё воздействовать, потому что это зашифрованный канал.

Представитель НИУ «МЭИ»

То есть разумными способами, которые есть в доступе, это сегодня невозможно?

Представитель НИУ «МЭИ»

У каждого дрона свой ключ, у каждого пульта свой ключ. Остается только их привязать, а дальше, не зная этого ключа, вот перехватить управление не получится.

Представитель КБ «Чистое Небо»

Но ключи-то мы можем взломать.

Представитель НИУ «МЭИ»

Ну, там миллиарды комбинаций. Если мы наберем вычислительные мощности, то да.

Представитель Фонда НТИ

Ну, это технически не целесообразно. Вот Вы сейчас это сказали. На тактическом уровне, там, до 20 километров, ключи-пульты, ключи-оператор, канал шифрованный. Вытекает ли из Вашего сообщения то, что перехват управления тактического канала невозможен в этой ситуации при наличии такого шифрованного канала?

Невозможен и не целесообразен, либо возможен за бешеные деньги.

Представитель НИУ «МЭИ»

А реальна техническая реализация?

Представитель Фонда НТИ

Да, это теоретически возможно.

Представитель НИУ «МЭИ»

Но не целесообразно.

Представитель Фонда НТИ

Дальше вы сказали, что надо сосредоточиться на перехвате ретрансляторов и операторов. Вы заканчивали, кажется, свое сообщение этим. Можно этот тезис сформулировать еще раз четко?

Представитель НИУ «МЭИ»

Ну, есть разведывательно-ударный контур противника. Он состоит из операторов-разведчиков и ретрансляторов сигнала управления, да и самих дронов, соответственно. Сейчас все борются с дронами, я говорю про тактический уровень, не про разведывательные БПЛА самолетного типа. Борьба должна быть построена именно с тем компонентом, чего меньше всего, это операторов ретрансляторов и разведчиков. Их же значительно меньше, но их сложнее достать. Почему сложнее достать? Потому что нет тактических комплексов РЭР. На чем они основаны? Есть простое решение, да, это спектроанализатор.

Представитель Фонда НТИ

Первое, вы говорите о том, что поскольку в этой массе нападающих дронов есть точки уязвимостей, к которым относятся, в первую очередь, операторы дронов разведки и ретрансляции сигнала, то нужна тактическая радиоэлектронная разведка для обнаружения этих двух компонентов. И если эти компоненты заглушить, тогда все дроны окажутся, мягко говоря, неуправляемыми. Потому, что бороться с каждым FPV-дроном, по вашему мнению сложно. Правильно ли я понимаю, что Вы сказали о тактической электронной разведке для обнаружения ретрансляторов и операторов? Дальше вы сказали, что на уровне взвода, дальше вы не успели, модератор вас пока остановил для ответа на дальнейшие вопросы, и я задал вопрос, что это такое, как это во взводе, и кто такой во взводе этим будет заниматься? Мы знаем, что такое, когда стрелковый взвод находится в обороне, проходили, - кто это. Но, как этот тактический радиоэлектронный комплекс во взводе будет привязан к батальонной сети? Вот хотелось бы понять техническую реализацию этой тактической радиоразведки, радиоэлектронной разведки для поиска операторов и ретрансляторов, и вот какие дальнейшие действия?

Представитель Фонда НТИ

Позвольте, я поделюсь по этому вопросу своими накопленными с фронта отзывами. Если в конце 22-го года только начиналось появление дронных бомбардировщиков, серьезных, первых, так сказать камикадзе, то 23-й год уже практически с февраля, начались налеты по 200–300 налетов за сутки. Но дело в том, что даже для того, чтобы полететь на дроне камикадзе на 10, на 15, на 20 километров, это, во-первых, невозможно без ретранслятора, иначе дистанции сокращаются до 7 километров. Но чтобы полететь, не важно на 5 или на 20 километров, нужно определенное время для того, чтобы наладить оборудование. Прямо из коробки вынутый дрон никогда не полетит. Его по крайней мере 5 минут нужно настраивать.

Вот эти 5 минут при средней скорости такого же противодрона у нас, например, в 50–20 метров в секунду, вполне достаточно для того, чтобы убить этот расчет до момента запуска им своего дрона. Как только мы включаем пульт, он сразу же начинает излучать в эфир радиоволны. Причем на диапазонах, которые при мощности в 1 Ватт могут распространяться на сотню километров. При нормальном, так скажем, обустроенном тыловом центре радиоразведки на 100 километров эти все сигналы можно запеленговать. А если еще применить самолеты радиоподдержки? Но у нас же все упирается в то, что мы не можем поднять воздушный ретранслятор, как это делает противник, потому что тут же соседи начинают в него стрелять несмотря на то, что их предупредили. Взаимодействия нет, радиосвязи нет.

Представитель НИУ «МЭИ»

По технике сейчас вопрос. Что такое комплекс радиоэлектронной разведки на тактическом уровне: рюкзак, чемодан, большой контейнер, вот вопрос был задан именно про это. Выступающий сказал, что надо развивать это направление.

Представитель НИУ «МЭИ»

Смотрите, я надеюсь, что штатно у нас в войсках скоро появятся подразделения беспилотных систем, не только на словах. Почему? Чтобы не было самодурства, чтобы реально можно было спецов подготовить. И однозначно, потом их не пошлют в штурмовики просто потому, что людей не хватает.

Представитель ВУЦ МЭИ

За три года подготовили немало специалистов, и все они ушли в штурмовики.

Представитель НИУ «МЭИ»

Ну, подождите. Это должно быть не то, что берем солдата, и теперь на вот тебе спектроанализатор, и ты идешь искать кого-то. Не работает это так. Вот из последнего, с чем удалось ознакомиться - тактический комплекс электронной разведки «Грань». Но дело в том, что надо помнить, что это - софт прежде всего, а смартфон — это убийца солдат. Преимущество этого комплекса в том, что у него карта на дисплее, на которую выводится сразу спектр выявленных источников.

Представитель АО ДПО Луис+

Так это пеленгатор?

Представитель НИУ «МЭИ»

Погодите, концептуально эта задумка очень хорошая. Вопрос в том, что если мы хотим бороться с ретрансляторами, и с операторами, то вместо спектроанализатора должен быть пеленгатор.

В идеале это должен быть пеленгатор воздушного базирования, то есть он должен быть на беспилотной системе, а построен он должен быть на чипах за счет реинжиниринга. Вот как тот комплекс, что я показывал, вскрывает коробочку, а там набор модулей. Система, объединенная единым микропроцессором, который сканирует и принимает какое-то решение, ищет нужную сигнатуру.

И дальше, соответственно, мы получаем пеленг. Один аппарат получает пеленг, два аппарата уже дают решение в координатах на плоскости. Ну хотя бы приблизительно эллипс куда нужно идти либо туда стрелять. Вопрос в том, что на базе антенной решетки это сложно сделать. Да можно поворотом, можно псевдо доплер. Дело в том, что самый лучший это интерферометр. То есть интерферометр это наилучшее будет решение по точности, так скажем. Вопрос, вот в фирме ИРКОС уже решение-то было изобретено, но оно тяжелое. Там антенная система весит около 20–25 килограмм, там механические антенны, но они просто хотели закрыть все диапазоны и ко-

гда с ними говоришь: «давайте LoRa искать». Ответ: нас это не интересует, мы тактическими комплексами не занимаемся, потому что нам экономически это не выгодно, нам выгоднее продавать комплексы, которые дорогие, штучные, это их бизнес-модель, то есть они говорят, если хотите заниматься тактикой, занимайтесь, мы вам не конкуренты.

Представитель Фонда НТИ

Массогабаритные характеристики такого пеленгатора какие? Ведь это пассивное устройство, ему не нужны мощные АКБ.

Представитель НИУ «МЭИ»

Это пассивное устройство, какова его масса и габариты?

Представитель НИУ «МЭИ»

Ну, вот у меня был слайд, там вот коробочки, да, и то там много пустого места, чип, он с экраном, занимает место как спичечный коробок, нужно несколько каналов, да, 3, 4, 5.

Представитель НИУ «МЭИ»

Да, то и дальше уже методика какая-то.

Представитель КБ «Чистое Небо»

Это оборудование мы поднимали в воздух.

Представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ

Мы прекрасно понимаем, что в текущих условиях, с этой системой (Silvus) у нас будут большие проблемы в области безопасности.

Представитель Фонда национально-технологической инициативы

Согласен с тем, что у нас, к сожалению, нет средств для того, чтобы прикрывать большие массивы.

Представитель КБ «Чистое Небо»

Желательно, доработать антенны, чтобы действовало по разной частоте, чтобы пеленг в автоматическом режиме проходил.

Представитель ВУЦ МЭИ

Можно я чуть-чуть про перспективу? Коллеги, я еще раз обращаю ваше внимание, что, например, это касается тех представителей, которые собираются как-то развивать эту тему не в смысле компетенции, а в смысле поддержки финансов. Еще раз говорю, что в Ярославском университете уже давно ведется работа по созданию такой системы. Сейчас она находится на этапе испытания. У меня есть фотографии, у меня есть слайды, у меня есть результаты работы. Эта система, поднимается на дроне, имеет три канала обнаружения, в том числе пассивного, активного и оптического. Пассивным каналом конкретно я занимаюсь, пеленгаторами. Активный канал уже работает, у меня есть готовые фотографии, съемки с экранов, где поднятый на пару десятков метров дрон в режиме вращения сканирует пространство. Это активный стреляющий, пассивный стреляющий, не видна для противника, и с учетом тех алгоритмов, которые мы предлагаем, в частности векторного сложения, мы увеличиваем дальность обнаружения сигнала до полутора десятков километров. Этого достаточно для тактического наблюдения. Имея два дрона, которые висят над нами, в пассивном режиме, по двум пеленгам мы находим точку пересечения и, соответственно, источник сигнала. Какая нужна точность для поражения? Сколько? 100 метров на 100 метров? Углы какие?

Представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ

Здесь я бы не привязывался только к дронам. Группы очень часто работают в городской застройке. С элеваторов, и так далее, поэтому было бы здорово, если бы он был съемный.

Представитель ВУЦ МЭИ

Он съемный. Дрон в данном случае, как исполнитель для подъема антенны.

Представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ

Откликайтесь на предложение по апробации и с удовольствием испытаем.

Представитель НИУ «МЭИ»

И как я понимаю, их можно выпускать не в виде полноценных постановщиков помех, а в виде плат расширения для китайских джаммеров, правильно? Да, так крайне желательно сделать.

Представитель ВУЦ МЭИ

По поводу имитационных помех. Вообще тема имитационных помех она стара как радио, что здесь может быть нового: нужно принять сигнал откуда-то, его усилить, ну может быть там повернуть его как-то чуть-чуть по фазе и отправить, не принять его вы не можете, вы не знаете его ключа. То есть он принимается просто полосой, не надо декодировать его просто нужно усилить, добавить имитационную помеху и просто повторить. Это же классика для больших блокадеров, это делается с самого начала появления блокадеров.

Представитель НИУ «МЭИ»

На самом деле мы обсуждаем очень такую интересную тему, мы говорим там про ППРЧ, что нужно закрыть большие диапазоны, ну сейчас ППРЧ, допустим, делают уже и 100 мегагерц, и 200 мегагерц на канал управления, но приемник становится широкополосным, и, соответственно, есть беда широкополосных приемников. Если у него стоит МШУ, то вы подаете просто прицельную помеху в этот диапазон и перегружаете ему приемник, и он уже больше ничего не примет, никаких команд. Даже не этот широкополосный джаммер. То есть тут как бы палка о двух концах. Либо вы расширяете полосу и бегаєте от этих джаммеров, тогда соответственно вам нужен КА-МАЗ или два КАМАЗа, чтобы это все подавить. Но расширяя полосу приема, соответственно разработчики вот этот изъян оставляют, то есть можно мощной помехой перегрузить входной каскад приемника на дроне и все, он ослепнет.

Представитель ВУЦ МЭИ

В какой полосе это вообще скачет? 100 мегагерц? Ну, 100 допустим. А полоса одного элементарного сигнала? 20 мегагерц? То есть, ну, оставьте вы эти 20 мегагерц, есть у вас этот диапазон, он все равно будет попадать в этот прием.

Представитель НИУ «МЭИ»

Конечно, но я просто не понимаю, почему? Я со своей стороны понимаю, что есть определенные пробелы. Кто-то учился, а кто-то, идет в институт, и начинает изучать азы. Потом начинает понимать, что все оказывается по-другому. Не так, как вот там пишут в Телеграме или там, где-то еще в каких-то этих соц. группах. Есть различные варианты, просто надо это тестировать, так сказать.

Представитель НИУ «МЭИ»

Вот тезис от коллег практиков: говорят, что джаммеры, поверхностно-шумовые, неэффективные. Есть ли, на ваш взгляд, возможность повысить их эффективность, беря за основу их силовую часть? Это вопрос, заслуживающий или не заслуживающий внимания?

Представитель НИУ «МЭИ»

Я бы не занимался этим, честно говоря. Мы с вами пришли заниматься «интеллектуальным» РЭБом, я так скажу. Дело в том, чтобы подать имитационную помеху, вы должны знать четко последовательность перескока частот приёмника-передатчика. То есть, как они синхронно перескакивают. Но, это невозможно. Есть вариант перегрузить приёмник, входной его каскад. Для этого просто нужно знать, в каком диапазоне у него буквально шейки расстраиваются. И чтобы это знать, нужно слушать эфир. Слушайте эфир.

Представитель НИУ «МЭИ»

Уважаемые коллеги, позвольте, в плане чисто общего развития, я хотел бы небольшую информационную вставку дать по нашему противнику, как они решают эту проблему, как они вообще борются с дронами. У них на сегодняшний день основные усилия сосредоточены на борьбе с разведывательными дронами. Как наиболее дорогой и более эффективный сегмент вообще беспилотного парка. На 23 марта, по данным Координационного центра помощи Новороссии, (у нас этот центр перевёл аналитическую справку Украинского Главного управления разведки). Они приводят следующие данные, что сбито всего 2517 разведывательных дронов наших, российских. Из них ЗАЛА и ЗАЛА-20 -1272, СУПЕРКАМ, ОРЛАН и ОРЛАН-30 -306.

Что используют для этого? Цифры сами обсуждать не будем. Скорее всего, они завышены, несмотря на то что это аналитическое управление приводит данные: видеосъемка, фиксация, привязка по карте, по каждому дрону. Что они используют, для поражения наших БЛА? Меня вот больше интересует именно приемы их работы по борьбе с дронами.

Первый этап — это пеленгатор. Обычный, дешевый, простой пеленгатор. Кратковременно включается РЛС для точного наведения дрона-перехватчика на цель. Как правило, это израильская РЛС, которая работает практически в импульсном режиме. По этой РЛС наводится дрон-перехватчик и максимальный эффект дают удары из нижней полусферы.

Вы знаете, наверное, что сзади сейчас на ЗАЛА ставится верхняя камера, точнее, задняя камера, которая просматривает заднюю верхнюю полусферу. Так вот они сейчас заходят снизу вверх атакуют с набором высоты и бьют из нижней задней полусферы. И, показывают вот такие вот результаты. Вы видите, они используют самые простые решения. Элементарное. Пеленгатор, РЛС, перехватчик. РЛС очень хорошо маскируется.

Представитель НИУ «МЭИ»

Вот аналог Silvus, он как раз-таки на среднее небо и нужен, наверное, это вот лучшее решение.

Представитель КБ «Чистое небо»

Противники используют на шарах, на этих длиннолётах, которые на тысячи километров летают.

Они много, где его сейчас будут использовать, и чаще, и чаще. Если мы посмотрим на историю развития авиации вообще, в принципе, то всё вполне логично, ничего нового мы не изобретаем. Появились самолёты-разведчики, появятся самолёты-истребители. Появились самолёты-бомбардировщики, появятся самолёты-истребители. Единственное, в этой всей гонке за качеством и надёжностью связи выигрывает количество юнитов. То есть всё вот это решается в обычном воздушном контроле. Все написано за нас в боевом уставе ВВС, но если появились самолеты, которые представляют угрозу, их надо перехватывать, там, где их можно сбить, вот, над городом перехватывать их уже бесполезно, зачем его сбивать над городом, он все равно в детский садик попадет. Это комплексное решение должно быть, одной какой-то волшебной палочкой с одной кноп-

кой ничего не решить, вот что касается планирования, в идеале, это самый главный вопрос.

Вопрос, который уже всех достал. У меня от него, глаз дергается: какой нам РЭБ купить? Естественно, ответный вопрос на это, а какая у вас там радиообстановка? А мы не знаем, какая у нас радиообстановка. То есть, вот эта вот вся ерунда, вот эти дешевые, моментально изготавливаемые, носимые комплексы, примитивная радиоразведка, они как раз для этого нужны, чтобы на уровне, там, рота-батальон, как бы, не дожидаясь информации из центра, могли понять, что у них там работает, на каких частотах и какой РЭБ купить. Как минимум один вопрос уже спасает жизнь целого подразделения. Для этого нужно примитивное совершенно устройство, радиоприемное. За 15 минут любого человека можно обучить им пользоваться. Чего искать? Вот таблицы, все частоты, все известные, все данные. Но у нас люди такие, что они смотрят на эту таблицу в гугле, это очень сложно для понимания. Тут все очень просто, все линейно. Вот уже три года у нас работает приложение с нейросетью. Ну извините меня, три года я ее учу эту нейросеть, а свою жизнь ей полностью не доверю, потому что я знаю, что она тупая, как тряпка. Хотя она сильно помогает. Но то многообразие сигналов, с которыми мы сталкиваемся, оно подразумевает присутствие человека. Какой-то аналитический центр с нормальным, реальным человеком, он должен присутствовать. Значит, на любое противодействие. То есть, как противник пришел к воздушному перехвату? Ну, потому что других реальных вариантов остановить нас, там, как бы нет. БПЛА можно перехватить заранее. А как это перехватить заранее? Нужен какой-то уже активный способ противодействия. Мы первыми начали летать на луковом огне, между прочим, и естественно тут же им помогли израильтяне, а помимо израильского радиолокатора, его еще можно обнаружить даже вот этим примитивным устройством. А британские, которые поступили вот-вот месяц назад, они уже на частотах 9 и выше гигагерц работают. Тут уже нужно специальное оборудование. И если все пойдет и дальше, в сторону 20–30 гигагерцовых радаров, компактное, маленькое, дешевое устройство, но приближающийся дрон может определить четко. Но нам надо бороться не с дронами, а с причинами. Как я уже говорил, 100–500 налетов за сутки — это суровая реальность, противник так может.

Это значит, что где-то есть точка, из которой все взлетает, где-то включаются пульта, где-то работает ретранслятор. Уничтожение, то есть практика обнаружения ретрансляторов при помощи вот этих вещей. Можно обнаружить, когда треуголируют ретранслятор, с земли. А если бы у нас был са-

молет радиоподдержки, если бы была система, то можно было бы вопрос, который поступает сейчас от наших военных, решить. А можно сделать так, чтобы у меня в бункере сидел человек, смотрел на экран монитора и там на карте вот эти вот все радиоаномалии были видны? Идеальный случай. Вот что они хотят. Технические возможности. Вот это возможно. У нас 2 тысячи датчиков гуляют по фронту. Я уже молчу о том, что десятки, сотни тысяч разных спектр-анализаторов, поставленных всевозможными волонтерами, народными фронтами и тому прочими вещами. Да, мы заточили свое программное обеспечение, чтобы оно работало со всеми спектр-анализаторами, специально для тех, кто любит обнаружить. Но как передавать данные? Куда передавать данные? Как их обрабатывать? В рамках батальона, батальон имеет повышенную выживаемость, имея в своем составе примитивного совершенно занюханного, вчера наученного, примитивной радиоразведке человека с оборудованием. Уже все живы, все здоровы. Уже они не полезут выполнять задачу вот этим путем, они обойдут и выполняют задачу другим путем. Задача заключается не в том, чтобы прятаться от людей с оружием, а для того, чтобы их эффективно уничтожать и лишать этого оружия.

Представитель МО

По сути, резюме получилось, что надо исключать и уничтожать наиболее ценные и наиболее малочисленные элементы системы управления, операторов и ретрансляторы, но в данном случае пеленгатор выступает уже целью, поскольку уже противник применяет дроны с установленными на них пеленгаторами.

То есть любое излучение, любое движение в радиоспектре обнаруживается и автоматически поражается.

Представитель КБ «Чистое небо»

И самое главное, предположим, у нас есть прекрасные мобильные устройства, боевые суперкомплексы, первое — взаимодействие, второе — минимизация времени прохождения информации от момента извлечения информации до принятия решения. Более расширенный и углубленный анализ радиообстановки призывает быть интегрированным в систему управления боем. И тут точно так же, как с радиосвязью, с системой управления боем, мне народ говорит просто смертоносные вещи.

В мобильном телефоне, найдем кучу приложений, без которых сейчас не работает ни артиллерия, ни пехота, но у нас полный топографический кренинизм. Карты не меняются, а на земле овраги плывут, реки изменяют свое русло. И пользоваться картами, которым 80 лет, да лучше AlpineQuest поставить. Лучше пользоваться SAS-планетой, где в том числе за небольшую сумму можно получить спутниковые фотографии планеты.

Представитель НИУ «МЭИ»

Всё-таки вернёмся опять к конструктиву не будем обсуждать, как всё плохо, а лучше обсудим, что с этим всем делать.

Представитель Фонда НТИ

Это проблема, нет военного гаджета, он не разработан. А военный гаджет нужен, это узкое место.

Представитель ВУЦ МЭИ

Мы на тактике учили РУК, разведывательно-ударные комплексы. Это сегодня важнейший компонент. Уже вопрос задавался, что комплексы эти у нас в стране требуют развития.

Представитель МО

Для чего мы собрались? У нас есть технологические задачи - нет, мы наоборот как раз формулируем эту задачу, ее дальше надо оформлять в ТЗ, дальше ее демонстрировать и уже после исполнять, претворять в жизнь. Вот, собственно говоря, то, чем мы должны заняться.

Представитель НИУ «МЭИ»

Задачи уже появились в результате обсуждения, спасибо. Да, я вас прервал, вы хотели что-то сказать?

Представитель Фонда НТИ

Угрозы мы знаем, где они, кто они, чем они грозят и кому, это все понимаем. Задача стоит в том, чтобы инициировать и выполнить ОКР, который на выходе должен дать продукт, изделие, которое возьмут товарищи, которые

находятся на передке и будут эффективно с этим воевать. Этот продукт должен быть максимально эффективным. В данном случае лишить противника «зрения» - ситуационной осведомленности, которая позволяет ударным дронам, ракетным комплексам наносить удары по нашим объектам. Вот я бы сосредоточился на этом, и в основу идеи положил бы этот тезис, что надо с помощью различных систем, выявлять ключевые системы разведывательно-ударного контура противника и эффективно их поражать. Это наиболее правильно, на мой взгляд, я летчик сам. Мы сейчас работаем над темой поднять в воздух не просто дрон, а целую систему дронов, которые позволят собирать данные, передавать их куда надо. В этом центре управления и обработки вырабатываются решения в поддержку командира. А с учетом того, что уничтожить обнаруженные цели надо немедленно, фактически в режиме реального времени, потому, что если противник послал перехватчик к нашему дрону-разведчику, мы его видим, то надо его уничтожить, потому что разведчика мы спасти в этот момент никак по-другому не можем. Он тихоходный, он еле разворачивается, перехватчик всегда маневреннее, он его собьет, если увидит, а наша задача сделать так, чтобы обнаружить противника и воспрепятствовать его действиям. Эта работа по вскрытию частотного диапазона, позволяет нам выбирать критически важные цели и наносить по ним немедленные удары разными способами. Распознавание цели позволяет выбрать оптимальный способ противодействия, а еще очень важно то, что я услышал, хоть я знал это и раньше, но получил подтверждение, что взаимодействие - наше больное место. Поэтому, предлагаю все, что я сказал занести в протокол.

Представитель МО

И аналитика.

Представитель Фонда НТИ

Как хотите.

Представитель ЦПЛ «Апробация-БПЛА» ФПИ при МелГУ

Было сказано, что как только перехватчик увидел в оптическую систему нашу цель, то он фактически идет на цель, но, тогда может быть имеет

смысл мешать не каналу управления. Давайте мы будем мешать цифровому и аналоговому видеоканалу.

Представитель НИУ «МЭИ»

Это решение уже есть.

Представитель КБ «Чистое небо»

Мы пытались сбить украинский Драгонфиш, дорогой, очень желанный трофей, который противнику выдавал разведданные. То есть, когда летал Драгонфиш, в это же время летели «мопеды», так называемые, с двигателями внутреннего сгорания, со взрывчаткой и, как я полагаю, Драгонфиш корректировал нанесение ударов по ним. Так вот, приблизились к FPV-дронам где-то на дистанции 500 метров, отвалилось видео. То есть на этом разведывательном БЛА самолётного типа они установили какую-то коробочку, которая быстро определила наш видеоканал и по этому видеоканалу была поставлена помеха. Соответственно, учитывая, что самолёт находится в воздухе, а у нас приёмник видео на земле, то мы находимся в ущербном состоянии.

Представитель НИУ «МЭИ»

Ну, это аналог зеркальца, да?

Представитель КБ «Чистое небо»

Ну типа того. Хотя нет. Оператор должен увидеть, что кто-то заходит на него.

Представитель НИУ «МЭИ»

А «зеркальца» они ставят, кстати, сейчас на свои разведчики самолетного типа. Эта система выявляет сигнал нашего перехватчика и, просто, бьет более мощным сигналом, перебивает аналоговый сигнал самого дрона-перехватчика.

Представитель Фонда НТИ

Вот такие вещи должны быть массово на наших бортах, чтобы защититься.

Представитель КБ «Чистое Небо»

Это решено другим способом, дистанционным изменением канала передачи видео.

Представитель НИУ «МЭИ»

Если вы хотите... Это обязательно нужно, чтобы не забыть. Тут было сказано про то, что крылья обнаруживают с помощью радиолокационных средств, но всё-таки РПС-42, это же не совсем массовая история. Дело в том, что этот израильский радар. Значит, изначально кто начал, инициировал борьбу с крыльями? Есть такой вражеский специалист по радиосвязи, РЭБу. Сейчас он не занимается ликбезом, а раньше в 2023–2024 годах он своим и нашим объяснял, как понять, что РЭБ работает и так далее.

Дело в том, что он на своих страницах в блоге говорил, что нужно собирать сигнатуры разведчиков. Именно радиочастотные сигнатуры. То есть наши разведывательные дроны сбрасывают видео. Скорее всего видео цифровое. То есть там не аналоговые передатчики, там шифрованное видео, и соответственно они научили расчеты. Там тоже есть аналоги «мастерков», я недавно видел. У них прямо на металле написаны частоты с указанием, какой аппарат соответствует какому диапазону частот. Без указаний каких-то модуляций, просто, куда смотреть и что это за аппарат.

Представитель КБ «Чистое Небо»

Но тут надо упомянуть обязательно, что в основном там даны частоты нашей техники, ЗАЛЫ, Ланцетов и Гераней, которые за все три года ни на грамм не сдвинулись. Обнаружение наших БЛА вести достаточно легко, потому что частоты находятся до 3 ГГц, а до 3 ГГц нам суперматематики и суперфизики не надо, для того чтобы эти частоты отслеживать и мониторить. Они пишут, что на 3 ГГц начинается танец с бубном. Ведь, смотрите, в 22-м году, где-то в конце апреля месяца, появился Mavic 3. Чем он отличался от предыдущих моделей? До этого все дроны подлетали на прямую видимость, то есть это 200–150 метров. Но 150–200 метров для нормального стрелка с автомата Калашникова, это дистанция, на которой спокойно уничтожается дрон разведчик если ты его услышал и заметил. А с появле-

нием Мавик-3 с оптическим зумом в четыре крата стало возможно следить за точкой интереса с дистанции в 2–2,5 километра. Все, ты его не видишь, не слышишь, поразить ты его не можешь. Тут возникла необходимость в пассивной пеленгации источников радиоизлучения, потому что прежде чем выдвинуться на КАМАЗе с вооружением на точку, надо проверить, нет ли глаз. Потому что артиллерия работала на ура, только заметили цель, через 2–3 минуты удар. И это стало проблемой. Встал вопрос о том, как обнаруживать разведчиков, потому что уже в конце 22-го года полностью пошли крылья, небо наполнилось БЛА, которые летают не 40 минут, как маленькие, а 2–3 - 4 часа. Но, имея возможность следить за какой-то областью, через буквально сутки мы знаем о подразделении все, где у них что находится, где склады, где машины прячутся, где люди прячутся, где они едят, где они в туалет ходят.

Представитель НИУ «МЭИ»

Вопрос, а у нас систематизируют их сигнатуры?

Представитель КБ «Чистое Небо»

Каждый тянет сигнатуру к себе куда-то. Я, никому не покажу, это моё, это ноу-хау, я знаю, никому больше не расскажу.

Представитель НИУ «МЭИ»

Потому что, самое удивительное, что та сторона, в открытую публикует наши частоты и даже тип сигнала показывает.

Представитель НИУ «МЭИ»

Мы говорили про центры, которые создали на Украине. Конечно, это одна из задач такого центра: сбор, обобщение, анализ материалов. Поэтому, в этом плане мы здорово отстаем.

Представитель НПО «Алмаз»

Кто может мне сказать: где у нас проводится сбор, обобщение и анализ информации о технических средствах противника.

Представитель КБ «Чистое Небо»

Трудно найти трофеи. Необходимые узлы куда-то растаскивают. То дают на один день, а за день я ничего не успею.

Представитель КБ «Чистое небо»

У меня есть вот здесь на флешке занятные документы, которые мы в 2023 году перевели. Один из документов в армии США. Обращайтесь. Всё грамотно расписано. Представлено и вертикальное, и горизонтальное взаимодействие между родами войск, между различными уровнями, командами, и так далее. И без результатов радиоразведки никаких решений вообще не принимают.

Представитель «Кристофор и Никас»

Давайте тогда - необходимы какие-то протоколы. Для систематизации, классификации использования, необходимо какие-то формулы. Мне надо какое-то системное решение по поводу хранения информации.

Представитель НИУ «МЭИ»

На этом наш семинар заканчиваем. Всем спасибо за участие.