



КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ
ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

Защита уязвимых объектов от террористических нападений с использованием беспилотных авиационных систем (БАС)

РУКОВОДСТВО ПО ПЕРЕДОВОЙ ПРАКТИКЕ

Специализированный модуль



Глобальная программа по противодействию террористическим угрозам
в отношении уязвимых целей

Осуществляется в партнерстве с:



UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)



UNAOC
United Nations Alliance of Civilizations



unicri
United Nations
International Crime and Justice
Research Institute



КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ
ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

Защита уязвимых объектов от террористических нападений с использованием беспилотных авиационных систем (БАС)

РУКОВОДСТВО ПО ПЕРЕДОВОЙ ПРАКТИКЕ
Специализированный модуль

**Глобальная программа по противодействию террористическим угрозам
в отношении уязвимых целей**

Осуществляется в партнерстве с:



UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)



UNAOC
United Nations Alliance of Civilizations



unicri
United Nations
Interregional Crime and Justice
Research Institute

Содержание

Предисловие	v
Указатель вставок	vii
Указатель конкретных примеров	viii
Указатель программных документов	ix
1. Террористические угрозы, связанные с применением БАС против уязвимых объектов	1
2. Подверженность уязвимых объектов террористическим нападениям с применением БАС	10
3. Снижение риска и реагирование: роли заинтересованных сторон и передовой опыт	13
3.1 Государства-члены	14
3.1.1 Субъекты, определяющие политику	14
3.1.2 Правоохранительные органы	35
3.1.3 Разведывательные службы	49
3.2 Неправительственные субъекты	51
3.2.1 Операторы уязвимых объектов	51
3.2.2 Производители БАС и важнейших подсистем	56
3.2.3 Поставщики и розничные торговцы БАС	60
3.2.4 Поставщики технологий противодействия БАС	63
3.2.5 Пользователи БАС	63
3.2.6 Пользователи уязвимых объектов	65
3.2.7 Организации гражданского общества (ОГО)	65
Справочные материалы	67



Предисловие

Этот документ был разработан Глобальной программой КТУ ООН по противодействию террористическим угрозам в отношении уязвимых целей¹ в качестве руководства по защите уязвимых объектов от террористических нападений с применением БАС. Он задуман как отраслевой модуль, дополняющий «Сборник передовых методов по защите критически важных объектов инфраструктуры от террористических атак» (Compendium of Good Practices on the Protection of Critical Infrastructure Against Terrorist Attacks)².

В настоящем модуле после обзора основных угроз террористических нападений с использованием БАС и уязвимости к такого рода нападениям, а также все более явных указаний на то, что террористы намерены использовать БАС для совершения нападений, рассматриваются конкретные роли, которые отдельные заинтересованные стороны могут и должны играть в сложной и часто нестабильной обстановке в плане безопасности, действуя в концептуальных рамках подхода, предусматривающего управление рисками и регулирование кризисов.

Каждая часть содержит подборку конкретных примеров, наглядно демонстрирующих, как ключевые принципы, связанные с вопросами безопасности, включая рекомендации, одобренные на международном уровне, используются на практике правительствами, субъектами частного сектора, операторами уязвимых объектов и организациями гражданского общества. В модуле также обобщается содержание нескольких программных документов (например, руководств, справочников и сборников), в которых содержатся директивы в отношении продуманных стратегий и оперативных параметров, помогающих снизить степень незащищенности целей, уязвимых к террористическим нападениям с применением БАС, и повысить их устойчивость.

Приведенные в этом модуле аналитические рамки, конкретные примеры, программные документы и материалы являются результатом интенсивных камеральных исследований, официального запроса на представление материалов, направленного всем 193 государствам — членам Организации Объединенных Наций, обсуждений с отдельными экспертами,

1 Эта программа осуществляется в партнерстве с Исполнительным директором Контртеррористического комитета Организации Объединенных Наций (ИДКТК), Альянсом цивилизаций Организации Объединенных Наций и Межрегиональным научно-исследовательским институтом Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ). Она осуществляется в тесном взаимодействии с другими соответствующими организациями, включая Интерпол. Дополнительная информация: <https://www.un.org/counterterrorism/ru/vulnerable-targets>.

2 Сборник был разработан в 2018 году в рамках Рабочей группы по защите критически важной инфраструктуры, в том числе уязвимых объектов, интернета и безопасности туризма, при Целевой группе Организации Объединенных Наций по осуществлению контртеррористических мероприятий (ЦГОКМ). В 2019 году ЦГОКМ вошла в структуры Глобального договора Организации Объединенных Наций по координации контртеррористической деятельности (Договор). В рамках этой новой структуры рабочие группы ЦГОКМ по защите критически важной инфраструктуры, в том числе уязвимых объектов, интернета и безопасности туризма, и по предупреждению нападений с применением оружия массового уничтожения и принятию ответных мер были объединены в Рабочую группу Договора по возникающим угрозам и защите критически важной инфраструктуры.

представителями международных организаций и партнерами по проектам, а также материалов, представленных Рабочей группой по возникающим угрозам и защите критически важной инфраструктуры Глобального договора Организации Объединенных Наций по координации контртеррористической деятельности³.

Важные выводы были сделаны по итогам двух совещаний Группы экспертов, которые были проведены КТУ ООН и в которых приняли участие эксперты со всего мира (представляющие государства-члены, международные и региональные организации, группы гражданского общества, частный сектор и научные круги). Первое совещание состоялось 29 июня 2021 года, во время проведения Организацией Объединенных Наций виртуальной Недели борьбы с терроризмом, а второе — 6 октября 2021 года. Кроме того, в этом процессе были использованы материалы, представленные Советником по гендерным вопросам КТУ ООН и специальным консультантом по правам человека КТУ ООН и Сектора специальных проектов и инноваций.

Настоящий модуль содержит обширные перекрестные ссылки на документ «К разработке технического руководства, призванного облегчить осуществление резолюции 2370 Совета Безопасности и применение соответствующих международных стандартов и передовой практики по недопущению приобретения оружия террористами» (далее — документ «Техническое руководство по резолюции 2370 СБ ООН»), который включает подмодуль II, посвященный предотвращению приобретения террористами БАС и их компонентов⁴.

3 URL: <https://www.un.org/counterterrorism/global-ct-compact>.

4 URL: www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Mar/technical_guidelines_to_facilitate_the_implementation_of_security_council_resolution_2370_2017_and_related_international_standards_and_good_practices_on_preventing_terrorists_from_acquiring_weapons.pdf. По состоянию на декабрь 2021 года документ «Техническое руководство по резолюции 2370 СБ ООН» находился на завершающей стадии разработки. Его составление является частью совместного проекта, осуществляемого ИДКТК от имени Рабочей группы по управлению границей и правоприменению Глобального договора Организации Объединенных Наций по координации контртеррористической деятельности (РГ УГП). Этот проект финансируется Контртеррористическим центром Организации Объединенных Наций (КТЦ ООН) при КТУ ООН и осуществляется совместно КТЦ ООН и Институтом Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИП) в тесном сотрудничестве с организациями, входящими в РГ УГП.



Указатель вставок

Вставка 1.	Угроза применения террористами БАС и химических, биологических, радиологических и ядерных (ХБРЯ) материалов	3
Вставка 2.	БАС как цели кибератак и как средства их совершения	5
Вставка 3.	Слабые места в информационно-технологической инфраструктуре для БАС	12
Вставка 4.	Рекомендация ИКАО по разработке общегосударственной стратегии в области применения БАС	18
Вставка 5.	Управление движением беспилотных авиационных систем (УДБ)	22
Вставка 6.	Перспективные задачи международного сотрудничества в области пресечения применения БАС в террористических целях	31
Вставка 7.	Соблюдение прав человека и основных свобод при проведении правоохранительных операций с использованием БАС	35
Вставка 8.	Включение информации, собранной с помощью БАС, в работу центров синтеза	38
Вставка 9.	БАС и поиски точек запуска	40
Вставка 10.	Потенциальная опасность сбитых беспилотных летательных аппаратов: случай в северном Ираке	45
Вставка 11.	Международный сговор с целью приобретения БАС	46
Вставка 12.	Сеть группы ДАИШ по закупке БАС	50
Вставка 13.	Производители БАС и решения, использующие технологию геозонирования	57
Вставка 14.	Сигналы опасности и отсутствие должной осмотрительности в деле группы компаний АйБАКС	61
Вставка 15.	«БАС как услуга»	64



Указатель конкретных примеров

Конкретный пример 1.	Стратегия Европейского союза по противодействию БАС в контексте борьбы с терроризмом	18
Конкретный пример 2.	Стратегия Соединенного Королевства по противодействию применению беспилотных летательных аппаратов	20
Конкретный пример 3.	Подход Сингапура к рискам для безопасности, связанным с БАС	21
Конкретный пример 4.	Нормативно-правовая база ЕС по БАС	23
Конкретный пример 5.	Система управления рисками, принятая в Объединенных Арабских Эмиратах в отношении воздушных судов, несанкционированно проникающих в контролируемое воздушное пространство	24
Конкретный пример 6.	Методология выбора правильной технологии противодействия БАС: проект «Отважный»	26
Конкретный пример 7.	Программа финансирования «Акселератор обороны и безопасности»	27
Конкретный пример 8.	Ресурсный центр «Безопасность БПЛА	28
Конкретный пример 9.	Использование БАС для предотвращения террористических актов: опыт Коста-Рики	34
Конкретный пример 10.	Тестирование и оценка мер противодействия БПЛА: учения Интерпола и норвежской полиции	41
Конкретный пример 11.	Применение БАС полицией Каталонии	42
Конкретный пример 12.	Полномочия на задержание и проведение досмотра в целях поиска БАС	46
Конкретный пример 13.	Отраслевая ассоциация коммерческой беспилотной авиации Южной Африки	58
Конкретный пример 14.	Группа по деятельности в отрасли беспилотной авиации	59
Конкретный пример 15.	Выявление уязвимостей: программа «Отлов багов»	60
Конкретный пример 16.	Программа сертификации «БАС-сейф» (UASafe) для розничных продавцов БАС в Великобритании	62
Конкретный пример 17.	БАС без границ	66



Указатель программных документов

Программный документ 1. Исламское государство и БАС: поставки, масштабы и будущие угрозы — Центр по борьбе с терроризмом в Вест-Пойнте, 2018 год	8
Программный документ 2. Как анализировать киберугрозы от применения БАС: исходные данные, рамки анализа и инструменты для проведения анализа — «Рэнд корпорейшн», 2020 год	9
Программный документ 3. Берлинский меморандум о передовых методах противодействия применению беспилотных авиационных систем в террористических целях — Глобальный контртеррористический форум (ГКФ), 2019 год	14
Программный документ 4. Инструментарий по БАС — ИКАО	16
Программный документ 5. Типовые правила ИКАО в отношении БАС	25
Программный документ 6. Работа с общественностью: просвещение и улучшение информированности — инструментарий ИКАО	29
Программный документ 7. Передовая практика и гарантии развертывания технологий противодействия БАС — Министерство транспорта Соединенного Королевства	43
Программный документ 8. Противодействие беспилотным авиационным системам: руководство по технологиям — Министерство внутренней безопасности и Национальная лаборатория технологий обеспечения безопасности в городах	44
Программный документ 9. Системы противодействия беспилотным летательным аппаратам: Центр изучения беспилотных летательных аппаратов при Бард-колледже	44
Программный документ 10. Рамочная программа реагирования на инциденты с применением беспилотных летательных аппаратов для сотрудников экстренных служб и специалистов по цифровой криминалистике, Интерпол	48
Программный документ 11. Заявление о глобальном контексте риска в области авиационной безопасности, документ 10108, ИКАО	53
Программный документ 12. Урегулирование инцидентов с беспилотными летательными аппаратами на аэродромах, Европейское агентство по авиационной безопасности (ЕАСА)	54
Программный документ 13. Защита от угрозы со стороны беспилотных авиационных систем: передовая практика Межведомственного комитета безопасности, Межведомственный комитет безопасности, США	55
Программный документ 14. Противодействие угрозам со стороны беспилотных авиационных систем: обеспечение готовности вашего объекта, Центр защиты национальной инфраструктуры, Соединенное Королевство	56

Террористические угрозы, связанные с применением БАС против уязвимых объектов



Беспилотные летательные аппараты (БПЛА) – это летательные аппараты, которые не требуют присутствия на борту человека в качестве пилота. БПЛА представляют собой летающий компонент беспилотных авиационных систем (БАС), в которые входят также наземные станции управления (НСУ) и полезная нагрузка⁵.

БАС могут использовать различные типы навигации, обеспечивающие им различную степень автономности от вмешательства человека⁶. Габариты и вес БАС, их форма и технологическое оснащение, а также цены на них могут быть очень разными. Их конструкция может предусма-

тривать их применение как в военной, так и в гражданской сфере. Среди моделей, предназначенных для применения в гражданских целях, встречаются любительские – приобретаемые для развлечения или как объект хобби – и те, что используются в профессиональных целях. Сфера применения последних широка и постоянно расширяется: от мониторинга и обработки сельскохозяйственных культур до промышленного контроля, спасательных операций/операций по оказанию помощи при стихийных бедствиях и т. д.

Совершенствованию БАС способствуют стремительный технический прогресс⁷, а

5 См. Техническое руководство по резолюции 2370 СБ ООН, подмодуль II, «Компоненты БАС» (п. 1.1.4).

6 Основными способами обеспечения навигации БАС являются: i) навигация в ручном режиме, осуществляемая по радиосвязи между БАС и наземной станцией управления; ii) GPS-навигация, не зависящая от радиосигналов и позволяющая запрограммировать БПЛА на автономный полет в заданные точки или на следование по определенным участкам маршрута; iii) автономная навигация, основанная на собственных бортовых датчиках БПЛА и позволяющая аппарату следовать за движущимися объектами/людьми или осуществлять наведение на неподвижные объекты.

7 Высокий рыночный спрос подстегивает разработку все более сложных датчиков, развитие возможностей автома-

также достижения в области разработки и применения искусственного интеллекта (ИИ)⁸. Модернизация или усовершенствование многих свободно продающихся БАС в соответствии с индивидуальными потребностями пользователей не требует больших усилий. Другие БАС (так называемые «БАС, выполненные по индивидуальному заказу») собираются с использованием компонентов, которые приобретаются и подбираются индивидуально, с тем чтобы готовые системы удовлетворяли конкретным требованиям, предъявляемым к ним пользователями.

Хотя во многих отношениях БАС вносят очевидный вклад в обеспечение безопасности и в процесс развития общества, они также открывают мир новых возможностей для террористов. Растущий уровень точности и надежности, а также простота применения и легкость, с которой пользователи могут интегрировать в эти устройства индивидуально разработанные функции, дают простор для чрезвычайно широкого законного их использования, но в то же время предоставляют возможность применять их в преступных и террористических целях.

Совет Безопасности Организации Объединенных Наций уже признал эту проблему и потребовал принять меры по снижению угрозы попадания БАС в руки террористов. В частности, в резолюции 2370 (2017)⁹ решительно осуждается «непрекращающийся поток оружия, включая стрелковое оружие и легкие вооружения, военную технику, беспилотные авиационные системы (БАС) и их компоненты и компоненты самодельных взрывных устройств, которые поступают к ИГИЛ (известному также как ДАИШ), «Аль-Каиде», их подразделениям и связанным с ними группам,

незаконным вооруженным группам и преступникам и циркулируют между ними», и государствам-членам рекомендуется «не допускать и дезорганизовывать сети по добычанию такого оружия, систем и компонентов».

В нынешней ситуации в области глобальной безопасности риск приобретения БАС террористическими группами и накопления ими опыта обращения с ними и их эффективного применения/использования, как представляется, растет под воздействием ряда сопутствующих факторов, таких как¹⁰: а) нерегулируемый и все более сложный гражданский рынок технологий БАС; б) широкая доступность нерегулируемых, неконтролируемых и незащищенных взрывчатых веществ, которые могут быть использованы в качестве полезной нагрузки для БАС; в) доступ к прекурсорам взрывчатых веществ (нитрат аммония, перекись и т.д.); д) наличие технических знаний у террористов и связанных с ними лиц и групп, а также передача этих знаний и опыта.

Вышеизложенное не обязательно означает, что в обозримом будущем БАС станут основным или широко распространенным средством совершения нападений в террористических целях. Однако поступает все больше сигналов о том, что негосударственные субъекты пытаются использовать БАС для достижения целей, связанных с терроризмом, далеко за пределами районов, затрагиваемых военными операциями. В сочетании с общей уязвимостью многих «слабозащищенных целей» к нападениям с воздуха и их потенциально несоизмеримым по силе воздействием это указывает на повышенный риск успешных нападений на такие объекты.

тики, производство более мощных аккумуляторов и т. д. При нынешнем высоком темпе внедрения инноваций в этом секторе модели БАС постоянно сменяются новыми, более эффективными продуктами.

8 Беспилотные авиационные системы с искусственным интеллектом будут представлять собой автономные системы вооружений, способные самостоятельно искать, выбирать и поражать цели. Возможно, их развертывание уже произошло в Ливии, когда «колонны тылового обеспечения и отступающие подразделения сил, примкнувших к Хафтару, были выслезены и дистанционно атакованы боевыми беспилотными летательными аппаратами или смертоносными автономными системами вооружений и другими барражирующими боеприпасами. Смертоносные автономные системы вооружений были запрограммированы на поражение целей, не требующее связи между оператором и боеприпасами: по сути, это было полноценное применение механизма автономного режима наведения» (Группа экспертов по Ливии 2021 год, п. 63).

9 Идентичное положение содержится в последующих документах Совета Безопасности, таких как резолюция 2482 (2019).

10 Источник: параллельное мероприятие, организованное КТУ ООН 29 июня 2021 года (в рамках виртуальной Недели борьбы с терроризмом, проведенной Организацией Объединенных Наций).



Вставка 1.

Угроза применения террористами БАС и химических, биологических, радиологических и ядерных (ХБРЯ) материалов

Для того чтобы вызвать инцидент, связанный с химическими, биологическими, радиологическими или ядерными материалами, враждебно настроенные субъекты могут применить БАС в качестве систем доставки таких материалов, используя способность БАС нести полезную нагрузку¹¹, или применить БАС в качестве оружия для нанесения удара по объекту, в котором имеются такие материалы.

Первый в истории случай, когда негосударственные субъекты попытались применить ХБРЯ-материалы в сочетании с БАС в террористических целях, произошел в 1994 году, когда милленаристская секта «Аум синрикё» предприняла неудачную попытку использовать два вертолета с дистанционным управлением для распыления зарина. В 2015 году одному человеку удалось запустить беспилотный летательный аппарат с радиоактивным песком на крышу офиса премьер-министра Японии. Примечательно, что беспилотник обнаружили лишь случайно спустя несколько дней. Годом позже со стороны тогдашнего премьер-министра Великобритании прозвучало предупреждение о том, что связанные с ИГИЛ/ДАИШ группы планируют осуществить террористические акты с применением «грязных» бомб, распыляя ядерные материалы с беспилотных летательных аппаратов над густонаселенными городскими районами.

В 2019 году французская Координационная группа по борьбе с терроризмом (UCLAT) опубликовало конфиденциальный доклад, в котором предупреждалось о «возможном террористическом акте на футбольном стадионе с использованием беспилотного летательного аппарата, который может нести боевые биологические вещества». Это предупреждение было воспроизведено комиссаром Европейского союза по вопросам безопасности¹².

11 Например, БАС, созданные для сельскохозяйственных целей, то есть для распыления пестицидов над сельскохозяйственными культурами, могут быть переоборудованы для распыления химических, биологических, радиологических или ядерных материалов.

12 Об угрозе применения БАС против зрителей и спортсменов, особенно во время многолюдных спортивных соревнований, упоминается в «Руководстве по обеспечению безопасности крупных спортивных мероприятий»; *Guide on the Security of Major Sporting Events*, UNOCT, UNICRI, UNAOC, ICSS, 2021, p. 36, at: <https://www.unaoc.org/wp-content/uploads/GUIDE-on-MSE-Security-with-Annex-Final.pdf>.

Вставка 1. (продолжение)

Эта угроза считается потенциально серьезной ввиду несоразмерных последствий, которые может иметь одна-единственная успешная попытка. Кроме того, хотя нападение с использованием БАС с нагрузкой из химического, биологического, радиологического и ядерного материала не обязательно нанесет большой ущерб людям, оно окажет на население сильное психологическое воздействие. Даже активные вещества нелетального действия могут вызвать массовую панику в том случае, если, к примеру, несколько БАС распылят токсичные вещества во время пролета над стадионом¹³. Кроме того, ликвидация последствий нападения, совершенного с применением химического, биологического, радиологического или ядерного вещества, может потребовать проведения весьма дорогостоящих операций по очистке больших территорий, а работа сотрудников аварийных и спасательных служб по разбору завалов, выполнению поисковых мероприятий и восстановлению инфраструктуры может быть серьезно затруднена из-за уровня загрязнения¹⁴.

Существующая международно-правовая база учитывает возможность использования БАС негосударственными субъектами для доставки химического, биологического, радиологического и ядерного оружия и требует от государств-членов принятия соответствующих мер контроля. Совет Безопасности в своей резолюции 1540 (2004), среди прочего, постановил, что государства в соответствии со своими национальными процедурами принимают и эффективно применяют соответствующие законы, запрещающие любому негосударственному субъекту производить, приобретать, иметь в собственности, разрабатывать, перевозить, передавать или применять ядерное, химическое или биологическое оружие и средства его доставки.

Поскольку БАС представляют собой «средства доставки», резолюцию 1540 можно рассматривать как полноценный инструмент, требующий от стран остановить распространение БАС, которые могут быть использованы для совершения террористических актов, в том числе с применением химического, биологического, радиологического или ядерного оружия.

В последние несколько лет правоохранные органы выявляли и срывали различные связанные с терроризмом планы, предусматривающие использование БАС вне зон конфликта¹⁵. Помимо прочего, к ним относятся следующие случаи:

- во время Олимпийских игр 2016 года в Рио-де-Жанейро боевики «Аль-Каиды» получили инструкции по совершению нападений на спортсменов и зрителей с использованием различных технологий, включая применение БАС со взрывчаткой. Как сообщается, на следую-

щий день, в связи с проведением игр бразильская полиция арестовала группу из десяти подозреваемых (Moore 2016);

- в 2019 году у группы боевиков в окрестностях Джакарты была обнаружена беспилотная авиационная система и аккумуляторы. В следующем году подразделение полиции Индонезии, занимающееся борьбой с терроризмом, провело ряд арестов, выявивших намерения террористов использовать БАС

13 Замечания старшего консультанта УНП ООН Гюнтера Поводена, высказанные на организованном КТУ ООН совещании Группы экспертов по уязвимым целям и беспилотным авиационным системам, прошедшем 6 и 7 октября 2021 года.

14 Общую оценку проблем, с которыми могут столкнуться негосударственные субъекты при применении химических, биологических, радиологических или ядерных действующих веществ с помощью БАС, см. в презентации Филиппа К. Блика «Угрозы применения террористами БАС и ХБРЯ-веществ и ответные меры» на конференции «Противодействие БАС, 2020», проведенной компанией Defense IQ 4 июня 2020 года, URL: <https://www.middlebury.edu/institute/news/UAS-and-cbrn-terrorism-threats-and-responses>.

15 Дон Расслер составил полный список предполагаемых террористических замыслов, предусматривавших применение БАС в период до конца 2016 года. Расслер проводит четкое различие между «террористическими структурами, которые проявляют ограниченный интерес» к БАС, и террористическими структурами, применение которыми БПЛА «является постоянным и достаточно развитым, чтобы называться "программой"» (Rassler 2016).

(Association of the United States Army, 2021);

- в сентябре 2020 года датский апелляционный суд подтвердил обвинительные приговоры, вынесенные судом первой инстанции в отношении трех человек, осужденных за содействие и оказание поддержки ДАИШ¹⁶. Примечательно, что «эти лица приобрели детали к летательным аппаратам (БПЛА, или «дронам») любительского класса, которые должны были использоваться в ходе реализации программы ДАИШ по применению БПЛА и в деятельности, связанной с боевыми действиями в Сирии и Ираке» (Europol 2021, p. 37).

С возвращением иностранных боевиков-террористов (ИБТ) из Сирии и Ирака возникли опасения, что связанные с ИГИЛ/ДАИШ группы планируют распространить в своих странах освоенные ими в боевой обстановке технологии, подразумевающие применение БАС, и соответствующую тактику¹⁷ (Глобальный контртеррористический форум, 2019 год).

БАС дают террористическим группам ряд преимуществ в рамках их стратегий нападения, наиболее важным из которых является возможность обойти традиционные меры физической защиты, предполагающие обеспечение безопасности на раз-

ных уровнях (например, путем создания укрепленного периметра объекта с целью пресекать нападения с использованием транспортных средств, привлечения вооруженной охраны или применения заграждений для осуществления досмотра посетителей). Более того, многие модели БАС дешевы и просты в обращении, что создает дополнительный стимул для групп или отдельных лиц, ищущих новые недорогие пути осуществления террористической деятельности.

Кроме того, управлять БАС можно из скрытых или защищенных мест, что снижает риск подвергнуться ответным мерам. Технологии, позволяющие управлять БАС, находящимися вне пределов прямой видимости, на данный момент широко применяются в различных коммерческих программах и приложениях, разработанных для нужд государственных органов. В случае использования этих технологий в незаконных, в том числе террористических, целях обнаружение и задержание правоохранительными органами лиц, управляющих БАС, значительно затруднено. Помимо этого, оснащение БАС видеокамерами дает потенциальным террористам возможность максимально усилить медийный эффект от своих действий, например путем размещения в социальных сетях видеозаписей своих нападений с воздуха¹⁸.



Вставка 2.

БАС как цели кибератак и как средства их совершения

В зависимости от того, взламывают их или используют для взлома других устройств, беспилотные авиационные системы могут быть как целями кибератак, так и средствами их совершения.

16. Последнее решение суда было обжаловано в Верховном суде Дании.

17. Отмечая, что «организация ИГИЛ/ДАИШ неоднократно использовала БАС в Ираке и Сирии для осуществления нападений, ведения разведки и пропаганды в боевой обстановке», составители Берлинского меморандума о передовых методах противодействия применению беспилотных авиационных систем в террористических целях утверждают, что «такие знания и опыт могут быть привезены из этих стран возвращающимися иностранными боевиками-террористами (ИБТ) или же могут послужить образцом для подражания для доморощенных террористов, включая одиночек».

18. Эксперты по безопасности также рассматривают потенциальные сценарии, в которых террористические группы интегрируют в БАС программное обеспечение для распознавания лиц, чтобы получить возможность совершать целенаправленные убийства, или переформируют программное обеспечение, разработанное для оценки размера толпы, таким образом, чтобы применение ими БАС повлекло за собой максимальное количество жертв (Дон Расслер, совещание Группы экспертов, проведенное КТУ ООН 6 и 7 октября 2021 года).



Вставка 2. (продолжение)

- **БАС как цели:** террористы могут попытаться получить контроль над БАС с целью ее захвата/уничтожения, изменения ее маршрута, а также осуществления вмешательства в ее данные¹⁹. Например, передавая фальшивую информацию в GPS-модуль беспилотной авиационной системы, можно обмануть это устройство, заставив его думать, что оно следует по запланированному маршруту. Если ошибки, присутствующие в программном обеспечении, не будут регулярно выявляться и исправляться, то у террористов появятся значительные возможности использовать эти бреши в системе безопасности для получения доступа к законно зарегистрированным и эксплуатируемым БАС, включая те, которые выполняют задачи по обеспечению правопорядка и иные задания органов государственной власти. Потенциально террористы могут получить контроль над официально действующей БАС и использовать ее против того уязвимого или многолюдного объекта, безопасность которого она была должна обеспечивать.
- **БАС как средства:** террористы могут попытаться использовать БАС для проведения кибератак на цели, не являющиеся БАС. В рамках этого сценария БАС применяется в качестве «кибероружия» для внедрения вредоносных программ в другие системы, например в критически важную информационную инфраструктуру. С распространением технологии 5G в качестве нового стандарта для широкополосных сотовых сетей «коммуникационная полезная нагрузка» может стать более простым в применении инструментом для нарушения работы частной беспроводной связи.

Источник: Ley Best & Others 2020.

Террористические группы могут использовать БАС для достижения различных целей²⁰. В отношении уязвимых целей они могут осуществлять:

- *разведку, наблюдение и рекогносцировку.* БАС могут использоваться для сбора информации о плохо заметных с земли слабых местах определенных объек-

19 В 2009 году иракские повстанцы, используя программное обеспечение, приобретенное в Интернете за 26 долл. США, смогли проникнуть в американские беспилотные авиационные системы и перехватить прямую видеотрансляцию, которая шла с самих БАС на американские приборы управления, что позволяло им выявлять потенциальные цели. Взлом был обнаружен только после того, как США получили доступ к принадлежавшим боевикам ноутбукам, на которых хранились многочасовые видеозаписи.

20 Cf. UNSCR 2370 Technical Guidance document, Submodule II, "Terrorist use of UAS" (1.1.2).

тов, с тем чтобы впоследствии использовать обнаруженные уязвимости для организации террористического нападения с помощью обычных средств или беспилотных летательных аппаратов;

- *нападения.* БАС могут быть намеренно направлены на столкновение с целью, с тем чтобы вызвать жертвы и/или нанести материальный ущерб. Террористы могут также использовать способность БАС нести полезную нагрузку для сброса взрывных устройств²¹ или распыления химических, биологических, радиологических или ядерных материалов (см. вставку 1). Полезной нагрузкой БАС могут также быть средства радиоэлектронной борьбы, например оборудование, создающее помехи на тех радиочастотах, которыми пользуется персонал служб безопасности во время проведения крупного мероприятия. Эффективность БАС, адаптированных под применение в военных целях, может быть многократно увеличена за счет их массового использования («роем»). В настоящее время управление БАС обычно происходит по схеме «один БПЛА — один оператор», однако в обозримой перспективе вполне может стать возможным одновременный запуск большого количества устройств, образующих мощный, слаженно действующий флот²²;
- *пропагандистскую деятельность.* Стремясь максимально усилить медийный эффект от своих действий, террористы могут применять БАС для видеодиффамации своих нападений на многолюдные и уязвимые объекты и публиковать эти шокирующие кадры. Использование беспилотных авиационных систем

в пропагандистских целях было отличительной чертой программы применения БАС группировкой ДАИШ²³;

- *вмешательство в работу служб и проведение мероприятий.* Даже если БАС не оснащены оружием, их полеты в воздушном пространстве контролируемого или ограниченного доступа могут крайне неблагоприятно сказываться на функционировании государственных органов и объектов критически важной инфраструктуры, проведении крупных мероприятий и т. д. В последние годы во всем мире отмечались случаи обнаружения БАС вблизи периметра аэропортов или внутри него, что приводило к сбоям в работе гражданской авиации и значительным экономическим последствиям и ущербу²⁴. Ни в одном из этих случаев не была установлена какая бы то ни было связь с террористической деятельностью, и можно предположить, что в большинстве этих случаев несанкционированное применение БАС стало результатом халатности или безрассудства операторов или их намерения нарушить правила и привлечь внимание СМИ.
- *вскрытие или усиление уязвимости целей:* нельзя исключать что БАС могут использоваться для конкретной задачи — отвлечь внимание сотрудников и ресурсы правоохранительных органов и органов безопасности от реальной цели. Если такую цель не обеспечить защитой, то впоследствии на нее может быть осуществлено нападение с применением обычных средств или оснащенных оружием БАС ввиду ее повышенной уязвимости.

21 В августе 2018 года было совершено неудавшееся покушение на президента Венесуэлы Мадуро с применением двух начиненных взрывчаткой БАС с GPS-наведением. В другом случае организация ИГИЛ/ДАИШ неоднократно использовала БАС в зонах конфликта для сброса небольших бомб размером с гранату. Хотя использование таких устройств не оказало решающего воздействия на исход конфликта, оно показало, насколько потенциально опасными могут быть последствия злонамеренного применения простейших БАС, разработанных в любительских и развлекательных целях.

22 Сценарий применения БАС роем был опробован в 2018 году в Сирии, когда две российские авиабазы были атакованы группой слаженно действующих, управляемых по GPS и несущих взрывчатку беспилотных летательных аппаратов в количестве тринадцати единиц. Принципиально важным является тот факт, что ни лица, совершившие это нападение, ни место запуска не были установлены.

23 Помимо применения БАС в сугубо военных целях ДАИШ использовала их в качестве инструментов стратегического воздействия, поскольку кадры, снятые с беспилотных летательных аппаратов, обеспечивали материалом ее хорошо организованную пропагандистскую машину.

24 Внимание широкой общественности к этой проблеме привлекли события, произошедшие в лондонском аэропорту Гатвик в период с 19 по 21 декабря 2018 года: за это время появление БПЛА было зафиксировано 115 раз, что привело к закрытию единственной взлетно-посадочной полосы этого аэропорта. В целом, перебои в его работе привели к отмене более чем 1000 рейсов и затронули около 140 000 пассажиров. С тех пор многие аэропорты повсюду в мире так или иначе сталкивались с помехами их деятельности, вызванными появлением беспилотных летательных аппаратов.



Программный документ 1.

«Исламское государство» и БАС: поставки, масштабы и будущие угрозы — Центр по борьбе с терроризмом в Вест-Пойнте, 2018 год
(<https://ctc.usma.edu/islamic-state-drones-supply-scale-future-threats>)

Цель данного доклада — понять, как группировке ДАИШ удалось за относительно короткий период разработать свою программу применения беспилотных летательных аппаратов и научиться эффективно использовать доработанные коммерческие БАС в качестве оружия. Также в нем освещается более широкая тема угроз и политических последствий применения ДАИШ беспилотных авиационных систем, в том числе то, как «модель», впервые реализованная этой организацией, может оказаться вдохновляющим примером для других субъектов, стремящихся разработать свои собственные средства и стратегии ведения гибридной войны.

- В докладе говорится о том, как страны могут бороться с применением БАС в террористических целях и добиваться снижения их доступности, для чего подробно рассматриваются следующие темы:
- проявление большей должной предусмотрительности при проверке сделок, предусматривающих доставку в районы, обстановка в которых осложнена соседством с зонами боевых действий;
- при отсутствии такой возможности — обращение к правительству или нейтральной третьей стороне, которая могла бы оказать такую помощь;
- взаимодействие с отраслевыми игроками в целях повышения эффективности и совершенствования методов отслеживания или поиска коммерческих БАС и соответствующей упаковки после обнаружения этих устройств и их компонентов в зонах конфликтов;
- привлечение дополнительного внимания и ресурсов к реализации усилий, направленных на предотвращение поставок отдельных товаров двойного назначения в районы, в которых находятся зоны крупных конфликтов;
- изучение и выявление сетей логистических цепочек;
- отслеживание происхождения обнаруженного на местах специфического оборудования, например беспилотных летательных аппаратов, в целях скорейшего перекрытия каналов его поставки.



Программный документ 2.

Как анализировать киберугрозы от применения БАС: исходные данные, рамки анализа и инструменты для проведения анализа — «Рэнд корпорейшн», 2020 год (www.rand.org/pubs/research_reports/RR2972.html)

Данный программный документ предлагает концепцию классификации связанных с применением БАС киберугроз, охватывающую использование БАС в качестве целей кибератак и средств их совершения. Для того чтобы проиллюстрировать спектр существующих угроз, авторы этого доклада классифицируют кибератаки, совершаемые с использованием БАС, используя таксономию под названием «СТРАЙД» (S.T.R.I.D.E.), что расшифровывается следующим образом:

- **искажение информации** (спуфинг) (S: Spoofing): нарушение протоколов контроля на аутентичность, позволяющее злоумышленникам выдавать себя за что-то или кого-то, кем они не являются. В тех случаях, когда целью являются БАС, искажение информации (спуфинг) может выражаться в попытке выдать себя за компьютер, уполномоченный получать данные, передаваемые беспилотным летательным аппаратом;
- **фальсификация** (T: Tampering): нарушение целостности системы путем внесения в нее каких-либо изменений. Например, применение БАС для доставки вредоносного программного обеспечения на целевой компьютер путем приближения на близкое расстояние для получения доступа к незащищенной беспроводной сети;
- **отказ** (R: Repudiation): злоумышленники отказываются брать на себя ответственность за определенное действие. Например, при применении БАС в качестве кибернетического оружия оператор может воспользоваться отказом от ответственности с целью отдалить свою личность от последствий, вмешавшись в работу узла связи, слабо связанного с точкой повреждения или нарушения работы;
- **информация** (I: Information): нарушение принципа конфиденциальности. Например, проникновение в систему данных датчиков БАС для получения доступа к видео, аудио или другим данным;
- **отказ в обслуживании** (D: Denial of service): предполагает, например, заражение программ управления БПЛА с целью сделать устройства невосприимчивыми к командам пользователя;
- **повышение привилегий** (E: Elevation of privilege): нарушение принципа авторизации для выполнения действия. Например, захват БАС путем выдачи себя за законного оператора.





Подверженность уязвимых объектов террористическим нападениям с применением БАС

Страны часто сталкиваются с особым комплексом проблем при обеспечении защиты людей и имущества от угрозы террористических актов с использованием БАС на открытых площадках, где люди массово собираются во время спортивных, религиозных или культурных мероприятий, а также вокруг туристических достопримечательностей и т. д. К числу этих проблем относятся:

- *недостаточно хорошее понимание характера и масштабов угрозы:* угрозы, связанные с БАС, еще не в полной мере учтены в планах обеспечения безопасности на ряде уязвимых объектов, находящихся под открытым небом. Если в планах обеспечения безопасности учитываются только угрозы нападений с земли, воды или из кибернетического пространства, то объект может оказаться незащищенным от вторжений с неба, осуществляемых с применением БАС. Ликвидация одного комплекса уязвимостей может побудить террористов воспользоваться тем, что другая группа слабых мест остается не устраненной.

Во время кризиса существенную трудность для правоохранительных органов и служб безопасности представляет оценка мотивации, стоящей за инцидентом с применением БАС, хотя именно такая информация может повлиять на тип, скорость и формы реагирования. Способность проводить различия между действиями, совершенными по халатности, и действиями, которые совершаются по злому умыслу, может иметь решающее значение для определения масштаба ответных мер, однако скудная доступная информация, противоречивые сообщения и необходи-

мость действовать быстро часто делают эту задачу особенно сложной;

- *несовершенная нормативно-правовая база:* даже там, где соответствующая нормативно-правовая база – в том числе база, призванная обеспечить защиту уязвимых объектов от нападений с применением БАС, – существует, она по большому счету находится на начальном этапе своего становления. Кроме того, этот рынок развивается значительно быстрее, чем применимые к нему нормативные акты. Чтобы найти надлежащий баланс между необходимостью признания/поощрения законного применения БАС и необходимостью обеспечить предотвращение их неправомерной эксплуатации, многим странам предстоит решить ряд важнейших вопросов. Диапазон этих вопросов – от наделения правоохранительных и других государственных органов эффективными и соразмерными полномочиями по противодействию несанкционированному применению БАС до создания надлежащих стимулов для того, чтобы операторы уязвимых объектов усиливали защиту этих объектов от потенциальных атак с применением БАС, в том числе путем формирования государственно-частных партнерств (ГЧП). Некоторым странам, уже сформировавшим нормативно-правовую базу, вероятно, потребуется навести порядок в порой неопределенных или дублирующих друг друга полномочиях, реализуемых в сложной межведомственной среде, а странам, в которых применение БАС практически не регулируется нормативными положениями, необходимо ознакомиться с существующими в этой сфере правовыми рамками и ин-

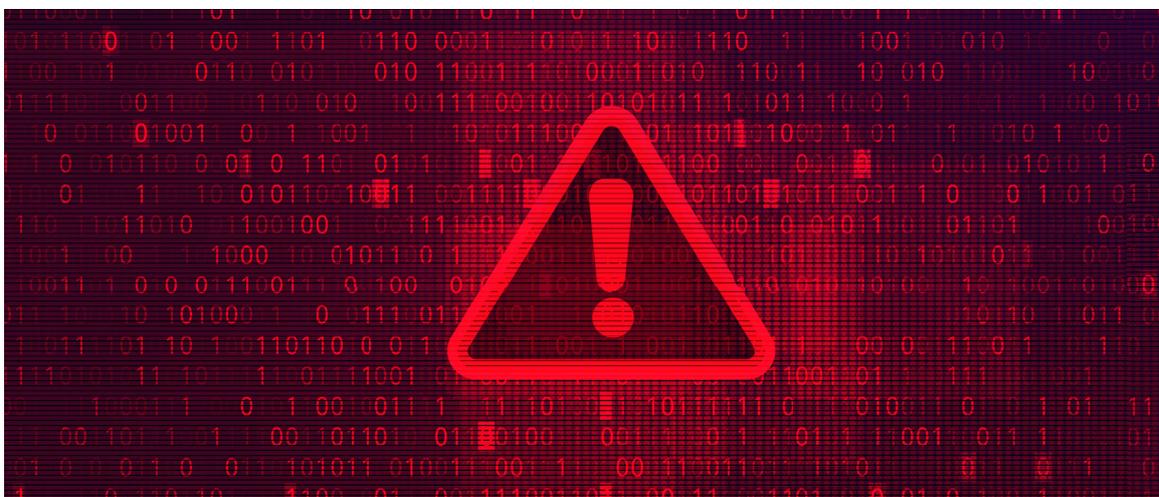
тегрировать их в свою нормативно-правовую базу;

- *недоступность технологий противодействия БАС или трудности применения этих технологий:* технологии противодействия БАС на данный момент не являются инструментами, полностью готовыми к применению. Их нельзя применять без предварительной точной оценки соответствия систем национальному законодательству и индивидуальным характеристикам объекта (объектов), где предполагается их использовать. Кроме того, поскольку технологии, связанные с БАС, развиваются стремительно, технологии противодействия им очень быстро устаревают. Кроме того, сложность этих систем определяет их высокую стоимость, а для их безопасного применения необходимо, чтобы уполномоченные пользователи проходили углубленную предварительную подготовку и были хорошо знакомы с их функциями.

Что касается использования этих технологий для защиты уязвимых целей, то диапазон доступных контрмер может быть существенно ограничен. Например, та или иная технология может представлять собой эффективное и разумное решение против БАС, используемых в террористических целях в отдаленном районе, но при этом быть абсолютно неподходящей для защиты воздушного пространства над аэропортом или местами массового скопления людей. Кроме того, уничтожение БАС, пролетающей над густонаселенным городским районом, или потеря операто-

ром контроля над нею может привести к падению аппарата на землю, что может нанести серьезный ущерб людям и имуществу, в том числе в том случае, если данная БАС будет оснащена оружием, а ее поражение приведет к неконтролируемому взрыву. Кроме того, использование электронных средств борьбы с беспилотными летательными аппаратами в условиях высокой электромагнитной активности — например, в районах городской застройки — может быть ограничено из-за риска создания помех на радиочастотах, обеспечивающих предоставление законных услуг;

- *усталость от БАС:* как подчеркнули составители Берлинского меморандума о передовых методах противодействия применению беспилотных авиационных систем в террористических целях, «многие инциденты с БАС будут являться следствием небрежного, непреднамеренного или неосторожного их применения без террористического умысла. Со временем череда мелких инцидентов с БАС может вызвать у органов власти и общественности ощущение самоуспокоенности. Это, в свою очередь, может привести к тому, что официальные лица и общественность перестанут обращать внимание на факторы уязвимости, сигналы раннего предупреждения, сообщения отдельных лиц или реально существующие угрозы, что повысит уязвимость к реальному нападению» (источник: GCTF 2019, Good Practice 5).





Вставка 3.

Слабые места в информационно-технологической инфраструктуре для БАС

Слабые места могут присутствовать в информационно-технологической инфраструктуре, созданной производителями БАС. Возможности для враждебного вмешательства умножаются, если производители подобных систем предлагают услуги в формате сложной экосистемы, состоящей из нескольких компонентов и сторонних приложений, предназначенных для расширения функциональности продаваемого устройства.

В 2018 году один из ведущих производителей БАС обнаружил уязвимость в своей облачной инфраструктуре. Уязвимость, о которой идет речь, могла позволить злоумышленнику завладеть учетными записями пользователей и получить доступ к частным данным, таким как фотографии и видео, снятые во время полетов БПЛА, информация о личном кабинете пользователя, журналы полетов, включая данные о местоположении. После обнаружения такой уязвимости производитель не только устранил ее, но и пересмотрел подход к организации проверок и аутентификации пользователей в своих ИТ-системах.

Источник: www.wired.com/story/dji-drones-bugs-exposed-users-data/.



Снижение риска и реагирование: роли заинтересованных сторон и передовой опыт

В следующих разделах рассматривается, каким образом отдельные заинтересованные стороны, имеющие отношение к функционированию экосистемы БАС, включая как институциональные, так и неинституциональные субъекты, могут внести свой вклад в снижение риска террористических нападений с использованием БАС и способствовать урегулированию кризисов и усилиям по восстановлению после

них, в том числе путем развития государственно-частных партнерств (ГЧП). В этой отрасли, где ведущую роль играют субъекты частного сектора, создание тесных и долговременных ГЧП имеет решающее значение в связи с особенностями рынков разработки, производства и коммерциализации БАС и технологий противодействия им.



3.1 Государства-члены

3.1.1 Субъекты, определяющие политику

Правительственные учреждения отвечают за создание общей структуры, способствующей: 1) предотвращению инцидентов, связанных с применением БАС, а также с ликвидацией их последствий; 2) быстрому восстановлению и реабилитации объектов и людей, пострадавших в таких инцидентах.

Параллельно с этим государственные органы должны сформировать правовую и институциональную рабочую среду для совместного использования технологий БАС в качестве средств обеспечения защиты уязвимых объектов, подверженных террористическим атакам в целом, одновременно поощряя и защищая права человека.

Для решения этих масштабных задач очень важно, чтобы правительственные субъекты привлекали разнообразные группы, имею-

щие отношение к экосистемам применения БАС (различные сообщества пользователей, производители БАС, поставщики решений в области технологий противодействия БАС, академические и исследовательские учреждения, организации гражданского общества, активисты и т. д.), к разработке политики в этой области на одном или нескольких этапах этого процесса. Их участие играет важную роль в обеспечении того, чтобы результаты регулирования: 1) учитывали ожидания и проблемы широкого круга конечных пользователей; 2) отражали проблемы, существующие в отрасли; 3) принимали во внимание соответствующие – в том числе только возникающие – угрозы, способы и формы осуществления нападений, выявленные исследовательскими организациями, разведывательным сообществом и т. д.; 4) учитывали нужды и потребности гражданского общества в отношении применения БАС для защиты уязвимых объектов.



Программный документ 3.

Берлинский меморандум о передовых методах противодействия применению беспилотных авиационных систем в террористических целях – Глобальный контртеррористический форум (ГКФ), 2019 год

URL: <https://www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fSJ4fl%3d&portalid=1>

Описание передового опыта, содержащееся в Берлинском меморандуме, призвано помочь правительствам в их усилиях по определению, разработке и совершенствованию политики, практических методов, руководящих принципов, правил, программ и методик противодействия использованию БАС в террористических целях. Меморандум обобщает выводы и опыт, которыми поделились правительства, правоохранительные органы, многосторонние организации, частные компании и специалисты в рассматриваемой области в ходе четырех региональных семинаров, проведенных в Германии, Иордании, Республике Корея и Нидерландах в 2018–2019 годах.

- В Берлинском меморандуме выделяется 26 передовых методов в четырех широких областях: оценка риска, оценка факторов уязвимости и повышение уровня осведомленности: действуя совместно с соответствующими заинтересованными сторонами, государства должны включить возможность применения БАС террористами в свои обычные процедуры оценки рисков для выявления факторов уязвимости и пробелов в защите. Государствам следует принимать во внимание все потенциальные способы применения БАС террористами и предугадывать направление развития технологий и другие факторы, которые могут оказать воздействие на эту угрозу, а также реагировать на появление новых и инновационных способов применения технологий, связанных с БАС, террористами;



- *расширение обмена информацией, взаимодействие с соответствующими заинтересованными сторонами и просвещение общественности:* многоаспектная угроза применения БАС террористами требует всеобъемлющего и скоординированного подхода, предполагающего участие государств, региональных и международных правительственных организаций, а также нетрадиционных заинтересованных сторон. Усилия по противодействию угрозе использования БАС террористами, принимаемые на национальном уровне, должны по мере необходимости дополняться соответствующими региональными и международными мерами. Кроме того, государства должны взаимодействовать с широкой общественностью, распространяя знания по вопросам ответственного использования БАС и надлежащего реагирования на подозрительные БАС;
- *осуществление стратегий и нормативных актов и планирование на случай кризисных ситуаций:* государства должны иметь четкие и обязательные к исполнению стратегии и нормативные акты, направленные на сдерживание и минимизацию потенциала распространения и неправомерного использования БАС террористами и другими злоумышленниками и позволяющие принимать эффективные контрмеры в связи с использованием БАС, а также проводить эффективные расследования, осуществлять судебное преследование и применять санкции после инцидентов с БАС. Правительствам следует также разрабатывать стратегии кризисного регулирования и уменьшения последствий, чтобы адекватно реагировать на инциденты с БАС;
- *разработка тактических контрмер и технических решений:* государствам следует внедрять и регулярно пересматривать меры защиты и другие технические решения, в том числе в плане необходимого оснащения и подготовки соответствующих органов, чтобы они могли выявлять случаи злоумышленного запуска БАС и противодействовать им. Прежде чем применять контрмеры, государства должны, действуя совместно с соответствующими заинтересованными сторонами, оценить и уменьшить негативные последствия этих контрмер, принимая во внимание тот факт, что они могут оказаться ресурсоемкими, а соответствующему персоналу потребуются значительная подготовка.



Программный документ 4.

Инструментарий по БАС – Международная организация гражданской авиации (ИКАО) (www.icao.int/safety/UA/UASToolkit/Pages/default.aspx)

Разработанный как веб-инициатива в сотрудничестве с предприятиями отрасли и сетью международных партнеров-экспертов ИКАО, данный инструментарий обобщает передовую практику и нормативные акты с целью поддержать усилия государств-членов по разработке эффективного оперативного руководства по использованию БАС. Среди прочего, инструментарий дает доступ к действующим в разных странах мира нормативным положениям; ресурсам, содержащим информацию по техническим и эксплуатационным вопросам, в том числе по тематике подготовки и обучения операторов БАС; и материалам, необходимым для проведения информационно-просветительских кампаний в странах.



3.1.1.1 Стратегии противодействия БАС

Борьба с угрозой применения БАС в террористических целях является обязанностью широкого круга заинтересованных сторон и требует координации и единства цели. Одна из основных задач правительств – инициировать, возглавлять и поддерживать такую координацию, четко формулируя общую концепцию и подходы, которые должны применяться странами в рамках всех мер по защите общества от использования БАС в террористических целях. В первую очередь это подразумевает определение каналов, используя которые различные ведомства с регуляторными и/или оперативными полномочиями и обязанностями относительно БАС должны объединить усилия и синхронизировать свои действия, а также выявление соответствующих видов и форм государственно-частного партнерства (например, платформы обмена информацией с отраслью,

программы повышения осведомленности операторов объектов и т. д.)²⁵.

Угроза, создаваемая применением БАС в террористических целях, может быть учтена и рассмотрена в специальных стратегиях противодействия БАС²⁶ или в рамках более широких стратегий борьбы с терроризмом и стратегий национальной безопасности, включая стратегии, направленные на защиту уязвимых объектов и общественных мест. При использовании нескольких документов и институциональных рамок важно, чтобы различные части этой мозаики складывались в единое целое в плане общей концептуальной основы, подходов, процедур и ожиданий²⁷. Наконец, некоторые страны могут решить интегрировать подход к предотвращению угроз, связанных с применением БАС, и противодействию им в комплексную стратегию, направленную на стимулирование развития безопасных, генерирующих рост

25 В Техническом руководстве по резолюции 2370 СБ ООН также подчеркивается необходимость комплексного, общегосударственного подхода к противодействию приобретению БАС и их применению террористами и особо оговаривается необходимость проведения регулярных обзоров в рамках всеохватного процесса с участием многих заинтересованных сторон. Cf. Submodule II, "Counter-UAS policy and strategy" (2.1.1.).

26 Соединенное Королевство последовало этому подходу и разработало специальную стратегию противодействия БАС (UK 2019).

27 Некоторые страны могут разрабатывать стратегии противодействия БАС на уровне отдельных правительственных ведомств. Например, Министерство обороны США при разработке специализированной стратегии (USA 2021) исходило из того, что малые БАС с каждым днем представляют все более серьезную опасность для его операций, персонала и объектов, вне зависимости от того, кем создаются эти опасности – государственными или негосударственными субъектами. Очевидно, что подобная стратегия, разработанная для конкретного агентства, должна быть вписана в более широкие государственные концепции управления угрозами, связанными с применением БАС.

и общественно полезных отраслей экономики, в которых применяются БАС²⁸.

Что касается процедуры, то странам, приступающим к разработке стратегии противодействия БАС, рекомендуется организовать проведение общегосударственных консультаций с целью выработать предметный стратегический документ высокого уровня.

В такой общенациональной стратегии должны быть учтены, в частности, следующие вопросы первостепенной важности:

- *связь между гражданским и военным секторами*: важнейшим аспектом моделей межведомственной координации является сотрудничество между гражданским и военным секторами. В этой связи в Берлинском меморандуме странам рекомендуется «принять во внимание опыт и уроки, полученные национальными силами обороны, поскольку многие военные ведомства уже имеют опыт противодействия использованию БАС агрессивными негосударственными субъектами во время вооруженных

конфликтов»²⁹ (источник: GCTF 2019, Good Practice 11);

- *координация между органами управления, деятельность которых связана с авиационной отраслью*: любая государственная стратегия должна способствовать установлению тесной коммуникации и формированию каналов обмена информацией между органами гражданской авиации, поставщиками услуг в области аэронавигационного обслуживания и ведомствами, отвечающими за авиационную безопасность. Для обеспечения предметности и актуальности нормативной базы, касающейся БАС, необходимо как минимум налаженное взаимодействие между этими ведомствами. Кроме того, как подчеркивается в Берлинском меморандуме, «учитывая, что применение контрмер может вызывать непредвиденные последствия, особенно в плане безопасности гражданской авиации и радиочастотных (коммуникационных) систем, наиболее эффективно способствовать смягчению этих последствий могут ор-



28 Например, канадская стратегия в отношении беспилотных летательных аппаратов содержит четко сформулированный компонент обеспечения безопасности. Этот документ, принятый в 2021 году, отражает стратегическую концепцию Канады в отношении БАС, особое внимание в которой уделяется повышению осведомленности о значении БАС и изложению первоочередных стратегических целей, достичь которых предполагается до 2025 года (Canada 2021).

29 Однако в Берлинском меморандуме отмечается, что «не все извлеченные уроки можно перенести с театров военных действий на стратегию противодействия БАС в условиях, сложившихся в странах, не затрагиваемых вооруженными конфликтами. Действительно, многие системы были разработаны для применения на поле боя, и их использование во внутреннем воздушном пространстве над населенными пунктами не представляется приемлемым».

ганы гражданской авиации и поставщики услуг в области аэронавигационного обслуживания» (GCTF 2019, Good Practice 13). Они могут также «внести ценный вклад на раннем этапе применения контрмер в отношении их последствий для авиационной безопасности и авиаперевозок»;

- *привлечение операторов уязвимых объектов*: правительствам необходимо определить, какого рода государственные программы и инициативы следует осуществлять для оказания поддержки операторам в их усилиях по повышению устойчивости их объектов к террористическим нападениям с применением

БАС. В зависимости от наличия бюджетных средств возможно применение различного рода стимулов, в том числе грантов, планов финансирования, налоговых льгот и т. д. Правительства могут также поддерживать операторов объектов, обеспечивая их доступ к имеющимся экспертным знаниям, например за счет организации оказания им специализированной консультационной помощи по вопросам управления рисками и регулирования кризисов компетентными подразделениями национальных органов безопасности или правоохранительных органов;



Вставка 4.

Рекомендация ИКАО в отношении общегосударственной стратегии по БАС

Учитывая сложность этого вопроса и большое число государственных структур, вовлеченных в его решение, в разработанном ИКАО инструментарии по БАС рекомендуется применение подхода, при котором государства разрабатывают общегосударственную стратегию по БАС, направленную на достижение следующих целей:

- разработка плана действий, в котором перед будущей индустрией БАС поставлены задачи в сфере безопасности и экономические задачи;
- создание государственного межведомственного комитета по БАС для обмена информацией и оказания помощи ведомствам, эксплуатирующим БАС, в планировании их деятельности;
- разработка методологии приведения потребностей этой отрасли в соответствие с имеющимися у государства ресурсами;
- координация деятельности по расширению доступа заинтересованных сторон данной отрасли к финансированию в целях изучения новых технологий и возможностей их коммерческого применения.

Источник: <https://www.icao.int/safety/UA/UASToolkit/Pages/default.aspx>.

Кроме того, при принятии мер по защите инфраструктуры гражданской авиации от актов незаконного вмешательства, совершаемых с применением беспилотных летательных аппаратов, государствам рекомендуется также принимать во внимание меры, описанные в Руководстве ИКАО по авиационной безопасности (Chapter 19 – Protection of civil aviation infrastructure against unmanned aircraft) (Doc 8973, Restricted).



Конкретный пример 1.

Стратегия Европейского союза по противодействию БАС в контексте борьбы с терроризмом

Нынешний подход ЕС предусматривает комплексную межведомственную и межсекторальную работу с участием различных учреждений и агентств ЕС, сетей правоохранительных и оборонных органов, а также финансируемых консорциумов. Результатом их деятельности и инициатив стало формирование быстро эволюционирующих правовых, стратегических и институциональных рамок, основными компонентами которых являются:

- «Стратегия ЕС в области безопасности 2020 года» и обновленная «Повестка дня в области борьбы с терроризмом (2020 год)»;
- нормативная база ЕС по безопасной эксплуатации БАС, закреплённая в регламентах 2019/945 и 2019/947;
- продолжающаяся работа по созданию пакета мер ЕС по организации движения беспилотных летательных аппаратов U-Space;
- план действий по координации деятельности структур гражданской обороны и отраслей космической промышленности (2021 год);
- реализуемые под руководством Объединенного исследовательского центра Комиссии Европейского союза инициативы по физической защите от БАС, включая защиту объектов критически важной инфраструктуры;
- руководство ЕС по обеспечению безопасности городских территорий от БАС, принадлежащих сторонам, отказывающимся от сотрудничества (в настоящее время находится на этапе проведения адресных консультаций, опубликование запланировано на конец 2021 года).

Источник: совещание Группы экспертов, организованное КТУ ООН (29 июня 2021 года).



Конкретный пример 2.

Стратегия Соединенного Королевства по противодействию применению беспилотных летательных аппаратов

Предполагается, что эта стратегия, разработанная как перспективный документ, будет развиваться вместе с основными технологиями, чтобы опережать появление угроз, связанных с применением БАС. В ней изложены действия, которые правительство планирует предпринимать для противодействия злонамеренному использованию малых БАС³⁰ и снижения риска, связанного с их незаконным использованием, наносящим наибольший вред, ориентируясь на следующие четыре задачи стратегического характера:

1. формирование всестороннего понимания эволюции рисков, связанных со злонамеренным и незаконным использованием БАС;
2. применение комплексного подхода к сдерживанию, выявлению и пресечению неправомерного использования БАС;
3. установление прочных отношений с отраслевыми производителями для обеспечения соответствия их продукции самым высоким стандартам безопасности;
4. расширение возможностей полиции и других подразделений реагирования за счет доступа к технологиям борьбы с беспилотными летательными аппаратами, действующему законодательству и возможностям прохождения подготовки и инструктажа.

Эта стратегия разработана в качестве дополнения к стратегиям Соединенного Королевства в области противодействия терроризму и в области борьбы с тяжкими преступлениями и организованной преступностью.

Источник: United Kingdom, 2019.



³⁰ Управление гражданской авиации Соединенного Королевства относит к категории «малых» БАС, весящие менее 20 кг. Разработчики указанной стратегии решили ограничить сферу ее применения малыми БАС ввиду того, что приобретение и эксплуатация более тяжелых БАС существенно ограничены.



Конкретный пример 3.

Подход Сингапура к рискам для безопасности, связанным с БАС

Хотя в Сингапуре не было случаев прямых вооруженных нападений с применением беспилотных летательных аппаратов, власти страны признают, что проникновение БАС может нести с собой и другие риски – например, угрозу безопасности при их появлении в местах проведения массовых мероприятий с присутствием большого количества людей. Кроме того, появление беспилотных летательных аппаратов в июне 2019 года в районе аэропорта Чанги привело к временному ограничению использования взлетно-посадочной полосы, что вызвало задержки рейсов и изменение их маршрутов.

В целом подход Сингапура направлен на балансирование рисков для безопасности/защищенности и возможностей законного использования БАС и опирается на три основных компонента:

- **регулирование:** в 2015 году парламент Сингапура принял Закон о беспилотных летательных аппаратах (общественная безопасность и защищенность), регулирующий применение БПЛА, а в 2019 году – Закон о воздушной навигации (поправка) с целью усилить контроль над их применением. Эти законодательные акты основаны на трех основных принципах: i) для осуществления полетов беспилотных летательных аппаратов в определенных условиях требуется разрешение (например, полеты в пределах 5 км от гражданского/военного аэродрома, или полеты в охраняемой/ограниченной по доступу/опасной зоне, или полеты на высоте более 200 футов (около 60 м) над уровнем моря); ii) запрещается использование БПЛА, представляющее опасность (например, сброс с БАС каких бы то ни было предметов и веществ); iii) БАС, вес которых превышает 250 г, подлежат регистрации.

Применимые санкции соизмеримы с последствиями, вызванными незаконным применением БАС (например, для лиц, впервые совершивших полет над охраняемыми районами без разрешений, предусмотрено наказание в виде штрафа в размере до 50 000 долларов США и/или лишения свободы на срок до 2 лет);

- **правоприменение:** органы власти реагируют на несоблюдение нормативных требований, проводят расследования и привлекают к ответственности;
- **просвещение:** активно осуществляются стратегии просвещения населения, направленные на поощрение ответственного использования БАС и повышение осведомленности о правилах применения БПЛА.

Источник: выступление г-на Ли Пенг Янга, старшего помощника директора Объединенной оперативной группы Министерства внутренних дел Сингапура на совещании Группы экспертов, проводившемся КТУ ООН (6 и 7 октября 2021 года).

3.1.1.2 Общая правовая основа использования БАС

Защита уязвимых целей от террористических нападений с использованием БАС требует, прежде всего, создания государствами-членами общей правовой базы, обеспечивающей проведение различия между законными/безопасными и незаконными/небезопасными способами применения БАС. Несмотря на то, что страны применяют различные подходы к регули-

рованию использования БАС на своей территории, приоритетом для большинства из них является принцип «безопасность превыше всего». Обычно реализация этого принципа предусматривает введение различного рода требований, в частности требований, касающихся выдачи летных свидетельств, регистрации летательных аппаратов, страхования и создания бесполетных зон (как правило, вокруг объектов критически важной инфраструктуры).

Хотя во многих странах эти требования обязательны только для коммерческих БАС, в некоторых юрисдикциях регистрировать теперь необходимо и малые БАС, используемые в развлекательных целях³¹.

ИКАО рекомендует государствам при разработке тех или иных частей своих нормативных рамок «проводить консультации с основными заинтересованными сторонами на ранних этапах процесса разработки нормативных положений. Эффективным решением в этой связи может быть создание совместной рабочей группы в составе представителей правительства и заинтересованных сторон для проведения обзора действующего законодательства и выработки рекомендаций в отношении

новых правил эксплуатации БАС. В число заинтересованных сторон в вопросах, касающихся БАС, следует включать эксплуатантов, производителей и организации пилотируемой авиации. После подготовки проектов новых правил важно запросить мнение о них заинтересованных сторон — как связанных, так и не связанных с авиационной отраслью, — с тем чтобы обеспечить, что в них охвачены все необходимые требования»³². Очень важно, чтобы законодательство, касающееся беспилотных летательных аппаратов, не отставало от темпов эволюции угроз, учитывало практический опыт эксплуатации и косвенно служило основой для подготовки и оказания консультационной помощи³³.



Вставка 5.

Управление движением беспилотных авиационных систем (УДБ)

Существующие системы организации воздушного движения не позволяют успешно регулировать движение с участием все большего числа самых разнообразных БАС, движущихся по самым разнообразным маршрутам. По этой причине важным аспектом регулирования эксплуатации БАС станет создание систем управления движением БАС (УДБ), которые позволят обеспечить контроль за маршрутами движения низковысотных БАС, определять зон ограниченного воздушного движения и выборочно предоставлять или не предоставлять доступ к зонам ограничения полетов³⁴.



31 В Техническом руководстве по резолюции 2370 СБ ООН говорится о необходимости создания надлежащей законодательной и нормативной базы для предотвращения и смягчения угроз, возникающих в результате приобретения/применения БАС террористами, и описываются некоторые трудности в этой области. Cf. Submodule II, “National legislation and regulations” (2.1.3).

32 Источник: инструментарий ИКАО (URL: <https://www.icao.int/safety/UA/UASToolkit/Pages/default.aspx>).

33 См. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840789/Counter-Unmanned_Aircraft_Strategy_Web_Accessible.pdf.

34 В зависимости от способа применения системы УДБ могут быть стационарными или мобильными. Стационарные УДБ будут обеспечивать непрерывное покрытие таких зон, как интенсивно используемое низковысотное воздушное пространство над крупными районами застройки городского типа. Мобильные образцы будут больше адаптированы к транспортировке в определенные места по случаю конкретных событий (например, на место скопления людей или в район, пострадавший от стихийного бедствия).

Что касается безопасности, то разработка и развертывание систем УДБ также могут помочь властям фиксировать законно используемые БАС и выявлять БАС, которые применяются незаконно или злонамеренно. Такие системы могут стать источником важнейшей информации в ходе принятия мер реагирования на тот или иной инцидент³⁵.

Однако, поскольку страны все чаще разрабатывают нормативно-правовую базу и стратегии ее реализации независимо друг от друга, потенциально проблемой может стать появление нескольких нескоординированных и несовместимых систем УДБ.

Это, в свою очередь, может привести к утечке чувствительной информации гражданского характера или государственной информации в результате несовместимости систем УДБ. Кроме того, для выявления несоответствующих устройств в конкретных местах и на определенных мероприятиях по-прежнему будут необходимы технологии обнаружения БАС (см. раздел 3.1.2.2). Вопросы совместимости технологий обнаружения БАС и систем УДБ могут приобрести в будущем особую важность.



Конкретный пример 4. Нормативно-правовая база ЕС по БАС

В 2019 году ЕС представил нормативную базу, призванную стимулировать получение экономических и социальных выгод от применения БАС, но при этом наложил на их производителей и операторов ряд ограничений по соображениям безопасности и общественной безопасности, защиты персональных данных, уважения к неприкосновенности частной жизни, охраны окружающей среды и защиты от шума. В рамках применяемого подхода, основанного на оценке рисков, в регламентах Европейского союза 2019/947 и 2019/945 не проводится различий между применением БАС в развлекательных и в коммерческих целях. Вместо этого в них берется в расчет вес системы и ее целевое предназначение. Согласно этой концепции, применение той или иной БАС, в зависимости от оцениваемого уровня риска, может быть отнесено к «открытой», «особой» или «сертификационной» категории: (4V).

- открытая категория: применение, несущее наименьший риск. Получать разрешение перед началом полета не требуется;
- особая категория: до начала эксплуатации оператору БПЛА необходимо получить разрешение на эксплуатацию от национального компетентного органа. Для получения такого разрешения оператор обязан оценить риски для безопасности, после чего на основании этой оценки будут сформулированы требования к безопасному применению данного беспилотного летательного аппарата;
- сертификационная категория: риск с точки зрения безопасности считается самым высоким, что подразумевает обязательную сертификацию оператора БПЛА и самого аппарата, а также получение лицензии пилотами данных аппаратов.

Источник: регламенты ЕС 2019/947 и 2019/945.

35 С этой целью ИКАО разработала методический материал по системам УДБ, который можно найти по адресу: <https://www.icao.int/safety/UA/Pages/UTM-Guidance.aspx>



Конкретный пример 5.

Система управления рисками, принятая в Объединенных Арабских Эмиратах в отношении воздушных судов, несанкционированно проникающих в контролируемое воздушное пространство

В ноябре 2016 года Управление гражданской авиации Объединенных Арабских Эмиратов (ОАЭ) ввело «меры реагирования в отношении летательных аппаратов, несанкционированно проникающих в контролируемое воздушное пространство» (решение по безопасности 2016-16). В этом подзаконном акте содержатся указания для поставщиков услуг в области аэронавигационного обслуживания по тактической оценке риска, сопряженного с конкретным вторжением в контролируемое воздушное пространство, и принятию мер по уменьшению его последствий при гарантированной соразмерности этих мер той угрозе, которую создает нарушитель.

В основе этих регулятивных рамок лежат следующие концептуальные блоки процессуальных действий:

- создание, внедрение и поддержание системы управления безопасностью полетов в подразделениях обслуживания воздушного движения;
- оценка тактического риска для определения соответствующих действий, которые необходимо предпринять в случае незаконного вторжения в воздушное пространство.

Полный текст решения по безопасности 2016–16 доступен в виде документа, представленного ОАЭ на Тринадцатой Аэронавигационной конференции ИКАО.

URL: https://www.icao.int/Meetings/anconf13/Documents/WP/wp_097_en.pdf





METEOROLOGY
DRONES



DRONE
DELIVERY



DRONE FLYING
REGULATIONS



Программный документ 5.

Типовые правила ИКАО в отношении БАС

(www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx)

Типовые правила ИКАО разработаны как подспорье для стран в создании и совершенствовании ими национальных руководств по эксплуатации БАС на своей территории. Они были сформулированы по итогам анализа ИКАО нормативных актов, регулирующих применение БАС в разных странах мира, — анализа, который был проведен с целью выявить общие признаки и передовые наработки, соответствующие требованиям ИКАО к ведению деятельности в авиационной отрасли.

Типовые правила в отношении БАС можно скачать с веб-сайта ИКАО; из планируется регулярно обновлять, чтобы они не отставали от эволюции и расширения национальных программ в области применения БАС. Страны могут принять типовые правила в полном объеме или выбрать положения, дополняющие существующие национальные правовые рамки. Действующие в настоящее время правила охватывают основные моменты, необходимые странам для организации сертификации БАС и их безопасной эксплуатации.

3.1.1.3 Поддержка разработки и соразмерного применения технологий противодействия беспилотным авиационным системам

Правительства несут общую ответственность за создание благоприятных условий для развития и надлежащего использования технологий противодействия БАС, в том числе для защиты уязвимых объектов от террористических нападений с применением БАС³⁶. В целом для целей разработ-

ки политики целесообразно рассмотреть по меньшей мере следующие три группы вопросов, касающихся применения технологий противодействия БАС для защиты уязвимых объектов:

- какие государственные/правоохранительные органы уполномочены прибегать к применению технологий противодействия БАС и на основании каких правовых гарантий и требований?³⁷ Доверяя определенным национальным органам прерогативы применения тех-

36 Резолюция 2370 Технического руководства содержит вводные положения и обзор технологий противодействия БАС, а также информация о задачах и проблемах, существующих в этой области. Cf. Submodule II, "Counter-UAS systems and techniques" (3.1). Cf. also Submodule II, "Capability, normative, and operational development for countering UAS" (2.2.), and "Further development of UAS countermeasures" (3.8.).

37 В настоящее время страны по-разному решают этот вопрос. Некоторые из них включили в свое законодательство положения о полномочиях в области применения технологий противодействия БАС, хотя иногда эти положения являются фрагментарными и сложными; другие же не предусмотрели никаких специальных положений.

нологий противодействия БАС, правительства должны сформулировать условия, обеспечивающие соразмерное и основанное на соблюдении прав человека применение таких технологий. Например, в соответствующие законодательные акты должны быть включены основные процедурные и доказательственные стандарты — такие как необходимость доказать наличие достаточных основания для подозрения или аналогичные требования, — прежде чем органам охраны правопорядка будет разрешено предпринимать действия, направленные на уничтожение БАС, создающих угрозу. В стратегиях противодействия БАС также можно рассмотреть вопрос о том, в какой степени действиям правоохранительных органов, направленным на уничтожение БАС, должно предшествовать предупреждение или уведомление, предоставляющее оператору данной БАС разумную возможность предпринять корректирующие действия (например, изменить направление движения аппарата, приземлить его за пределами периметра безопасности и т. д.);

- поскольку технологии противодействия БАС часто не являются инструментами, готовыми к применению, и требуют наличия существенных технических навыков и соответствующей подготовки,

в нормативной базе можно предусмотреть требование о том, что до приобретения/использования этих технологий компетентные органы обязаны пройти соответствующее тестирование в целях обеспечения безопасного и компетентного применения таких средств;

- каким образом государственные органы намерены взаимодействовать с отраслевыми заинтересованными сторонами, отвечающими за разработку технологий противодействия БАС? Такое взаимодействие должно быть широким по охвату и направленным, как минимум, на то, чтобы технологии, которые в конечном итоге будут интегрированы в устройства, призванные противодействовать применению БАС, в обязательном порядке соответствовали положениям нормативных актов и содержащимся в них ограничениям. В зависимости от наличия бюджетных средств, действующих правил, регулирующих конкуренцию, и иных факторов правительствам следует также выработать стратегию финансирования научных и технологических разработок в области технологий противодействия БАС, обеспечив среди прочего малым компаниям и стартапам возможность получать поддержку для разработки инновационных решений³⁸.



Конкретный пример б.

Методология выбора правильной технологии противодействия БАС: проект «Отважный»

В основе проекта «Отважный», реализуемого исследовательским подразделением Бельгийской королевской военной академии³⁹ — лабораторией «Робототехника и автономные системы», — лежит тот факт, что «по мере повышения доступности беспилотных авиационных систем правоохранительным органам приходится активно решать новую задачу по обеспечению полицейского надзора за доступом в воздушное



38 Например, стратегия Великобритании по противодействию беспилотным летательным аппаратам предусматривает выстраивание с производителями технологий противодействия БАС прочных партнерских отношений, направленных среди прочего на создание единого государственного каталога утвержденных на национальном уровне возможностей по противодействию БПЛА. Предполагается, что этот каталог, в свою очередь, будет доступен партнерам, что поможет им принимать эффективные решения о закупках (UK Counter-Unmanned Aircraft Strategy, p.24).

39 При поддержке Европейской комиссии.

пространство на малых высотах. Коммерческие поставщики уже разработали широкий спектр решений в этой области, но оценка возможностей этих систем представляется затруднительной. В результате конечные пользователи с большим трудом подбирают нужные средства для конкретных вариантов применения в тех случаях, с которыми они сталкиваются». Например, в 2019 году для приобретения были доступны более 100 коммерческих систем противодействия БАС, причем заявления об их эффективности часто не были подкреплены доказательствами, а различные методики испытаний чрезвычайно затрудняют их сравнение. Проект «Отважный» направлен на решение этих проблем путем разработки стандартизированной методики испытаний систем обнаружения БАС, слежения за ними и их идентификации. Эта методика основана на серии стандартных сценариев, формулируемых пользователем (например, обеспечение безопасности тюрем и аэропортов, защита критически важной инфраструктуры, обеспечение охраны границ, борьба с наркотиками и торговлей людьми). Для этих сценариев конечные пользователи проекта «Отважный» формулируют свои оперативные потребности и требования к функциональным характеристикам. На основе этой информации будет разработана методика проведения комплексных испытаний, позволяющая проводить качественное и количественное сравнение между различными системами противодействия БАС. Методика проведения испытаний будет проверена в ходе трех валидационных испытаний по сценариям пользователей.

Источники:

URL: <https://mecatron.rma.ac.be/index.php/projects/isf-courageous/>

Выступление Геерта де Куббера, Королевская военная академия, Бельгия, на организованном КТУ ООН совещании Группы экспертов (6–7 октября 2021 года)



Конкретный пример 7.

Программа финансирования «Акселератор обороны и безопасности» – Соединенное Королевство

В 2020 году в рамках межведомственной инициативы Министерства обороны Великобритании «Акселератор обороны и безопасности» был объявлен конкурс на финансирование предложений по разработке технологий противодействия БАС и их интеграции в целях формирования дееспособной системы. Все предложения должны были демонстрировать возможность перспективной доработки представленных технологий для их встраивания в систему оперативного противодействия угрозам, создаваемым малыми коммерческими, самодельными или военными БАС, а также включать доказательства того, что:

- в них применяется инновационный подход к разработке;
- они явно превосходят уже существующие технологии противодействия БАС;
- соответствующие технологии можно интегрировать, чтобы они образовали готовые решения;
- разработка может применяться на практике.

Источник: <https://www.gov.uk/government/organisations/defence-and-security-accelerator>.



3.1.1.4 Просвещение и повышение осведомленности

Значительная часть конечных пользователей БАС, в особенности те, кто использует эти системы в развлекательных целях, не демонстрирует стремления ознакомиться с соответствующими актуальными законами и соблюдать стандарты безопасности. Таким образом, важная роль органов государственной власти заключается в том, чтобы (зачастую) технически сложные нормативно-правовые акты в области охраны и безопасности были непременно доведены до сведения этих пользователей и стали для них понятными.

Любая программа повышения информированности должна учитывать неоднородность членов сообщества пользователей БАС по таким параметрам, как возраст, пол, мотивация, уровень образования. Основная информация может передаваться с помощью различных средств и методов, в том числе через онлайн-платформы поставщиков, социальные сети, листовки и инструкции по применению, которые производители БАС поставляют вместе со своей продукцией, а также в ходе проведения обязательных или добровольных мероприятий по обучению и повышению осведомленности операторов БАС⁴⁰.



Конкретный пример 8. Ресурсный центр «Безопасность БПЛА»

«Безопасность БПЛА» — это ресурсный центр, финансируемый правительством Канады. Он предоставляет информационные и учебные материалы для операторов беспилотных летательных аппаратов, начиная от описания порядка регистрации БПЛА, и заканчивая получением сертификата пилота. Имеющаяся онлайн-форма позволяет пользователям сообщить об инциденте с БПЛА.

Источник: <https://tc.canada.ca/en/aviation/drone-safety>.

⁴⁰ Правительства могут также рассмотреть возможность опубликования материалов, посвященных беспилотным летательным аппаратам, и использования средств массовой информации в качестве каналов для повышения осведомленности пользователей о вопросах обеспечения безопасности, как это предусмотрено в Стратегии Соединенного Королевства по борьбе с беспилотными летательными аппаратами. В той же Стратегии также планируется «поощрять общественность сообщать о случаях неправомерного использования беспилотных летательных аппаратов, а в рамках более широких кампаний по поощрению бдительности приравнивать подозрительное применение БПЛА к другим видам террористической или преступной деятельности. Если мы будем лучше освещать случаи уголовного преследования за преступления, связанные с применением БПЛА, мы шире распространим эти знания и снизим вероятность того, что лица, преследуемые по закону за такие деяния, смогут заявить о своей неосведомленности» (УК 2019, р. 21).



Программный документ 6.

Работа с общественностью: просвещение и улучшение осведомленности – инструментарий ИКАО (www.icao.int/safety/UA/UASToolkit/Pages/Narrative-Considerations.aspx)

Для обеспечения успешной интеграции БАС в существующую систему пилотируемой авиации крайне важно, чтобы пилоты, операторы, производители, покупатели, продавцы, импортеры и широкая общественность были осведомлены о применении БАС. Самое главное, пилот, управляющий летательным аппаратом в удаленном режиме, должен осознавать свою ответственность и понимать, что он отвечает за безопасность эксплуатации БАС. В информационные кампании могут быть включены слоганы, подчеркивающие ответственность лиц, осуществляющих дистанционное пилотирование БАС, за управление ими. Частью информационного заполнения кампании также должно являться напоминание о риске с точки зрения безопасности, который может представлять пилотирование БАС вблизи аэропорта или самолета.

Просвещение

Необходимо повышать уровень информированности производителей, импортеров и продавцов беспилотных авиационных систем, чтобы они могли донести ключевую информацию о безопасности непосредственно до покупателей БАС. Такая работа по улучшению осведомленности должна включать в себя следующие элементы:

- предоставление по легко доступным ссылкам онлайн-справочника, содержащего руководство или правила в отношении БАС, применяемые в конкретном государстве;
- размещение на веб-сайте простой и понятной памятки о том, что следует делать при эксплуатации БАС и чего делать не следует;
- распространение брошюр или учебных материалов касающихся руководства и/или правил, среди производителей, дилеров и продавцов БАС, изготовителей некоторых «самодельных» беспилотных летательных аппаратов, собранных в развлекательных или экспериментальных целях, среди сотрудников правоохранительных органов и научных учреждений.

Кампании по вопросам безопасности

Эффективными могут быть информационные стенды на конференциях, авиасалонах и торговых выставках. Рассмотрите возможность использования проходящих мероприятий в качестве платформ для повышения осведомленности о БАС.



Программный документ 6. (продолжение)

Ниже перечислены другие организации, которые могут сыграть свою роль в просвещении и повышении осведомленности. Пользуясь услугами этих организаций, можно распространять информацию во всем мире.

- Иммиграционные службы, включая их рекомендации в отношении поездок
- Туристические бюро
- Социальные сети, включая часто обновляемые веб-страницы, такие как YouTube, и блоги
- Для информирования широкой общественности и операторов БАС можно использовать веб-сайты и справочник, разъясняющий вопросы регулирования, листовки, кампании в средствах массовой информации
- При наличии составленных Управлением гражданской авиации списков рассылки зарегистрированных операторов также можно информировать по электронной почте
- Полезной может оказаться страница часто задаваемых вопросов, предусматривающая функцию отправления ответов на вопросы по электронной почте
- Онлайн-средства информирования о ситуации и планирования полетов
- Кампании по вопросам безопасности, проводимые регулирующими органами в рамках их государственной программы повышения уровня безопасности в авиации и информированности об этой отрасли

3.1.1.5 Межправительственное сотрудничество

Любая всеобъемлющая национальная стратегия, направленная на защиту гражданских объектов, в том числе наиболее уязвимых, от БАС, используемых в террористических целях, должна предусматривать ответы на следующие вопросы:

- как в такой национальной стратегии можно использовать опыт, накопленный другими странами, в том числе в отношении поощрения и защиты прав человека и основных свобод?
- как информация о достижениях данной страны в понимании/смягчении угроз, связанных с применением БАС, и урегулировании соответствующих кризисов может быть с пользой распространена среди более широкой аудитории?
- как поддерживать следственные действия и уголовные расследования, осуществляемые в зарубежных странах по факту совершения террористических актов с применением БАС или подготовки к их совершению, при наличии транснациональной составляющей в этих действиях, обеспечивая при

этом соблюдение прав человека пострадавших?

- как обеспечить соответствие национальной стратегии принципам верховенства права и соблюдения прав человека?

Достижение указанных целей требует от стран активного взаимодействия с их зарубежными партнерами в рамках двусторонних, региональных и/или многосторонних форумов и механизмов. Возможности для совместной деятельности чрезвычайно широки⁴¹ и включают в себя следующие направления:

- согласование определений и классификаций систем БАС, инцидентов, связанных с их применением, и стандартов тестирования мер противодействия БАС. Формирование общей терминологической базы и рабочих стандартов поможет обеспечить составление сопоставимых на международном уровне статистических данных и, следовательно, будет способствовать проведению сравнения между странами (например, в отношении оценки степени угрозы, эффективности контрмер, наличия пробелов в практике и стратегиях и т. д.) (GCTF, Good Practice 8);

41 Cf. UNSCR 2370 Technical Guidance document, "International and regional cooperation including information-sharing" (2.5).

- создание механизмов обмена опытом между национальными органами управления в авиационной отрасли для согласования соответствующих нормативных актов, в первую очередь между соседними странами;
- возможное принятие — посредством многосторонних инициатив, которые будут реализовываться в рамках ВТамО, — специальной таможенной классификации для БАС, призванной повысить эффективность выявления подозрительных поставок таких систем⁴²;
 - в соответствии с инструментарием ИКАО по БАС — инициирование или укрепление совместных усилий в следующих областях:
 - технические и эксплуатационные требования, а также требования в области техники безопасности, предъявляемые к БАС с целью обеспечить их безопасную эксплуатацию;
 - исследования и разработки, включая выполнение обмена результатами и выявление возможностей для сотрудничества по будущим проектам, в первую очередь в области управления воздушным движением;
 - информационные системы;
 - стратегии правоприменения и соблюдения требований, включая партнерство с правоохранительными органами;
 - программы обучения государственных служащих, в обязанности которых входит осуществление надзора за БАС;
- использование двусторонних/региональных соглашений и многосторонних платформ для расширения обмена полученной от правоохранительных органов информацией об угрозах, тактике, личности/местонахождении/деятельности подозреваемых и т. д.;
- формирование — через национальные законы о выдаче/взаимопомощи и/или договоры и иные документы в области уголовного правосудия — правовых основ и каналов для упрощения обмена доказательствами и выдачи скрывающихся от правосудия лиц с целью содействовать уголовному судопроизводству по делам о совершении террористических актов с применением БАС или подготовки к их совершению.



Вставка 6.

Перспективные задачи международного сотрудничества в области пресечения применения БАС в террористических целях

Появление интернета вещей, работающего на основе технологий пятого поколения (5G), может вскоре привести к тому, что управление БАС будет осуществляться через Интернет, причем оператор сможет находиться на большом расстоянии от управляемого им летательного аппарата (Palestini 2020). Такое развитие событий, скорее всего, приведет к тому, что всякий конкретный инцидент с БАС будет затрагивать больше юрисдикций, чем раньше, и это в значительной степени повлияет на способность стран осуществлять сотрудничество в вопросах правоприменения и отправления правосудия. Например, юрисдикция, из которой управляется беспилотный летательный аппарат, должна иметь возможность оперативно выполнить запрос об идентификации пилота и отключении его от управления, исходящий из юрисдикции, где данный БПЛА осуществляет полет, создающий угрозу. Некоторые из мер, которые в настоящее время необходимы для обеспечения эффективного сотрудничества между правительствами в борьбе с киберпреступностью, вскоре также могут стать важнейшими средствами пресечения враждебной деятельности с применением беспилотных летательных аппаратов.

42 Отсутствие специальной нормы таможенной классификации для БАС приводит к тому, что легальные их производители в настоящее время пользуются иными номенклатурными обозначениями, маркируя, например, свои международные отправления как цифровые камеры.



3.1.1.6 Применение БАС для защиты уязвимых объектов

Те же технологии, которые лежат в основе применения БАС в террористических целях, могут использоваться органами государственной власти и операторами объектов для решения важных задач по управлению рисками и урегулированию кризисов. Потенциальные возможности применения БАС в качестве средства защиты уязвимых объектов от террористических нападений (вне зависимости от того, будут эти нападения осуществляться с помощью БАС или нет) являются многогранными, и лица, ответственные за разработку политики, должны поощрять активное использование БАС для этих целей. Если говорить конкретно о защите уязвимых объектов в районах, не затрагиваемых конфликтами, то наиболее актуальными направлениями непосредственного применения БАС представляются следующие:

- выявление уязвимых мест, которые плохо видны и различимы при осмотре с земли, особенно на больших объектах (например, ослабленные участки ограждения по периметру, чувствительные зоны, недостаточно защищенные от потенциальных нападений с воздуха);
- оказание помощи в управлении большими скоплениями людей на крупных

спортивных мероприятиях и концертах, например оповещение сотрудников служб безопасности о чрезмерной концентрации посетителей в определенных местах;

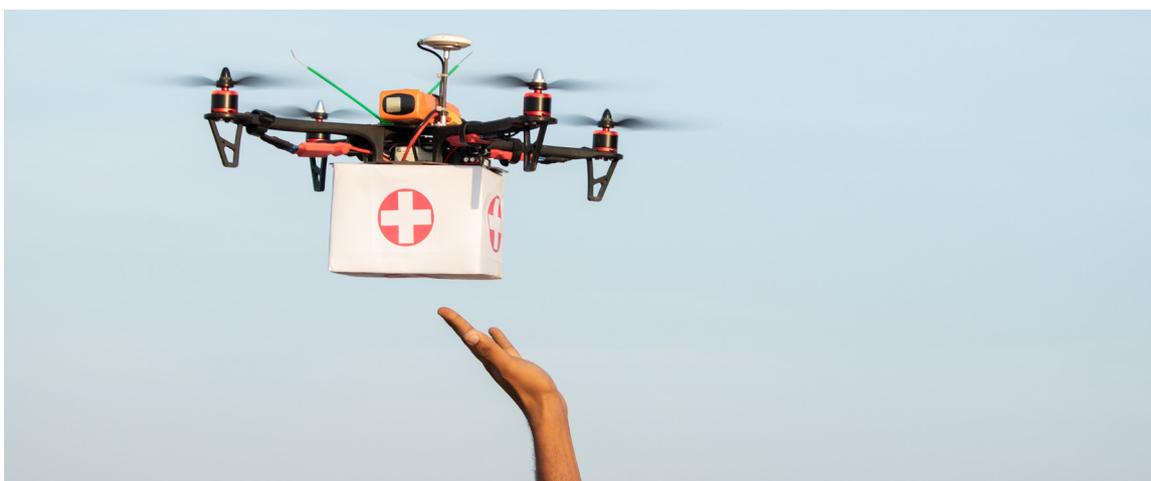
- во время террористического инцидента или сразу после него – применение в качестве средства оказания поддержки при реализации усилий по урегулированию кризиса. Например, БАС могут способствовать повышению эффективности действий по эвакуации пострадавших или предоставлять в режиме реального времени информацию о том, какая территория затронута происшествием, и о характере и масштабах нанесенного ущерба; также эти системы могут помочь сотрудникам аварийных служб быстрее и эффективнее оказывать помощь пострадавшим (например, путем обнаружения узких мест и участков с затрудненным движением в близлежащих районах). БАС, оснащенные тепловизорами, также могут быть использованы для поиска тепловых сигналов при проведении дневных или ночных поисково-спасательных операций;
- поддержка усилий по восстановлению на местном уровне, например путем использования БАС для доставки продовольствия или безопасной передачи медицинских материалов при невоз-

возможности быстрой доставки традиционными транспортными средствами;

- сбор разведывательных данных, например установление личности людей на запланированном мероприятии или подсчет их числа, а также выявление подозрительных перемещений людей вокруг и/или вблизи уязвимых объектов. Например, при сопоставлении с данными из других источников снимки, полученные с помощью БАС, могут служить дополнительным подтверждением подготовительной деятельности, направленной на срыв запланированного мероприятия, на котором ожидается большое скопление людей. Любое применение такого рода должно в обязательном порядке осуществляться в соответствии с обязательствами государств-членов по международному праву в области прав человека;
- обнаружение химических, биологических, радиологических и ядерных материалов, которые террористические группы могут попытаться использовать на уязвимых объектах. В результате ряда технологических прорывов появилась возможность оснащать устройства БАС датчиками, которые могут быть настроены на обнаружение определенных вредных химических веществ, биологических средств или радиоактивного излучения.

Разработка и применение БАС в перечисленных целях сопряжены с рядом важных оговорок:

- при применении БАС для защиты уязвимых объектов, а также иных объектов — особенно в режиме наблюдения — крайне важно, чтобы это делалось в соответствии с законом и с принципами необходимости и соразмерности, с тем чтобы свести к минимуму неблагоприятное воздействие на основные права человека, в том числе на право на неприкосновенность частной жизни;
- следует обратить внимание на то, чтобы гендерные, расовые, религиозные и другие предрассудки не проявлялись в ходе разведывательных операций, осуществляемых с помощью БАС, с тем чтобы не подвергать уязвимые сообщества дальнейшей виктимизации и стигматизации;
- необходимость проявлять сдержанность и соблюдать в соответствии с международными стандартами и требованиями все применимые процессуальные гарантии представляется особенно актуальной в тех ситуациях, когда применяемые БАС оснащаются устройствами, использующими технологии распознавания лиц⁴³.



43 Эффективному использованию установленных на БАС систем распознавания лиц пока препятствует ряд технических проблем, таких как обеспечение расположения устройства под определенным углом, позволяющим должным образом распознать лицо, и возможность получения качественных изображений во время движения или зависания. Обе задачи являются значительно более сложными, чем получение совпадающих изображений из статичных кадров. Однако, несмотря на эти трудности, некоторые технологические компании, специализирующиеся на предоставлении услуг в области наблюдения, разрабатывают БАС с расширенными возможностями распознавания лиц. Патентные заявки еще находятся на стадии подачи, однако правоохранные органы некоторых стран уже рассматривают возможность интеграции таких возможностей в свои беспилотные устройства.



Конкретный пример 9. **Использование БАС для предотвращения террористических актов: опыт Коста-Рики**

Поскольку Коста-Рика является местом проведения ряда международных мероприятий с большим количеством участников, она сталкивается с потенциальными террористическими угрозами в отношении уязвимых объектов. Часть превентивных мер, принимаемых страной, подразумевает применение технологий БАС:

- БАС применяются в рамках деятельности по защите объектов, в первую очередь для обнаружения уязвимостей, остающихся необнаруженными при наблюдении с земли;
- во время крупных мероприятий видеозаписи, сделанные с помощью БАС, передаются в прямом эфире на командный пункт для обеспечения информированности о положении дел не только в месте проведения мероприятия, но и в близлежащих районах;
- БАС также применяются для патрулирования границ страны, особенно на участках несанкционированного проникновения в преддверии крупных мероприятий;
- объекты критически важной инфраструктуры, например трубопроводы, проходящие по территории Коста-Рики, также являются объектами наблюдения, осуществляемого с применением технологий БАС;
- распространенной практикой является также оперативная межведомственная коммуникация, в том числе с Национальным управлением гражданской авиации, в целях обмена информацией и информирования каждого ведомства о последних событиях.

Источник: выступление г-жи Мерседес Кесады, начальника отдела операций с применением БАС Разведывательного управления Коста-Рики, на совещании Группы экспертов, организованном КТУ ООН (6 и 7 октября 2021 года).

3.1.2 Правоохранительные органы

Сообщество правоохранительных органов выполняет несколько важнейших функций в плане сдерживания и расследования террористической деятельности, осуществляемой с применением БАС. Правоохранительные органы оказывают консультационную поддержку операторам объектов, и применяют в рамках своих полномочий технологии противодействия БАС, что делает их важнейшей действующей стороной в работе по обеспечению физической защиты уязвимых объектов.

В следующих разделах дается обзор тех этапов процесса планирования в области безопасности, на которых правоохранительные органы могут адресно вмешиваться, с тем чтобы обеспечивать снижение рисков, содействовать уменьшению ущерба в случае кризисов и осуществлять преследование в отношении предполагаемых преступников, в том числе путем поиска способов дезорганизации преступных сетей, стоящих за их незаконной деятельностью.



Вставка 7.

Соблюдение прав человека и основных свобод при проведении правоохранительных операций с использованием БАС

Поскольку технологии, связанные с БАС, распространяются с очень высокой скоростью, их применение в правоохранительных и антитеррористических целях вызывает серьезные опасения с точки зрения соблюдения прав человека⁴⁴. Следовательно, государства должны тщательно изучать обоснованность и необходимость проведения операций с применением БАС, будь то на этапах планирования, выполнения или последующего расследования. В то же время, даже сотрудничая с другими государствами в решении задач по поддержанию правопорядка, государственные органы должны обеспечивать соблюдение прав человека в ходе реализации процесса передачи и распространения технологий, связанных с применением беспилотных летательных аппаратов. В частности:

1. использование БАС внутри страны в целях поддержания правопорядка, включая защиту уязвимых объектов, должно полностью соответствовать обязательствам государств по международному праву в области прав человека, включая:
 - a) право на жизнь, в той степени, в которой технологии ударных БПЛА или БАС применяются для содействия осуществлению более широких стратегий в области поддержания правопорядка, основанных на применении силы⁴⁵;
 - b) право на неприкосновенность частной жизни, принимая во внимание применение беспилотных летательных аппаратов для наблюдения; и
 - c) свободу выражения мнений и свободу ассоциаций, которые опосредованно нарушаются при осуществлении широкомасштабного и дистанционного наблюдения с применением технологий беспилотных летательных аппаратов;

44 В 2020 году Специальный докладчик Организации Объединенных Наций по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях сообщил, что по меньшей мере 102 страны располагают запасом активно применяемых БПЛА, а около 40 обладают вооруженными БАС или находятся в процессе их приобретения.

45 Право на жизнь затрагивается как в случаях применения ударных БАС, так и при использовании таких систем для поддержки применения силы правоохранительными органами на земле. Разведывательные БАС можно легко и с небольшими затратами переделать в ударные, и, по имеющейся информации, производители беспилотных летательных аппаратов активно продвигают на рынке модели, оснащенные электрошокерами, устройствами для распыления слезоточивого газа и перцового аэрозоля, предлагая их правоохранительным органам США, Южной Африки, Франции и Индии.



Вставка 7. (продолжение)

- 2) обязательства по защите прав человека влекут за собой практические ограничения на этапах планирования операций с применением БАС и расследования любых предполагаемых нарушений после их совершения:
 - a) планирование операций с БАС: государства должны убедиться в том, что то или иное действие является необходимым и соразмерным намеченным целям. Перед принятием любого решения о применении БАС, которые могут обладать возможностями целеуказания, необходимо провести тщательный анализ. Планов и приказов общего характера, направленных против выявленных значимых лиц, будет недостаточно при отсутствии зафиксированной прямой связи между целями и непосредственными угрозами для других людей;
 - b) расследование предполагаемых нарушений права на жизнь: такое расследование должно проводиться оперативно, эффективно и тщательно. Лица, которым стало известно о возможном нарушении права на жизнь, обязаны незамедлительно доложить об этом своему руководству. Более того, расследования и лица, проводящие их, должны быть независимыми от ненадлежащего влияния (и восприниматься таковыми);
- 3) государства должны помнить о серьезных потенциальных правозащитных последствиях, возникающих в связи с передачей технологии применения беспилотных летательных аппаратов тем государствам, в которых права человека не соблюдаются в должной степени. В соответствии с нормами международного права на государства возлагается обязанность следить за тем, чтобы их деятельность не способствовала, намеренно или в результате отсутствия должной осмотрительности, незаконному использованию другими государствами технологий применения ударных беспилотных летательных аппаратов⁴⁶. Кроме того, в результате широкого распространения передовых технологий БПЛА повсюду в мире государства столкнутся с серьезными проблемами в попытках установить контроль за их распространением среди негосударственных субъектов.

Источник: выступление г-жи Фионнуалы Ни Аолаин, Специального докладчика Организации Объединенных Наций по вопросам поощрения и защиты прав человека и основных свобод в условиях борьбы с терроризмом, на организованном КТУ ООН совещании Группы экспертов (6 и 7 октября 2021 года)

⁴⁶ Эти опасения представляются особенно актуальными с учетом того, что государства регулярно оправдывают удары вооруженных БПЛА целями борьбы с терроризмом на их территориях, тогда как — и это неизменно подчеркивает Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом — эта борьба часто используется самими государствами как прикрытие для незаконной деятельности, служащей достижению идеологически обусловленных внутренних целей.

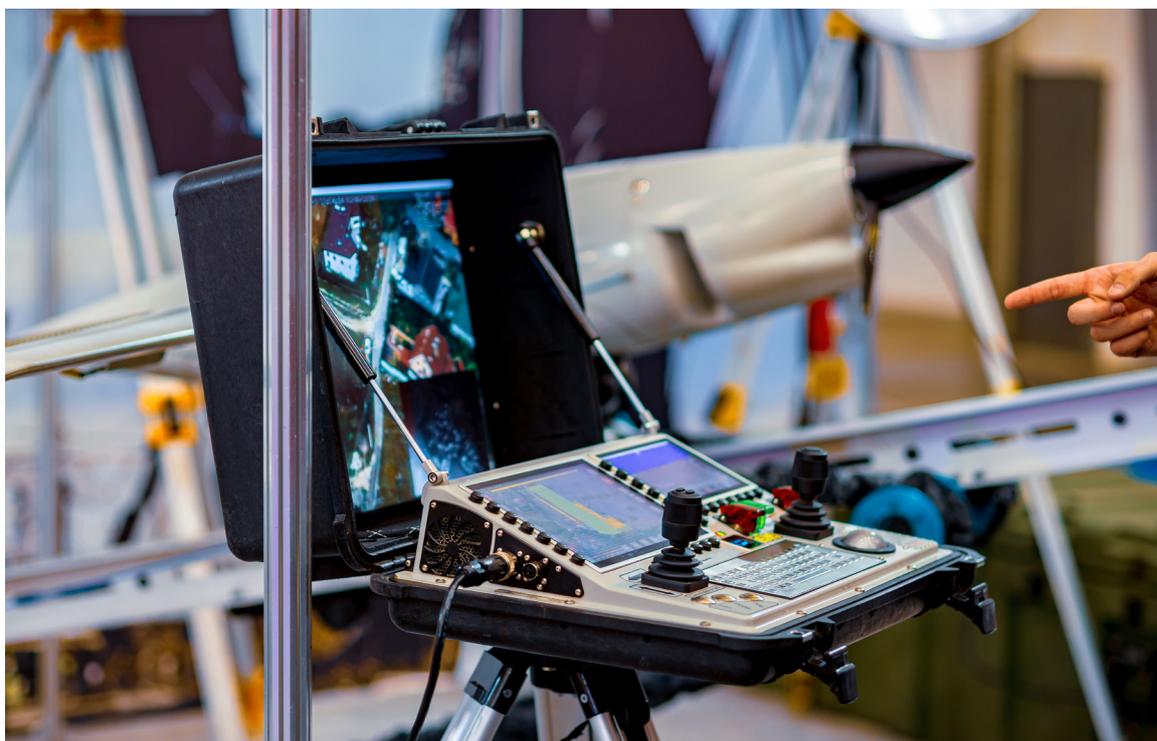
3.1.2.1 Поддержка операторов уязвимых объектов

Поскольку угрозы, связанные с применением БАС, пока недостаточно изучены и/или недооцениваются, правоохранные органы должны играть важную роль в оказании помощи операторам уязвимых объектов в оценке и понимании конкретных угрожающих сценариев, затрагивающих их помещения и оборудование. В частности, в рамках цикла управления рисками эта поддержка может оказываться по следующим направлениям:

- помощь в разработке плана обеспечения безопасности, начиная с оценки намерений и возможностей соответствующих субъектов, представляющих угрозу, а также в выявлении угроз и уязвимостей;
- предоставление персоналу, обслуживающему объект, руководящих указаний по реализации плана, в том числе подготовка этого персонала;
- предоставление экспертных консультаций по применимым мерам управления рисками и доступным возможностям финансирования с целью получения помощи в модернизации системы безопасности.

Что касается готовности к кризисным ситуациям, то местные правоохранные органы должны тесно взаимодействовать с операторами объектов в области подготовки планов действий в чрезвычайных ситуациях на случай, если ударным БАС удастся обойти меры безопасности, действующие на уязвимом объекте. Задачей первоочередной важности должно быть проведение незамедлительной эвакуации посетителей и персонала объекта из находящейся под угрозой зоны. Для того чтобы максимально увеличить шансы на проведение при необходимости эффективной эвакуации, следует поощрять проведение регулярных учений/тренировок по конкретным кризисным сценариям и проводить их под контролем правоохранных органов и персонала объекта, отвечающего за безопасность.

Кроме того, чтобы подготовиться к развитию кризиса, вызванного применением БПЛА, рекомендуется составить матрицу рисков и включить ее в планы обеспечения безопасности. Надлежащее понимание ситуации, сформированное у сотрудников служб реагирования на кризисы, включая сотрудников правоохранных органов и служб безопасности, до начала кризиса, повышает уровень их осведомленности о положении дел и позволяет им действовать более эффективно.





Вставка 8.

Включение информации, собранной с помощью БАС, в работу центров синтеза

Конечной целью центров синтеза является обеспечение расширенного обмена информацией и межучрежденческого сотрудничества, поскольку они связывают воедино информацию из многочисленных правоохранительных и разведывательных источников на местном, национальном и даже международном уровнях. В этом контексте БАС могут стать для центров синтеза еще одним ценным источником собираемой и обрабатываемой информации по теме борьбы с терроризмом. В частности, возможности БАС в области разведки, наблюдения и рекогносцировки могут быть особенно полезны для центров синтеза при сборе разведывательной информации общего характера и, в частности, информации, связанной с границей, а также информации, способствующей защите уязвимых объектов и критически важной инфраструктуры.

Например, одной из основных обязанностей бельгийского национального центра синтеза – Координационного органа по анализу угроз – является определение степени угрозы на национальном уровне и подготовка скоординированных анализов угроз для критически важной инфраструктуры страны и Европейского союза. Информация, полученная с помощью БАС, может стать ценным вкладом в анализ угроз и быть полезной для определения степени угрозы на национальном уровне.

Потенциальной проблемой, возникающей при использовании БАС во взаимодействии с центрами синтеза, является возможность хакерского взлома. Поскольку аппараты, входящие в БАС, являются элементами сетевой структуры, передающей информацию в центр синтеза, они могут стать точками взлома, в которых хакеры получают доступ к хранящейся информации. Этот риск можно значительно снизить за счет последовательного анализа и устранения потенциальных недостатков в системе обеспечения безопасности используемого программного обеспечения.

Источник: параллельное мероприятие на тему «Коммерческие беспилотные авиационные системы в условиях борьбы с терроризмом», организованное КТУ ООН в рамках виртуальной Недели борьбы с терроризмом, 29 июня 2021 года (система веб-вещания Организации Объединенных Наций, URL: <https://media.un.org/en/asset/k1g/k1gt7x766e>).





3.1.2.2 *Защита уязвимых целей с помощью технологий противодействия БАС*

На базовом уровне технологии противодействия БАС в зависимости от их назначения можно разделить на технологии обнаружения и технологии отключения/ перехвата⁴⁷.

- *Технологии обнаружения БАС:* по сравнению с визуальным наблюдением эти технологии предлагают значительно более точные и надежные средства обнаружения создающей угрозу БАС в пределах определенного радиуса. Они могут быть основаны на радиочастотном (РЧ) анализе, акустических датчиках, оптических датчиках или на применении радара. Каждая из этих технологий имеет свои преимущества и недостатки, и уполномоченные сотрудники правоохранительных органов/служб безопасности должны в полной мере оценить их сильные стороны и ограничения, исходя из таких факто-

рах, как стоимость, простота развертывания и условия, в которых они должны работать (например, уровни радиочастотных перегрузок и помех, освещенность и атмосферные условия)⁴⁸. Потенциальным способом обхода технологий обнаружения БАС является использование алюминия для покрытия GPS-модуля БАС. Это подтверждает, что операторам уязвимых объектов следует выстраивать многоуровневую систему безопасности, включая визуальное наблюдение, даже при использовании высокоэффективных технологий противодействия БАС.

- *Технологии отключения/перехвата БАС:* зафиксировав присутствие угрожающей БАС, уполномоченные сотрудники службы безопасности и/или правоохранительных органов должны быстро принять решение о наиболее подходящих мерах, которые необходимо принять, чтобы предотвратить причинение создающим угрозу устройством вреда людям и/или материальным ценностям.

47 В Техническом руководстве по резолюции 2370 СБ ООН также содержится обзор различных технологий обнаружения и отключения/перехвата, включающий соображения/опасения для правоохранительных органов при использовании различных технологий, имеющихся в их распоряжении. Cf. Submodule II, «Counter UAS systems and techniques» (3.1.).

48 Например, при попытке обнаружить сигналы, с помощью которых осуществляется управление БАС, производительность устройств на основе радиочастот резко снижается в густонаселенных районах, где спектр электромагнитного излучения насыщен помехами и перегружен. Микрофоны акустических датчиков имеют ограниченную эффективность обнаружения в среде, насыщенной шумами, а эффективность оптических технологий обнаружения может быть снижена в условиях низкой освещенности. Радарные системы являются основным средством обнаружения объектов на больших расстояниях. Они также способны обнаруживать низколетящие и малые БАС, но зачастую оказываются не в состоянии отличить птицу от малого БПЛА (Association of the United States Army 2021).

Технологии отключения/перехвата БАС делятся на две широкие категории: кинетические и некинетические. Первые предусматривают устранение или уменьшение угрозы, исходящей от летающего объекта. Как правило, они связаны с использованием сетевых, метательных устройств или лазерного оружия. В свою очередь, некинетические технологии предполагают создание помех сигналу БАС (например, за счет мощного микроволнового излучения). Как правило, основной формой воздействия некинетических устройств является генерация радиочастотных сигналов, что позволяет воспрепятствовать штатному процессу управления БАС.

Операторы уязвимых объектов обычно не имеют доступа ко многим технологиям противодействия БАС, особенно к тем, которые направлены на пресечение процесса управления БАС. Таким образом, использование технологий отключения/перехвата часто является прерогативой правоохранительных органов и других уполномоченных государственных органов или сотрудников служб безопасно-

сти. Уполномоченные должностные лица должны быть знакомы с преимуществами и недостатками имеющихся решений и обеспечивать, чтобы их применение соответствовало применимым правовым рамкам, а также конкретным условиям, в которых их предполагается использовать. Для понимания физических и технических особенностей объектов, а также окружающих территорий необходимо тесное взаимодействие с операторами уязвимых объектов⁴⁹. Кроме того, рекомендуется регулярно проводить оценку технологий противодействия БАС, чтобы определить, способствует ли их включение в протоколы обеспечения безопасности совершенствованию системы охраны, и не формирует ли при этом спрос, который невозможно поддерживать. Развертывание технологий противодействия БАС при проведении крупного мероприятия будет также зависеть от глубины понимания динамики самого мероприятия с точки зрения его различных фаз, ожидаемого перемещения большого количества людей, прибытия и отъезда высокопоставленных лиц и т. д.



Вставка 9. БАС и поиски точек запуска

После обнаружения и нейтрализации БАС можно использовать различные технологии для отслеживания сигналов этой системы до точки запуска и точки, с которой осуществлялось дистанционное управление. Потенциально эта мера противодействия БАС позволяет правоохранительным органам не только выводить из строя враждебные БАС, но и задерживать лиц, несущих ответственность за их эксплуатацию, что дает возможность получать важную информацию о деятельности террористов и базах командования и управления.

Возможно также применение БАС в координации с центрами синтеза: такая совместная деятельность обеспечивает более высокую эффективность поисковых рейдов по местам запуска БАС. Информация, полученная или собранная государствами-членами в отношении террористов в ходе рейдов по местам запуска БАС, может быть затем проанализирована и переработана в национальном центре синтеза (см. вставку 8) для своевременного и точного распространения среди соответствующих правоохранительных органов или разведывательных служб.

Источник: параллельное мероприятие на тему «Коммерческие беспилотные авиационные системы в условиях борьбы с терроризмом», организованное КТУ ООН в рамках виртуальной Недели борьбы с терроризмом, 29 июня 2021 года (система веб-вещания Организации Объединенных Наций, URL: <https://media.un.org/en/asset/k1g/k1gt7x766e>).

⁴⁹ Например, некоторые технологии больше подходят для применения в сельской местности, тогда как другие лучше использовать в условиях городской застройки.



Конкретный пример 10.

Тестирование и оценка мер противодействия БПЛА: учения Интерпола и норвежской полиции

С 28 по 30 сентября 2021 года Интерпол и полиция Норвегии провели трехдневные учения с участием представителей правоохранительных органов, научных кругов и отраслевых экспертов из Европы, Израиля и Соединенных Штатов. Цель учений заключалась в тестировании и оценке 17 мер противодействия БПЛА, направленных на обеспечение безопасности в окружающем аэропорт пространстве посредством обнаружения, отслеживания и идентификации БАС и их пилотов⁵⁰.

Каждая контрмера оценивалась и получала балльный рейтинг по определенным критериям. Это позволит обобщить результаты в рамочной программе Интерпола по борьбе с БПЛА, которая, как ожидается, станет глобальной площадкой для сотрудничества и обмена знаниями между правоохранительными органами 194 стран – членом Интерпола.

Учения проводились в аэропорту Осло Гардермуэн в период его активной эксплуатации. Активация любой из систем в аэропорту предполагала обязательное лицензирование и одобрение со стороны регулирующего органа, а также получение разрешения от оператора аэропорта. Сложность учений потребовала тесного сотрудничества с владельцем аэропорта, Норвежским управляющим органом в области коммуникаций, Управлением гражданской авиации и норвежским регулятором использования БАС, что позволило обеспечить соответствие всех систем и испытаний требуемым стандартам и не оказывать воздействия на работу аэропорта.

50 Испытанные средства противодействия БПЛА были разделены на 4 группы: пассивные, активные, мультисистемные и эффекторные системы; каждое из которых оценивалось по эффективности обнаружения, отслеживания и определения местоположения беспилотного летательного аппарата, вошедшего в ограниченное воздушное пространство. За время учений было проведено более 2000 активных перемещений летательных аппаратов.

Конкретный пример 10. (продолжение)

Помимо учений, были проведены семинары и презентации по вопросам сохранения доказательств случаев вторжений БПЛА. На этих встречах участники обменивались передовым опытом и обсуждали возможные перспективные решения проблемы вторжения БПЛА.

Источники: <https://www.interpol.int/News-and-Events/News/2021/INTERPOL-carries-out-full-scale-drone-countermeasure-exercise>; выступление г-на Кристофера Черча, старшего специалиста по мобильной криминалистической экспертизе, Интерпол, на совещании Группы экспертов, организованном КТУ ООН (6 и 7 октября 2021 года).



Конкретный пример 11.

Применение БАС полицией Каталонии

Всемирный конгресс операторов мобильной связи 2019 года, проходивший в Барселоне, стал для автономной полицейской службы («Mossos d'Esquadra») испанской провинции Каталония первой возможностью развернуть систему наблюдения, обеспечивающую безопасность этого мероприятия с помощью БАС. Развертывание данной системы стало возможным в соответствии с положениями нового закона



Испании о БПЛА (Королевский указ 1036/2017), который позволяет силам безопасности применять беспилотные устройства в различных ситуациях, в первую очередь в контролируемом воздушном пространстве, над людьми в зданиях и в ночное время. Беспилотные летательные аппараты, развернутые региональными полицейскими силами, производили фото- и видеосъемку в режиме реального времени над территориями, за которыми велось наблюдение.

При проведении операций вблизи аэропорта Барселоны (Эль-Прат) сотрудники Региональной полиции также координировали свои действия с испанской компанией — оператором аэропортов (AENA - Aeropuertos Españoles y Aeronavegación Aérea) и с поставщиком услуг по регулированию воздушного движения в Испании (государственная компания ENAIRE). Все действия производились в пределах операционной зоны на объявленной высоте до 50 метров и в тесной координации с вертолетными службами, а также в постоянном контакте с диспетчерской вышкой аэропорта Барселоны.

Источник: <https://www.unmannedairspace.info/uncategorized/barcelona-security-forces-pioneer-urban-drone-services-spain/>.



Программный документ 7

Передовая практика и гарантии развертывания технологий противодействия БАС – Министерство транспорта, Соединенное Королевство, 2018 год (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729458/taking-flight-the-future-of-drones-in-the-uk.pdf)

В консультационном документе, разработанном Министерством транспорта Соединенного Королевства в 2018 году, признается необходимость введения ряда гарантий для обеспечения надлежащего использования технологии БАС как в целях обнаружения, так и в целях пресечения/перехвата⁵¹:

- применение технологий БПЛА ограничено и осуществляется только специально подготовленными и/или лицензированными операторами;
- существует четкая цель и сфера применения этой технологии, а также операционная стратегия, индивидуально скорректированная для каждой стороны и соответствующая применимым нормативным документам, например конкретному кодексу практики;
- в соответствующих случаях проводится полная оценка риска в соответствии с законодательством в области охраны труда и техники безопасности;
- при необходимости с соответствующими регулирующими органами можно заключить меморандум о взаимопонимании, охватывающий механизмы разрешения споров и урегулирования трудностей, возникающих в результате возникновения неисправности или неправильного использования технологии;
- все данные, полученные с помощью технологии обнаружения БПЛА, обрабатываются в соответствии с действующим законодательством, например с правилами в области защиты данных;
- данные технологии применяются только в соответствии с оперативными требованиями, когда их использование признается необходимым и соразмерным в соответствии с применимыми правовыми нормами, включая стандарты в области прав человека, например со статьей 8 Европейской конвенции по правам человека;
- сами технологии проверяются на соответствие их целевому назначению, с тем чтобы свести к минимуму возможность возникновения случайных помех;
- информирование регулирующих органов, отвечающих за надзор за развернутыми технологиями, производится при установке оборудования для применения технологии БПЛА и, по возможности, до начала установки;
- в зависимости от характера участвующей стороны или мероприятия, организации предупреждают общественность (через средства информирования общественности, на основе работы с населением на местах и посредством размещения объявлений) о том, что несанкционированное использование БПЛА будет отслеживаться и что возможно применение мер принуждения;
- разработана и применяется соответствующая страховка.



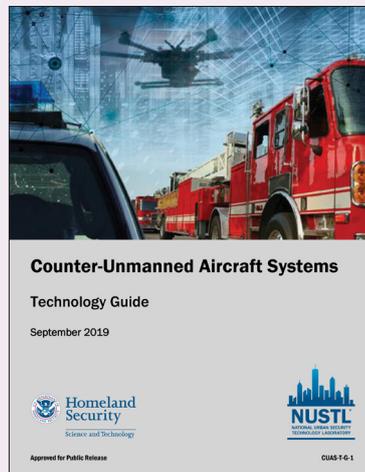
51 Документ «Taking Flight: The Future of UAS in the UK», пп. 7.21 и 7.38 текста на английском языке



Программный документ 8

Противодействие беспилотным авиационным системам: руководство по технологиям – Министерство внутренней безопасности и Национальная лаборатория технологий обеспечения безопасности в городах, США, 2019 год (www.dhs.gov/publication/st-c-uas-technology-guide)

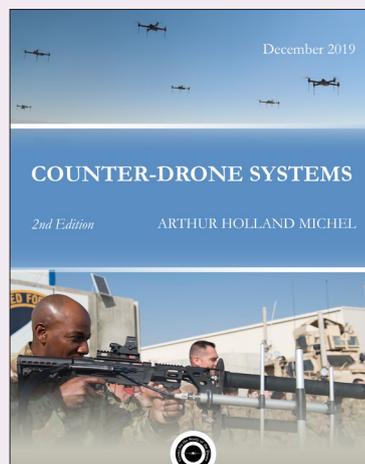
Руководство по технологиям предназначено для ознакомления сообщества служб экстренного реагирования с технологиями противодействия БАС. В нем представлен обзор технологий малых беспилотных авиационных систем, включая основные компоненты, обеспечивающие их функционирование. Информация, представленная в данном руководстве, отражает технический, научный и инженерный опыт, накопленный Национальной лабораторией технологий обеспечения безопасности в городах, а также содержит информацию, полученную на основании интернет-исследований, отраслевых публикаций и данных, предоставленных производителями.



Программный документ 9.

Системы противодействия беспилотным летательным аппаратам: Центр изучения беспилотных летательных аппаратов при Бард-колледже, 2019 год (<https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf>)

В данном докладе содержится справочная информация о растущем спросе на технологии противодействия БАС и о том, как они функционируют, представлена база данных известных товаров в категории противодействия БАС со всего мира, а также объясняются некоторые проблемы, связанные с применением этих технологий. Анализ основан на изучении технических и программных докладов, письменных свидетельств, новостей и аналитических материалов из открытых источников, а также на информации, представленной производителями; на тематических интервью с представителями органов государственной власти и правоохранительных органов, представителями отрасли и экспертами в данной области; и на результатах участия как в открытых, так и в закрытых конференциях и семинарах.



3.1.2.3 Расследование инцидентов, связанных с применением БАС

Лица, расследующие дела о нападениях, связанных с применением БАС, должны соблюдать общеприменимые процедуры, установленные внутренним уголовным

законодательством и нормами международного права (например, исполнять обязанность сообщать причины ареста в момент задержания и незамедлительно доставлять подозреваемого в суд, соблюдать презумпцию невиновности и не признавать доказательства, полученные под

пытками, проводить справедливое судебное разбирательство). В то же время в ходе расследований инцидентов с участием БАС часто возникают особые ситуации и проблемы. Правоохранительным органам важно оценить особенности нападений, совершенных с применением беспилотных летательных аппаратов, и мобилизовать соответствующий набор навыков проведения расследования, в частности при выполнении следственных действий на месте преступления и при расследовании деятельности преступных/террористических сетей, стоящих за этими нападениями.

- Следственные действия на месте преступления: расследование инцидентов, связанных с применением беспилотников, должно проводиться как можно раньше, пока место преступления еще не подверглось посторонним воздействиям. Подобранные с земли и при-

веденные в неопасное состояние, БАС могут стать ценными уликами, поддерживающими ведение уголовного процесса. Эксперты по цифровой криминалистике играют важную роль в извлечении из изъятых БАС таких данных, как скорость, высота, GPS-координаты и записи полетов, при этом другие эксперты могут организовать поиск «более традиционных» физических свидетельств, таких как отпечатки пальцев и образцы биоматериалов, оставленных на компонентах беспилотных систем, в том числе на брошенных пультах управления. С той же вероятностью лица, совершившие указанное преступление, могут оставить ценные улики на объектах, с которых они совершали нападение, особенно в тех случаях, когда они были вынуждены покинуть свое «рабочее место» в спешке⁵².



Вставка 10.

Потенциальная опасность сбитых беспилотных летательных аппаратов: случай в северном Ираке

Сотрудники правоохранительных органов и/или другие уполномоченные должностные лица должны обращаться со сбитыми БАС с особой осторожностью, поскольку такие системы потенциально могут быть использованы в агрессивных целях, даже если на земле они кажутся безобидными. Такой случай произошел на севере Ирака, когда курдские ополченцы сбили небольшой беспилотник размером с модель самолета, приняв его за одну из многочисленных БАС, которые в этом районе использовались ДАИШ в разведывательных целях. Полагая, что устройство может быть полезным для получения информации об использовании беспилотных летательных аппаратов в террористической деятельности, ополченцы подвергли его тщательной проверке. Неожиданно для тех, кто разбирал этот БПЛА, произошел взрыв: сдетонировало небольшое самодельное взрывное устройство, спрятанное внутри аппарата.

Источник: Stanifort, 2017.



52 Cf. 2370 Technical Guidelines, Submodule II, in particular: "UAS incident scene – safety and security" (3.2), "Recovery and preservation of evidence" (3.3.), "Technical exploitation of recovered UAS and components" (3.4.), "Information management" (3.5).

- **Расследование деятельности сетей обеспечения:** в большинстве инцидентов с применением БАС «лицо, совершившее нападение, пользовалось помощью других лиц, организованных в более широкую террористическую сеть или группу, оказывавших данному лицу помощь в приобретении технологий БАС, в выборе целей, совершении нападения или в период после совершения нападения. Выявление таких сетей имеет решающее значение для предотвращения дальнейших нападений со стороны тех же или связанных с ними групп, как с применением БАС, так и с использованием другого оружия» (GCTF 2019, Good Practice 20). В процессе раскрытия охвата и масштабов преступной деятельности, приведшей к нападению с использованием БАС, в тех случаях, когда преступники не использовали БАС, сделанные

по индивидуальному заказу, важные для следствия данные могут быть получены из архивов сведений о лицензировании операторов и регистрации БАС, а также из документов, составляемых в рамках экспортного контроля⁵³.

Насколько позволяют имеющиеся ресурсы, расследования должны быть направлены на изучение обеспечивающей сети пособников и соучастников, а также на поиск лиц, участвовавших в подготовке нападения на начальном этапе. Углубленное расследование может выявить наличие транснациональных элементов и связей, что требует от лиц, ведущих расследование, готовности и способности получать информацию и доказательства от иностранных партнеров, в том числе по каналам взаимной правовой помощи.



Вставка 11.

Международный сговор с целью приобретения

Расследования, проведенные как минимум в четырех странах (в Соединенном Королевстве, Бангладеш, Испании и Дании), выявили сложные механизмы, лежащие в основе программы применения БАС со стороны ДАИШ, а также широкий транснациональный характер этой программы. В рамках этой схемы в 2015 году в Соединенном Королевстве, Бангладеш и Испании было создано несколько предприятий, действовавших в сфере информационных технологий, электроники и веб-услуг и выступавших в качестве подставных компаний для приобретения и переправки в распоряжение ДАИШ оборудования, имеющего отношение к применению БАС. Указанная продукция закупалась как минимум у девяти различных компаний, расположенных в США и Канаде. Стремясь выдать свою активность за законную деятельность, участники заговора использовали вымышленные имена и приложения с шифрованием данных для обмена сообщениями, рассчитывая таким образом избежать обнаружения правоохранными органами.

Источник: Ressler 2018

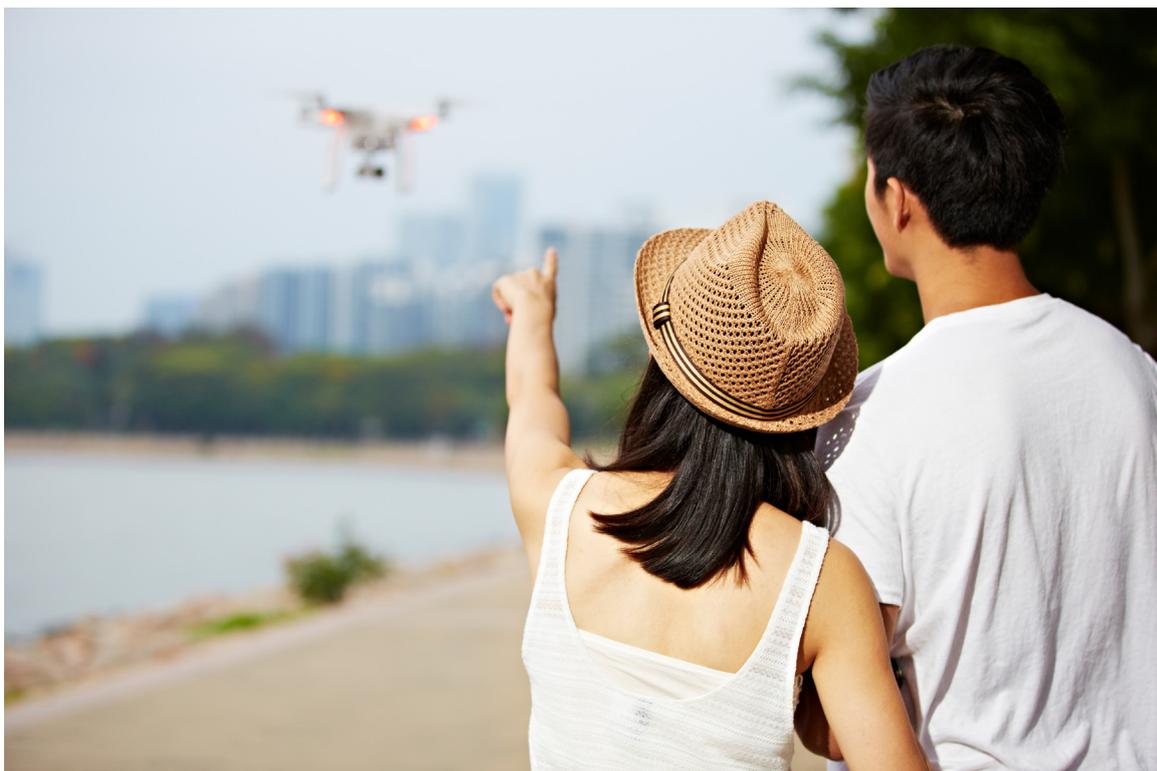


Конкретный пример 12.

Полномочия на задержание и проведение досмотра в целях поиска БАС

В 2018 году правительство Соединенного Королевства (в лице Министерства внутренних дел) выпустило для проведения консультаций с общественностью документ под названием: «Задержание и досмотр: расширение полномочий полиции для охвата правонарушений, связанных с использованием беспилотных летательных аппа-

53 Cf. 2370 Technical Guidelines, Submodule II, in particular: "Identification of perpetrators" (3.6.).



ратов (БПЛА), лазерных указок и коррозионных веществ» (Stop and search: extending police powers to cover offences relating to unmanned aircraft (UAS), laser pointers and corrosive substances). Этот документ содержит следующий гипотетический сценарий, иллюстрирующий типичный случай, когда отсутствие у правоохранительных органов конкретных полномочий на проведение задержания и досмотра может привести к повышению степени уязвимости объектов перед нападениями с применением БАС: «Полиция неоднократно получала от населения телефонные сообщения о человеке, управляющем беспилотным летательным аппаратом в месте скопления людей, что является правонарушением согласно Постановлению об авиационной навигации 2016 года. У полиции имелось в распоряжении описание этого человека и места происшествия. Сотрудники полиции выполняли патрулирование указанного района в то время, когда поступало большинство звонков с сообщениями об этом инциденте, и обнаружили человека, подходящего под имевшееся у них описание. На тот момент указанное лицо не управляло беспилотным летательным аппаратом, но имело при себе большую сумку. Сотрудники полиции подошли к мужчине и спросили, что он делает в этом месте. Во время разговора мужчина давал уклончивые ответы, и было видно, что наличие сумки в руках заставляет его нервничать. Приняв во внимание место и время, соответствие внешности мужчины имеющемуся описанию, а также поведение указанного лица, сотрудники полиции констатировали, что у них есть достаточные основания полагать, что у подозреваемого имеется беспилотный летательный аппарат, с помощью которого он совершал правонарушение, а именно управлял БПЛА в месте скопления людей (что является правонарушением согласно Постановлению об авиационной навигации 2016 года). На основании имеющихся подозрений и при наличии предмета обыска сотрудники полиции четко и в полной мере объяснили задержанному лицу свои действия и произвели досмотр, в результате которого был изъят БПЛА и сопутствующие предметы».

Источник: Министерство внутренних дел Соединенного Королевства, 2018 год



Программный документ 10.

Рамочная программа реагирования на инциденты с применением беспилотных летательных аппаратов для сотрудников экстренных служб и специалистов по цифровой криминалистике, Интерпол, 2020 год
(www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf)

Данное руководство содержит технические указания по управлению и обработке инцидентов, связанных с беспилотниками. Оно адресовано двум основным целевым группам: сотрудникам служб быстрого реагирования и полиции, выезжающим на место происшествия, и специалистам по цифровой криминалистике, обрабатывающим электронные улики после инцидента. Прокуроры, судьи и адвокаты также могут извлечь из него полезную информацию.

Сведения консультационного характера, содержащиеся в руководстве, предназначены для использования в качестве справочной информации как на стратегическом, так и на тактическом уровнях и дополнены выдержками из руководства по исследованию мест совершения преступлений, опубликованного Национальным институтом правосудия США⁵⁴. Оно включает разделы, посвященные компонентам БПЛА, полезной нагрузке БПЛА, данным БПЛА, способам поиска и местам сохранения источников доказательств (телефон, пульт дистанционного управления, SD-карта, внутренняя память), процедурам безопасности, мерам предосторожности перед приближением к БПЛА, мерам предосторожности при обращении с БПЛА, первой помощи и экстренным процедурам, процедуре изъятия БПЛА, цифровой судебной экспертизе, сохранению отпечатков пальцев, сбору и сохранению цифровых доказательств.

3.1.2.4 Таможенный и пограничный контроль

Актуальность БАС с точки зрения таможенного и пограничного контроля проявляется как минимум в трех областях, касающихся деятельности по предупреждению терроризма⁵⁵:

- обнаружение и изъятие БАС и соответствующих компонентов, незаконно перемещаемых через границу для использования в террористических целях;
- обнаружение и изъятие БАС, рассматриваемых как средство транспортировки оружия, товаров, оборудования, наличных денежных средств и т. д., предна-

значенных для использования при подготовке террористических актов;

- использование БАС в качестве инструментов правоохранительной деятельности служб охраны границы для мониторинга трансграничной деятельности, включая несанкционированное пересечение границ на отдаленных и слабо охраняемых участках, расположенных между установленными пунктами въезда⁵⁶.

Характерной проблемой для таможенных властей является обращение с товарами двойного назначения (например, физические компоненты, программное обеспечение для технологических разработок)⁵⁷.

54 URL: <https://nij.ojp.gov/topics/articles/crime-scene-investigation-guides-law-enforcement>.

55 Cf. UNSCR 2370 Technical Guidance document, Submodule II, "Customs and border controls" (2.3.1).

56 БАС могут предоставлять важнейшую визуальную информацию и использоваться как средство наблюдения на слабо охраняемых участках границы для предотвращения потенциальных террористических угроз путем обнаружения аномальной активности с большого расстояния. Кроме того, при оснащении БАС инфракрасными или тепловыми датчиками они могут оказывать помощь патрульным группам в охране пограничных районов в темное время суток

57 Режим контроля за ракетной технологией (РКРТ) и Вассенаарские договоренности являются двумя многосторонними режимами, в рамках которых закладывается нормативная база контроля за экспортом БАС. В частности, РКРТ представляет собой поддержанную 35 сторонами инициативу в области лицензирования экспорта, направленную на предотвращение распространения беспилотных систем, способных служить средствами доставки оружия массового



Эти трудности в значительной степени совпадают с проблемами, возникающими при торговле веществами, которые также могут быть использованы для изготовления самодельных взрывных устройств, — например, нитратом аммония. И в этой области любые достижения зависят от способности пограничных и таможенных органов обмениваться точной предварительной информацией о поступающих товарах, обрабатывать такую информацию и разрабатывать индикаторы риска⁵⁸.

3.1.3 Разведывательные службы

Способность стран понимать развитие и принципы действия незаконных сетей поставок БАС, точно выявлять вовлеченных в них субъектов и фиксировать маршруты передвижения людей и товаров как в Интернете, так и в обычной жизни является важнейшим условием реализации общих усилий по снижению риска. В то же время мобилизация ресурсов, необходимых

для разрушения цепочек поставок/закупок для применения БАС в террористических целях, зависит от способности стран собирать и обрабатывать значительные объемы высококачественных разведывательных данных. Эти сведения могут быть получены из различных источников и должны обрабатываться путем перекрестного анализа всех доступных данных.

Например, при наличии соответствующей нормативно-правовой базы на поставщиков БАС может быть возложена обязанность производить должную проверку потенциальных клиентов и сообщать компетентным органам о подозрительных сделках (см. раздел 3.2.3). Это может стать источником ценной информации, потенциально открывающей новые направления расследований, подтверждающей достоверность уже разрабатываемых версий, а также обеспечивающей поступление новых подробностей об уже идущих сделках и личностях вовлеченных в них лиц.

Критически важную информацию можно также получать на местах путем сбора и

уничтожения. Вассенаарские договоренности обязывают 42 страны-участницы, среди прочего, предотвращать приобретение террористами товаров двойного назначения путем применения мер экспортного контроля ко всем товарам, включенным в список товаров и технологий двойного назначения и список боеприпасов, в целях предотвращения несанкционированной передачи или реэкспорта этих товаров.

58 В Техническом руководстве к резолюции 2370 СБ ООН рассматриваются типы подсистем БАС, в отношении которых государства могут применить регулирование. Cf. Submodule II, "Control of UAS and key sub-systems".

анализа фотографических и документальных свидетельств, в том числе из зон конфликта. В некоторых случаях правительства прибегают к услугам организаций частного сектора, задача которых заключается в работе на местах, когда силами их следственных групп производится документирование наличия незаконного оружия, боеприпасов и соответствующих материальных средств в районах, затронутых конфликтом, и в отслеживании источников их поставок. Например, недавнее исследование приобретения, разработки и использования ударных БАС группой

ДАИШ в Ираке и Сирии пролило свет на обширную сеть ее поставщиков программного обеспечения и компонентов аппаратного обеспечения, используемых для сборки беспилотных авиационных систем. Это исследование также показало, каким образом террористические группы используют международные рынки, в частности онлайн-рынки, для осуществления поставок БАС и соответствующих компонентов, что объясняет растущее внимание разведывательных служб к осуществлению надзора за сделками, оформляемыми через Интернет (см. вставку 12).



Вставка 12.

Сеть группы ДАИШ по закупке БАС

Расследование, проведенное компанией «Конфликт армамент ресерч» (КАР)⁵⁹ по найденным коммерческим БАС, которые ДАИШ использовало в Ираке, пролило свет на то, как были приобретены девять из них. Это расследование началось с установления связи между серийными номерами БАС и некоторыми поставщиками, у которых они были приобретены.

Согласно углубленному анализу программы применения БАС группой ДАИШ, проведенному Центром по борьбе с терроризмом в Вест-Пойнте, «одним из основных выводов из (расследования КАР) была сложность выявления путей получения БАС группой ДАИШ, поскольку семь из девяти коммерческих БАС были приобретены у различных дистрибьюторов, расположенных в пяти государствах, или на веб-сайтах, зарегистрированных в них. (...) Еще одним интересным моментом является многоуровневый характер приобретения «Исламским государством» девяти БАС, поскольку в ряде изученных случаев представленный в свободной продаже БПЛА приобретался в одной стране, проходил активацию в другой, а затем применялся в третьей (в Ираке или Сирии)».

Источник: Ressler 2018



59 КАР — базирующаяся в Соединенном Королевстве организация, специализирующаяся на отслеживании поставок обычного оружия, боеприпасов и сопутствующего военного имущества в районы, затронутые конфликтами.

3.2 Неправительственные субъекты

Сотрудничая с институциональными субъектами в соответствующих сегментах рынка, разработчики программного обеспечения для БАС и производители деталей аппаратного обеспечения и технологий ПБАС могут способствовать тому, чтобы затруднить доступ к БАС и их использованию в террористических целях. С другой стороны, пользователи БАС, операторы уязвимых объектов, общественность и организации гражданского общества в состоянии принять значимые меры по смягчению последствий, проводя целевые информационно-просветительские кампании, правильно применяя комплекс стимулов и формируя надлежащие каналы связи с правоохранительными и другими государственными органами.

3.2.1 Операторы уязвимых объектов

Владельцы уязвимых объектов и лица, управляющие ими, могут предпринять ряд важных действий для защиты своих объектов от риска применения БАС в террористических целях:

- *включить оценки угроз применения БАС и уязвимостей к этим угрозам в планы обеспечения безопасности объекта: для операторов уязвимых объектов крайне важно обеспечить включение конкретных оценок угроз применения БАС и уязвимостей к этим угрозам в общий цикл управления рисками террористической угрозы. Ценные сведения для разработки планов обеспечения безопасности можно получить, рассмотрев, каким образом БАС ранее воздействовали на аналогичные объекты в той же стране или других странах. Уже имевшие место инциденты могут предоставить принципиально важную информацию об угрозах и уязвимостях, позволяющую операторам объектов точно сформировать*

перечень наиболее подходящих мер по смягчению последствий⁶⁰;

- *определить характер и уровень угрозы, воздействующей на объект: все открытые объекты, скорее всего, потребуют принятия мощного комплекса мер по противодействию беспилотным летательным аппаратам, однако объекты, открытый доступ в которые возможен только через отдельные точки (например, окна музея), могут нуждаться только в рассмотрении степени вероятности проникновения дистанционно управляемых БАС по узкому ограниченному маршруту;*
- *отслеживать изменения на рынке БПЛА: знания, которые операторы площадок могут получить о достижениях в области технологий БАС, помогут лучше оценить характер и степень риска. Осведомленность о новых функциях и возможностях любительских или коммерческих БАС по мере их появления на рынке может обеспечивать важную пищу для размышления;*
- *провести отбор наиболее подходящих вариантов обнаружения и снижения риска: при определении наиболее подходящих мероприятий по снижению опасности не существует стандартного универсального решения. Поскольку в настоящее время на рынке представлены сотни различных решений, конечным пользователям часто бывает трудно определить, какие из них в наибольшей степени соответствуют их потребностям. Этот выбор будет зависеть от уникальных рисков, выявленных в конкретной оперативной обстановке, а также от финансовых соображений. В этом контексте необходимо также принимать во внимание наличие в расположенных поблизости районах мест, подходящих для запуска. Точки, с которых оператор с большой долей вероятности сможет управлять БАС, следует*

60 Угрозы, связанные с применением БАС, необходимо рассматривать как потенциально динамичные и далеко не всегда статичные. Планы в области кризисного регулирования должны быть соответствующим образом скорректированы. Например, БПЛА может приземлиться в уязвимой точке определенного объекта и сразу после этого переместиться в другую уязвимую точку того же объекта или даже преследовать большие группы людей во время их эвакуации. Кроме того, при оценке угроз не следует исключать возможность того, что малые БАС могут быть незаконно доставлены на объект и активированы изнутри.

выявлять⁶¹, контролировать и учитывать при составлении планов обеспечения безопасности;

- внедрять нетехнологичные методы противодействия БАС: в большинстве нормативно-правовых систем операторы площадок не имеют полномочий отключать БАС, уничтожать их или перехватывать управление ими⁶². Поэтому им важно понимать, в какой степени использование конкретных технологий противодействия БАС может быть запрещено или ограничено каким-либо иным образом⁶³. В то же время, в зависимости от применимой правовой базы, операторы площадок могут иметь возможность самостоятельно применять целый ряд тактических приемов, призванных снизить эффективность применения БАС без использования технологий противодействия им. К ним относятся следующие приемы:
 - *сокрытие или маскировка уязвимого имущества*: уязвимое имущество может быть полностью или частично укрыто от наблюдения с воздуха с помощью непрозрачных экранов, листвы и т. д. Потенциальные места запуска БАС на прилегающих территориях могут быть сделаны менее привлекательными путем перекрытия обзора с них, применения дополнительной подсветки и мер контроля доступа. Реализация этих мер может потребовать их координации с владельцами или управляющими территориями, на которых расположены точки потенциальных запусков, а также разрешения от этих лиц и организаций (например, муниципалитетов) или их вмешательства;
 - *наблюдение за местами, удобными для запусков*: открытые участки, та-

кие как дворы и крыши, следует регулярно проверять на наличие БАС или доставленных ими предметов. Это обуславливает необходимость активного применения мер по уменьшению угрозы применения БПЛА не только при большом скоплении людей или во время проведения мероприятий. С БАС могут сбрасываться опасные устройства или осуществляться наблюдение в то время, когда целевой объект не используется или закрыт для посещения;

- *анализ в зоне прямой видимости/визуальное обнаружение*: этот метод обнаружения подразумевает наблюдение человеком за видимой линией горизонта для выявления любых БАС, потенциально создающих угрозу. В случае обнаружения БАС на охраняемом объекте или вблизи него важнейшей обязанностью операторов этого объекта становится быстрое оповещение сотрудников службы безопасности и правоохранительных органов. К анализу в зоне прямой видимости следует прибегать не только в случае отсутствия технических средств обнаружения, но и в сочетании с такими средствами ввиду их подверженности ошибкам;
- *средства коммуникации/предупреждения*: в прилегающих районах и транспортных узлах можно размещать предупреждения и объявления с целью информировать/напомнить о запрете полетов БАС над определенными уязвимыми объектами. Подобные меры, вероятно, не отпугнут злоумышленников, однако они, скорее всего, позволят сократить число БАС, запускаемых по незна-

61 Это могут быть дороги с удобными маршрутами отхода, возвышенности, с которых открывается хороший вид на охраняемый объект, парковочные площадки и т. д.

62 Применение технологий, направленных на перехват управления/пресечение полета БАС, может спровоцировать возникновение сложных проблем технического и юридического характера, однако ряд средств обнаружения БАС (например, применение радара) может быть менее проблематичным с этой точки зрения и быть доступным для операторов площадок, пусть часто и ценой существенных расходов. Решения по обнаружению БАС позволяют операторам объектов определять такие критически важные факторы, как скорость, размер, грузоподъемность создающего угрозу объекта и способ управления им. Основываясь на этом, можно сделать выводы относительно, например, степени риска нанесения сопутствующего ущерба людям или имуществу, что, в свою очередь, повлияет на выбор соответствующей меры по уменьшению угрозы.

63 Например, в Соединенных Штатах БАС считаются летательными аппаратами и пользуются такой же защитой, как коммерческие или пассажирские воздушные суда. В результате, согласно федеральному законодательству США, частным организациям и частным лицам, как правило, запрещается вмешиваться в полет БАС, подавляя, например, их сигналы.

нию. В свою очередь, это позволит сотрудникам правоохранительных органов и служб безопасности более эффективно концентрировать ресурсы и внимание на меньшем количестве проблемных событий. В рамках информационно-разъяснительной работы с населением можно также указывать номера телефонов, по которым следует сообщать о подозрительных наблюдениях, и использовать официальные веб-сайты операторов, а также их аккаунты в социальных сетях⁶⁴;

- *повышение возможностей в области обнаружения БАС и обработки информации о них*: персонал объектов можно информировать о том, как оценивать риски, связанные с незаконным использованием БАС в отношении деятельности объектов, а также о том, как визуально обнаруживать инциденты и сообщать о них. Сотрудники также должны пройти подготовку по обращению с подозрительными БАС как во время полета, так и на земле. Например, от обращения персонала объекта с разбившейся БАС зависит, не будет ли поставлено под угрозу последующее расследование и судебная экспертиза, нарушена цепочка обеспечения сохранности доказательств и т. д. (см. раздел 3.1.2.3). В ожидании вмешательства правоохранительных органов персоналу объекта может быть дано указание просто вести фото- или видеосъемку инцидента с БАС;

- *установить партнерские отношения с правоохранительными и другими государственными органами*: при подготовке к проникновению враждебных БАС операторы объектов могут сознавать недостаток имеющихся у них знаний в области методов и приемов борьбы с так называемыми «угрозами нового типа». Поскольку кривая обучения действительно может быть крутой, крайне важно, чтобы эти сотрудники в максимальной степени использовали опыт и знания, накопленные местными органами государственной власти, начиная с ранних этапов процесса планирования в области обеспечения безопасности с целью добиться понимания рисков, трудностей и вариантов смягчения последствий. Кроме того, государственные органы могут предоставлять финансовые средства и субсидии. По одним каналам финансовые средства могут выделяться напрямую на усиление защиты объектов от угроз применения БАС, в по другим — на общее усиление защиты от террористических нападений, включая нападения с применением БАС, но не ограничиваясь ими.

В целом, ожидается, что операторы уязвимых объектов получают значительную выгоду от партнерского сотрудничества с государственными органами в выявлении тех решений по борьбе с активностью враждебных БПЛА, которые будут наилучшим образом соответствовать местным условиям с учетом применимых правовых рамок и бюджетных ограничений.



Программный документ 11.

Заявление о глобальном контексте риска в области авиационной безопасности, документ 10108 - ИКАО

Признавая важность подхода к авиационной безопасности, основанного на оценке рисков, Рабочая группа по угрозам и рискам Группы по авиационной безопасности ИКАО в 2012 году составила первое издание Заявления о контексте риска. Текущее издание Заявления о контексте риска предлагает методологию и механизм предоставления информации для поддержки в государствах — членах ИКАО процессов, направленных на обеспечение национальной и местной авиационной безопасности. В нем также представлен обзор актуальных глобальных угроз авиационной

64 Для размещения предупреждающих знаков и объявлений в тех точках (включая места виртуального размещения), которые не находятся под контролем или управлением операторов объектов, последним будет необходимо связаться с другими землевладельцами, менеджерами сайтов и т. д.



Программный документ 11. (продолжение)

безопасности (включая угрозы, создаваемые применением БАС) и выводы проведенных на высоком уровне глобальных оценок риска, призванных информировать государства о национальных программах обеспечения безопасности полетов воздушных судов гражданской авиации. Наконец, оно используется ИКАО в качестве подспорья для совершенствования и обновления приложения 17 «Стандарты и рекомендуемая практика в области безопасности» и методических материалов.

Рабочая группа по угрозам и рискам обновляет Заявление о контексте риска на ежегодной основе и предоставляет Группе по авиационной безопасности анализ и рекомендации по рискам для авиационной отрасли. Деятельность Рабочей группы по угрозам и рискам зависит от вклада экспертов, а также от эффективного и своевременного предоставления отчетности государствами — членами ИКАО и обмена информацией с ними.

ИКАО рекомендует, чтобы Заявление о контексте риска было доступно тем, кто отвечает за проведение национальных и других оценок рисков в области авиационной безопасности, а также лицам, принимающим решения по авиационной безопасности, специалистам-практикам и другим соответствующим заинтересованным сторонам. Процедуры обработки, передачи и хранения данного документа должны применяться в соответствии с правилами каждого государства-члена в отношении информации, затрагивающей область авиационной безопасности.

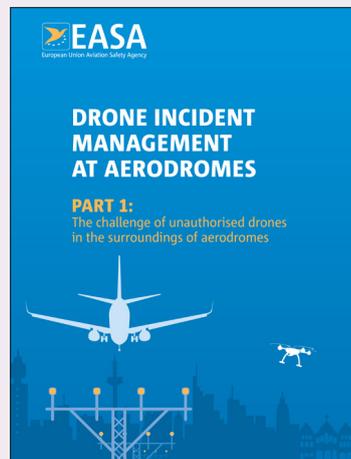
Источник: презентация г-на Сильвена Лефойера, заместителя директора ИКАО по авиационной безопасности и упрощению формальностей на организованном КТУ ООН совещании Группы экспертов (6 и 7 октября 2021 года).



Программный документ 12.

Урегулирование инцидентов с беспилотными летательными аппаратами на аэродромах, Европейское агентство по авиационной безопасности (ЕАСА) 2021 год (www.easa.europa.eu/drone-incident-management-aerodromes-part-1)

В Руководстве ЕАСА содержатся рекомендации по разработке механизмов и процедур, способствующих быстрому, эффективному и соразмерному реагированию на инциденты с применением БАС. Одним из важнейших и необходимых условий нахождения эффективных решений во время чрезвычайных ситуаций является создание совместной рабочей группы с представителями правоохранительных органов, эксплуатантов воздушных судов, авиадиспетчеров и т.д. Документ также нацелен на поиск равновесия между возможностями, которые предоставляют БАС, и обязанностями, возлагаемыми на производителей и операторов БПЛА в отношении безопасности, соблюдения неприкосновенности частной жизни, охраны окружающей среды, защиты от шума и поддержания общественной безопасности.



Это руководство, адресованное всем заинтересованным сторонам, отвечающим за авиационную безопасность и охрану, состоит из трех частей: часть первая – проблема несанкционированного появления БАС в окрестностях аэродромов; часть вторая – указания и рекомендации; часть третья – сборник ресурсов и практических инструментов.

В открытом доступе на сайте ЕАСА находится только первая часть этого руководства. Полный текст Руководства предоставляется субъектам, деятельность которых связана с авиационной отраслью, правоохранительным органам и национальным управлениям гражданской авиации по запросу, направляемому ЕАСА.

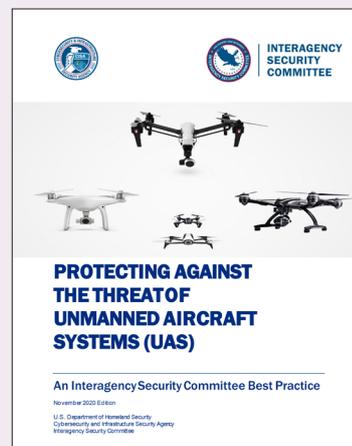


Программный документ 13.

Защита от угрозы со стороны беспилотных авиационных систем: передовая практика Межведомственного комитета безопасности, Межведомственный комитет безопасности, США, 2020 год

(www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf)

В Сборник примеров передовой практики, адресованный специалистам по безопасности, отвечающим за защиту объектов от вредоносных и пилотируемых авиационных систем, включено описание мер по повышению осведомленности и смягчению последствий. В нем рассматриваются следующие темы: обзор БАС и угроз, исходящих от них, оценка уязвимости, защитные меры и мероприятия, разработка плана реагирования объекта на инциденты с участием БАС, повышение осведомленности персонала и взаимодействие с партнерами из числа представителей местного населения.



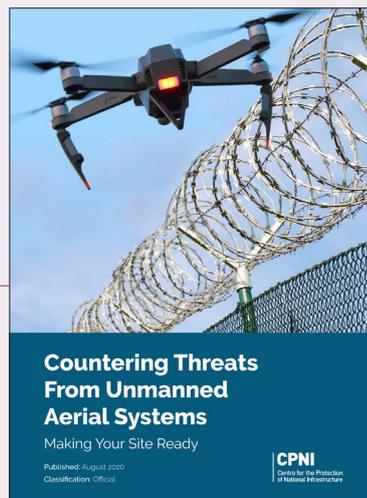


Программный документ 14.

Противодействие угрозам со стороны беспилотных авиационных систем: обеспечение готовности вашего объекта, Центр защиты национальной инфраструктуры, Соединенное Королевство, 2020 год
(www.cpni.gov.uk/system/files/documents/40/14/cuas-branded-doc-public-V4.1.pdf)

Данный документ представляет собой введение в разработку стратегии и плана противодействия беспилотным авиационным системам для конкретного объекта.

В документе обсуждается ряд контрмер, которые может принять объект для уменьшения опасности, исходящей от создающих угрозу БАС, в том числе: снижение интенсивности использования БАС по незнанию или халатности, повышение эффективности физической защиты, введение в технические возможности и разработка эффективных оперативных мер реагирования.



3.2.2 Производители БАС и важнейших подсистем

Динамика бурно развивающегося рынка и устойчивый спрос на коммерческие и любительские беспилотные авиационные системы подталкивают производителей БАС и их важнейших подсистем к постоянному совершенствованию своей продукции путем повышения ее производительности и удобства пользования ею. Действуя в соответствии с рыночной логикой и стремясь превзойти своих конкурентов, производители БАС должны использовать все доступные технологические инновации, чтобы сделать свою продукцию менее подходящей для использования враждебно настроенными субъектами. В настоящее время для этой цели используются механизмы, которые можно разделить на две основные группы.

- *Применение функции геозонирования:* это базовая функция безопасности, обеспечивающая невозможность эксплуатации БАС в воздушном пространстве над определенными зонами, такими как аэропорты, пенитенциарные учреждения, электростанции и т. д. Программное обеспечение, поддерживающее функции геозонирования, легко обновляется в зависимости от изменений в местных условиях. Например, система может получать указания не осу-

ществлять полеты над тем или иным участком, где происходит или должно произойти разовое событие с присутствием большого количества людей. Геозонирование не является универсальным средством. Вполне очевидна его уязвимость к взлому, и даже самая эффективная и труднокорректируемая функция вполне может быть обойдена при использовании БПЛА, изготовленного по индивидуальному заказу. Тем не менее геозонирование можно назвать важным передним краем обороны в борьбе против вредоносной деятельности, осуществляемой слабо подготовленными субъектами или злоумышленниками, не располагающими достаточным временем или значительным кибернетическим потенциалом.

- *Передача идентификационной информации, получаемой от БАС:* Производители БАС постоянно экспериментируют с технологией передачи идентификационной информации о БАС по радио. Как и регистрационный знак автомобиля, идентификационный код, передаваемый БАС, помогает принимающим его сотрудникам служб безопасности и правоохранительных органов отличать БАС, функционирующие законно, от тех систем, функционирование которых законным не является. Хотя передача данных идентификации беспилотных

летательных аппаратов не даст убедительных доказательств того, какой летающий объект представляет опасность, а какой нет, она может помочь в ранжировании угроз и, соответственно, способствовать процессам принятия решений в сжатые сроки.

Одной из основных проблем, связанных с рядом технологических решений в области безопасности, является зависимость их применения от конкретного производителя. Риск заключается в создании фрагмен-

тированной среды, в которой различные технологии работают только с определенными моделями или марками БАС. Это очевидно подчеркивает необходимость того, чтобы производители БАС внедряли такие решения в тесной координации не только с государственными органами, но и — что особенно важно — с другими производителями подобных систем, с тем чтобы в максимальной степени обеспечить применение общих стандартов и протоколов, а также подходов, учитывающих вопросы соблюдения прав человека.



Вставка 13.

Производители БАС и решения, использующие технологию геозонирования

Один из ведущих производителей беспилотных авиационных систем в 2013 году впервые создал для своих БАС функцию «Бесполетные зоны», а три года спустя представил свою систему геозонирования, добавив обновления в режиме реального времени и ввод новых запретных районов. Получая сигналы навигационных спутников, система в автоматическом режиме не позволяет БАС совершать полеты вблизи мест ограниченного доступа, таких как аэропорты, тюрьмы, атомные электростанции и места проведения широко освещаемых мероприятий. В некоторых местах БАС не может взлетать на территории, защищенной системой геозонирования, или проникать в такую зону. Пилоты БАС, имеющие подтвержденные учетные записи в приложении DJI, при наличии у них законных оснований и необходимых разрешений могут направлять свои беспилотные аппараты в определенные закрытые зоны, но для разблокировки зон с более жесткими ограничениями по доступу требуются дополнительные шаги. В соответствии с процедурой утверждения, подав онлайн-заявку, профессиональные операторы БАС, имеющие разрешение на совершение полетов в особо защищенных зонах, могут получить коды разблокировки в течение 30 минут.

Источник: www.dji.com/newsroom/news/dji-refines-geofencing-to-enhance-airport-safety-clarify-restrictions.



Производители беспилотных авиационных систем не только сдерживают незаконное применение БАС путем интеграции самых передовых технологических решений в свои новые устройства, но и являются важнейшими участниками обмена технической информацией о будущих продуктах с регулирующими государственными органами⁶⁵. Получая заблаговременное уведомление о проектах, находящихся в стадии разработки, государственные организации — и в конечном итоге операторы уязвимых объектов — будут обладать более широкими возможностями для прогнозирования угроз и подготовки более точных планов

по смягчению и ликвидации последствий. В то же время любой канал или механизм обмена информацией между частным и государственным секторами в этой области должен будет гарантировать участникам надлежащий уровень конфиденциальности. Эффективность обмена информацией будет зависеть от гарантий соблюдения прав на интеллектуальную собственность и сохранения коммерческой тайны, с тем чтобы передаваемая конфиденциальная информация не попала к конкурентам и не обеспечила им тем самым несправедливое преимущество.



Конкретный пример 13.

Отраслевая ассоциация коммерческой беспилотной авиации южной части Африки

Эта ассоциация, изначально созданная для поддержки своих членов в получении надежной правовой основы для их деятельности в ожидании появления новой правовой базы применения БАС в южной части Африке, стремится служить интересам отрасли коммерческих дистанционно пилотируемых летательных аппаратов, поощрять и продвигать их применение, обеспечивать соответствующий надзор и осуществлять взаимную защиту этих интересов. В число членов ассоциации входит ряд компаний-производителей высокотехнологичной продукции и продавцы таких товаров, поставщики БПЛА и соответствующих юридических услуг, а также поставщик курсов по подготовке пилотов БПЛА. Ассоциация выступает в качестве связующего звена между этой отраслью и соответствующими органами государственной власти в регионе юга Африки, и ее мандат предусматривает оказание помощи ее членам в совершенствовании системы безопасности, повышении стандартов деятельности и подготовке ее членов к принятию новой правовой базы.

Вступая в эту ассоциацию, ее члены обязуются:

- вести деятельность в области применения дистанционно пилотируемых летательных аппаратов законно, этично, профессионально и, в применимых случаях, в соответствии с разрешениями, регулирующими использование воздушного пространства, в котором участник осуществляет свои полеты;
- поддерживать и продолжать развитие отрасли и самой Ассоциации;
- сообщать о происшествиях в полицию, Управление гражданской авиации или соответствующий отраслевой орган, с тем чтобы содействовать развитию отрасли в правильном направлении.

Члены Ассоциации должны признавать и соблюдать кодекс поведения, который представляет собой набор руководящих принципов и рекомендаций, направленных на обеспечение безопасности полетов дистанционно управляемых летательных аппаратов и на обеспечение неинтрузивного характера этих полетов. Кодекс поведения сформулирован на основе принципов безопасности, профессионализма и уважения и обязывает уважать права других пользователей воздушного пространства, неприкосновенность частной жизни отдельных лиц и обеспокоенность

⁶⁵ В Берлинском меморандуме правительствам эта мера включена в число прочих мер, которые правительствам предлагается принять в целях установления и укрепления координации с отраслевым частным сектором и другими нетрадиционными заинтересованными сторонами (GCTF 2019, Good Practice 14).



общественности в связи с эксплуатацией беспилотных летательных аппаратов. Целью принятия данного кодекса является также предоставление производителям и пользователям контрольного перечня операций и средств демонстрации их приверженности безопасному и ответственному развитию отрасли.

Источник: <https://cuaasa.wixsite.com/cuaasa>



Конкретный пример 14.

Группа по деятельности в отрасли беспилотной авиации
(www.arpas.uk/drone-iag/)

Группа по деятельности в отрасли беспилотной авиации – это многосторонняя площадка, на которой заинтересованные стороны отрасли беспилотной авиации объединяются для взаимодействия с правительственными учреждениями, а также научными кругами, исследовательскими и технологическими бюро, регулирующими органами, инвесторами и конечными пользователями. Целью этого объединения является достижение понимания возможностей и проблем сектора, а также формулирование программы действий, необходимых для решения и преодоления этих проблем. От членов Группы ожидается активное участие в реализации ее важнейших целей:

- поддерживать инновации и сотрудничество, способствующее росту коммерческого применения БПЛА и более широкому использованию беспилотных технологий и решений в Соединенном Королевстве;
- содействовать встраиванию БАС в процессы решения широкого круга задач в государственном и частном секторах Соединенного Королевства, а также надзору за их применением, его анализу и внесению в соответствующие стандарты;
- развивать возможности для внедрения БАС и способствовать координации, сотрудничеству и использованию в Соединенном Королевстве технологий и системы управления воздушным движением, распространяющейся и на БАС, и на более широкую категорию летательных аппаратов общего назначения;

Конкретный пример 14. (продолжение)

- обеспечивать возможность участия отрасли в работе правительства и в создании структуры, деятельность которой будет направлена на смягчение последствий неправомерного применения БАС и преодоление обеспокоенности общества;
- обеспечивать соблюдение прав других пользователей воздушного пространства;
- обеспечивать соблюдение права людей на неприкосновенность частной жизни;
- уважительно относиться к обеспокоенности общественности в связи с эксплуатацией беспилотных летательных аппаратов.

В настоящее время в структуру Группы входят следующие рабочие группы:

- по примерам безопасного применения: разработка возможных улучшений принятой в Управлении гражданской авиации процедуры оценки рисков;
- по пространству развития: решение трудностей, связанных с тестированием новых или сложных приложений;
- по общественному и коммерческому восприятию: решение вопросов, связанных с отношением общественности и способами повышения осведомленности об услугах БПЛА в соответствующих секторах.



Конкретный пример 15.

Выявление уязвимостей: программа «Отлов багов»

Один из ведущих производителей БПЛА реализует программу выявления ошибок в программном обеспечении, в рамках которой сторонним исследователям систем безопасности предлагается внести свой вклад в укрепление безопасности данных путем активного поиска уязвимостей в существующей системе и оповещения о них. Для того чтобы получить право на участие в программе, необходимо соответствовать ряду требований, таких как: самому не быть автором соответствующей уязвимости, не подвергать какой-либо опасности полеты в воздушном пространстве общего пользования, не использовать и не эксплуатировать найденную уязвимость по каким бы то ни было причинам в целях дальнейшего исследования вопросов, связанных с безопасностью. Соответствующие требованиям участники могут получить денежное вознаграждение, рассчитанное на основе предварительно оцененной опасности и тяжести воздействия выявленной уязвимости.

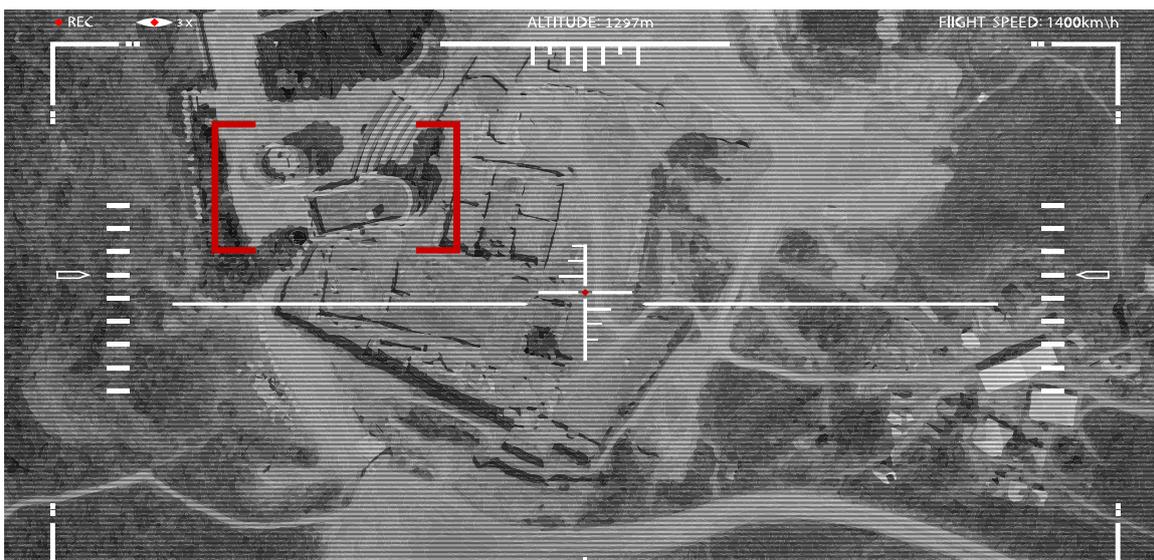
Источник: https://security.dji.com/policy?lang=en_US.

3.2.3 Поставщики и розничные торговцы БАС

Являясь самым близким к потребителям звеном экосистемы БАС, поставщики и розничные продавцы часто находятся в привилегированном положении в отношении формирования восприятия пользователей, предоставления им четкой и удобной в применении информации, касающейся вопросов безопасности и защиты, а также применимых законов и правил. Магазины и веб-сайты поставщиков могут, при наличии соответствующих материалов, распространять и демонстрировать выпущенные государственными

органами листовки, баннеры и другие официально представленные к ознакомлению материалы по теме безопасности.

Поставщики и розничные продавцы БАС могут внести значительный вклад в работу по предотвращению попадания БАС и соответствующего оборудования в руки враждебно настроенных субъектов. Нормативно-правовая база некоторых стран уже может требовать от поставщиков и розничных продавцов принятия мер должной осмотрительности в этом отношении, в том числе путем проверки личности потенциальных клиентов и ведения архивов совершенных сделок.



Вставка 14

Сигналы опасности и отсутствие должной осмотрительности в деле группы компаний АйБАКС

Случай с группой компаний АйБАКС связан с покупкой нескольких БАС компаниями, связанными с ДАИШ. Этот случай показывает, как законно работавшие компании, участвовавшие в этих сделках, могли не допустить поставки товаров, имеющих отношение к БАС, группе ДАИШ, просто проведя элементарную проверку в соответствии с принципом «знай своего клиента». Действительно, эти сделки проходили в довольно необычных обстоятельствах, которые немедленно должны были вызвать подозрения. Странными были следующие моменты:

- характер приобретаемых предметов (БПЛА, дистанционно управляемый самолет, компоненты ракеты, оборудование для контрнаблюдения);
- адреса доставки приобретенных товаров (недалеко от границ территории, которую на тот момент контролировала группа ДАИШ);
- период покупки (именно в это время ДАИШ были посвящены первые страницы мировых СМИ);

Возможно, «эта ситуация (...) заставляет задаться рядом важных вопросов о внутренней проверке закупок в этих конкретных компаниях и/или о политике (...), применяемой розничными продавцами для выявления и предотвращения подозрительных сделок, а также об очевидном отсутствии правил осуществления контроля за распределением такого рода компонентов, особенно когда товары должны быть доставлены в места, непосредственно прилегающие к зонам активных военных действий». Кроме того, «перечень покупок этой сети привлекает внимание к еще одной проблеме, которая, по всей видимости, должна была вызвать тревогу или способствовать более тщательному изучению совершаемых покупок: количество приобретаемых товаров или количество транзакций, совершенных в течение короткого периода времени». Например, в какой-то момент «один из участников этой незаконной сделки последовательно совершил 11 покупок одной и той же партии товаров в один и тот же день у одной и той же компании, используя разные имена, причем все товары должны были быть доставлены в одно и то же место, а в общей сложности за один день были проданы запчасти для беспилотных летательных аппаратов на сумму более 16 000 долларов».

Источник: Rassler, 2018.



Конкретный пример 16.

Программа сертификации «БАС-сейф» (UASafe) для розничных продавцов БАС в Великобритании

Число покупок беспилотных летательных аппаратов растет год от года, и эта инициатива была направлена на стимулирование более безопасного применения БАС и улучшение информированности людей о том, когда, где и как они могут безопасно их использовать. В рамках этой программы, которая реализовывалась до 2021 года, пользователям было рекомендовано обращать внимание на наличие символа UASafe, чтобы убедиться в том, что они совершают покупки у надежного и ответственного поставщика. Чтобы получить сертификат программы «БАС-сейф», розничные продавцы должны были декларировать, что они выполняют следующие условия:

- предоставление клиентам копии программного обеспечения Dronocode в упаковке с любым БПЛА с весом более 250 г;
- в качестве альтернативы диск с программами Dronocode должен быть предоставлен покупателю в месте продажи;
- проведение наглядной демонстрации программ Dronocode в магазине;
- предоставление клиентам четких рекомендаций по соблюдению требований платформы Dronocode;
- добавление ссылок на сайт UASafe.uk на страницы онлайн-продуктов для беспилотных летательных аппаратов.

Наконец, в штате каждого магазина должен был состоять сотрудник, обладающий знаниями в этой области и способный отвечать на вопросы покупателей и обучать коллег.

Розничные продавцы могли подать заявку на участие в этой инициативе, сообщив Управлению гражданской авиации о том, что они отвечают вышеуказанным критериям. После получения заявки Управление гражданской авиации связывалось с розничными продавцами, чтобы подтвердить, могут ли они впоследствии использовать знак одобрения программы UASafe.



3.2.4 Поставщики технологий противодействия БАС

Поставщики решений в области противодействия БАС проектируют и разрабатывают технологии обнаружения, идентификации, отслеживания и отключения/пресечения незаконных действий с применением БАС для использования уполномоченными субъектами в соответствии с национальной законодательной базой каждой страны. Такие технологии активно используются для защиты уязвимых объектов по всему миру. Например, во время чемпионата мира по футболу 2018 года в России власти и силы безопасности развернули системы противодействия БАС на месте проведения игр для отражения возможных нападений с применением БПЛА. Другая система противодействия БАС была размещена для защиты высокопоставленных лиц и инфраструктуры на саммите, проходившем в Буэнос-Айресе в 2018 году⁶⁶.

Для поставщиков решений по противодействию БАС важно наладить очень тесное

взаимодействие с органами государственной власти и охраны правопорядка, которые в конечном итоге будут использовать эти технологии. Совместные усилия крайне необходимы для того, чтобы заинтересованные стороны отрасли оперативно оповещались об изменениях в постоянно корректируемых правовых нормах и последовательно развивали/адаптировали свои технологии, направленные на устранение новых и возникающих угроз, связанных с применением БАС, а также обеспечивали разработку решений, соответствующих принципам соблюдения прав человека.

3.2.5 Пользователи БАС

Число конечных пользователей продуктов и услуг, связанных с БАС, растет в геометрической прогрессии вследствие того, что все новые частные лица, компании и организации внедряют технологии БАС для достижения различных рекреационных, коммерческих и других профессиональных целей⁶⁷. Во всех случаях операторы БАС несут основную ответственность за обращение со своими устройствами



66 Эта система оснащена трехмерным радаром, работающим в X-диапазоне и предназначенным для обнаружения потенциально опасных объектов, оптоэлектронной/инфракрасной камерой для их классификации и излучателем помех для вывода их из строя.

67 В эту категорию заинтересованных сторон входят организации, владеющие парком БАС и осуществляющие полеты для выполнения проектов по заказу своих клиентов, реализуя тем самым новую бизнес-модель, известную как «БАС как услуга» (см. вставку 15).

в полном соответствии со стандартами безопасности и охраны и действующими правовыми требованиями. Это относится и к действиям, направленным на регистрацию беспилотных систем, получение необходимых лицензий и прохождение необходимых испытаний.

С одной стороны, соблюдение требований операторами БАС снижает риск создания угрозы для людей и имущества и ограничивает масштаб их персональной ответственности. С другой стороны, формирование сообщества ответственных конечных пользователей гарантирует снижение числа случаев использования БАС в воздушном пространстве ограниченного доступа по халатности. Это, в свою очередь, позволяет правоохранительным органам и сотрудникам служб безопасности, включая тех, кто занимается защитой уязвимых объектов, направлять ограниченные ресурсы и возможности обнаружения на более узкий круг происшествий с БАС, потенциально создающих угрозу.

Пользователи также могут значительно снизить риск перехвата их устройств или их переадресации каким-либо иным образом. Во многих случаях важнейшие действия по преодолению рисков сводятся к соблюдению основных норм кибербезопасности, таких как регулярное обновление программного обеспечения БАС, выбор надежных паролей, снижение уязвимости наземных устройств управления, в том числе смартфонов и ноутбуков, к воздействию вредоносного программного обеспечения, а также использование доступа через виртуальную частную сеть (VPN) для предотвращения доступа хакеров к интернет-соединениям⁶⁸. Кроме того, оснащение БАС функцией возврата к дому (RTH), позволяет пользователю вернуть такую систему в случае угона, поскольку устройство будет автоматически возвращаться в точку запуска в случае потери сигнала управления или его глушения⁶⁹ (Kaspersky 2021).



Вставка 15. «БАС как услуга»

В последние годы некоторые государственные учреждения начали прибегать к услугам частных компаний в вопросе развертывания БАС высокой сложности для выполнения задач по наблюдению и осуществлению контроля. Концепция «БАС как услуга» представляет собой новый аспект государственно-частного партнерства в экосистеме применения БАС. Подкрепленная нормативно-правовой базой, соответствующей этически и юридически обоснованным принципам, она позволяет органам государственной власти сосредоточиться на результатах, а не на средствах их достижения, использовать в каждом конкретном случае наиболее подходящие ресурсы и применять при заключении контрактов гибкие условия, соответствующие операционной гибкости организаций, предоставляющих данную услугу⁷⁰.

Эта концепция может быть особенно интересна тем правоохранительным органам, которые недостаточно хорошо оснащены современными технологиями, использующими БАС, или не обладают соответствующими техническими навыками для работы с ними. Кроме того, ее применение может покрыть потребности тех стран, ограниченные финансовые возможности которых не позволяют приобретать БАС, применять их и нести расходы на управление собственным парком таких систем.

68 Виртуальная частная сеть (VPN) функционирует как безопасный шлюз в Интернет, шифруя соединение.

69 Поскольку возвращение в точку запуска (RTH) происходит на основании данных GPS-навигации, эта функция может не работать в случае «подмены GPS», то есть если GPS-трекер устройства обманным путем заставляют думать, что устройство находится в другом месте.

70 Например, модель «БАС как услуга» была использована Министерством внутренних дел Соединенного Королевства в качестве важнейшего инструмента предотвращения нелегальной миграции и незаконного рыболовного промысла.

3.2.6 Пользователи уязвимых объектов

На основе четких и простых указаний сотрудников правоохранительных органов и/или служб безопасности, посетители туристических достопримечательностей, зрители мероприятий, проводимых под открытым небом, и т. д. могут играть важную роль в устранении угроз, связанных с применением БАС, воздействующими на уязвимые объекты. Например, некоторые из этих объектов могут быть не оборудованы технологиями противодействия беспилотным авиационным системам, направленными на обнаружение угрожающих БАС. На других объектах могут применяться технологические решения, которые при определенном освещении или в определенных условиях оказываются ограниченно применимыми или недостаточно эффективными. Во всех этих случаях готовность общественности в целом выявлять тревожные ситуации и сообщать о них может стать важнейшим ресурсом в рамках многоуровневой среды обеспечения безопасности.

3.2.7 Организации гражданского общества (ОГО)

Организации гражданского общества могут использовать свое положение, совершенствуя связи между общественностью и органами власти, отвечающими за вопросы безопасности и защиты в связи с применением БПЛА. Например, они могут

выступать посредниками в деле доведения до сведения общественности информации о нормативно-правовой базе и государственной политике в отношении угроз, связанных с применением БПЛА, и предотвращения этих угроз. Кроме того, независимые низовые организации могут играть важную роль в эффективном формулировании обеспокоенности и идей гражданского общества и их перенаправлении в директивные, регулирующие и правоохранительные органы. Также эти организации могут стать источником ценных предложений или рекомендаций по важнейшим проблемам, волнующим данное сообщество, в том числе по укреплению прав человека в условиях применения рассматриваемых систем. Вклад ОГО может быть востребован на различных этапах процессов разработки стратегии и правовой базы, включая оценку компромиссов и рисков, процесс разработки и распространения правил.

ОГО могут не только выступать в качестве средства обеспечения коммуникации, но и принимать участие в материальной поддержке усилий по восстановлению и по предоставлению лицам, пострадавшим от террористических нападений с применением БАС, помощи, в том числе юридической помощи, направленной на защиту прав жертв. Некоторые ОГО активно используют БАС в качестве вспомогательных инструментов в кризисных ситуациях, вне зависимости от того, применялись ли БАС в том или ином инциденте (см. конкретный пример 17).





Конкретный пример 17.

«БАС без границ» (www.droneswithoutborders.org/)

Организация «БАС без границ» — это основанная в 2019 году неправительственная организация, миссия которой заключается в использовании технологии БАС для предоставления услуг по выполнению технического мониторинга и передачи в режиме реального времени информации, адресованной специалистам по ликвидации последствий чрезвычайных ситуаций и стихийных бедствий и другим партнерам на местах в процессе реализации мер реагирования на кризисы как природного, так и антропогенного характера.

Организация «БАС без границ» реализует свою миссию в рамках трех оперативных блоков — оценка воздействия, учет потребностей и проведение информационно-пропагандистских мероприятий в гуманитарной области — и принимает участие в осуществлении усилий по урегулированию кризисов и восстановлению от их последствий, уделяя при этом особое внимание уязвимым лицам, пострадавшим в результате чрезвычайных ситуаций.



Справочные материалы

Association of the United States Army, 2021. The Role of Drones in Future Terrorist Attacks (www.ausa.org/publications/role-drones-future-terrorist-attacks#).

Canada, Department of Transport (Transport Canada), 2021. Transport Canada's Drone Strategy to 2025 (<https://tc.canada.ca/en/aviation/publications/transport-canada-s-drone-strategy-2025>).

Europol, 2021. European Union Terrorism Situation and Trend Report (www.europol.europa.eu/tesat-report).

Global Counterterrorism Forum (GCTF), 2019. Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems (www.thegctf.org/LinkClick.aspx?fileticket=j5gj4fSJ4fl%3D&portalid=1).

Kaspersky, 2021. Security and drones: what you need to know (www.kaspersky.com/resource-center/threats/can-drones-be-hacked).

Ley Best, Katharina and others, 2020. *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools*, Rand Corporation (www.rand.org/pubs/research_reports/RR2972.html).

Moore, Jack, 2016. Rio Olympics: Al-Qaeda Jihadis Call for Attacks on American, British, French and Israeli Athletes, *Newsweek*, 22 July 2016 (www.newsweek.com/al-qaeda-jihadis-call-attacks-american-british-french-israeli-athletes-rio-483145).

Palestini, Claudio, 2020. Countering drones: looking for the silver bullet, *NATO Review* (www.nato.int/docu/review/articles/2020/12/16/countering-drones-looking-for-the-silver-bullet/index.html).

Rassler, Don, 2016. Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology, Combating Terrorism Center at West Point (www.jstor.org/stable/resrep05632).

_____, 2018. Islamic State and Drones: Supply, Scale and Future Threats, Combating Terrorism Centre at West Point (<https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf>).

Staniforth, Andrew, 2017. Attack of the drones: Emerging threats from Unmanned Aerial Vehicles, TRENDS Research & Advisory (<https://trendsresearch.org/insight/attack-of-the-drones-emerging-threats-from-unmanned-aerial-vehicles/>).

United Kingdom Home Office, 2018. Stop and Search: Extending police powers to cover offences relating to unmanned aircraft (drones), laser pointers and corrosive substances: Government consultation (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/739629/06_09_18_Stop_and_Search_Consultation_Document_.pdf).

_____, 2019. UK Counter-Unmanned Aircraft Strategy (www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy).

Совет Безопасности Организации Объединенных Наций, Заключительный доклад Группы экспертов по Ливии, учрежденной в соответствии с резолюцией 1973 (2011), 8 марта 2021 года, URL: www.un.org/securitycouncil/sanctions/1970/panel-experts/reports.

United States Department of Defense, 2021. Counter-Small Unmanned Aircraft Systems Strategy (<https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf>).

Дополнительная информация представлена на веб-сайте:
www.un.org/counterterrorism/vulnerable-targets

