

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ,
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056

DOI: 10.17212/2782-2230-2024-3-63-77

БПЛА КАК КИБЕРФИЗИЧЕСКАЯ СИСТЕМА*

Е.А. ВАСИЛЬЕВ¹, Е.С. АБРАМОВ²

¹ 347922, РФ, г. Таганрог, ул. Чехова, 2, Институт компьютерных технологий и информационной безопасности ИТА ЮФУ, аспирант кафедры безопасности информационных технологий. E-mail: evva@sfedu.ru

² 347922, РФ, г. Таганрог, ул. Чехова, 2, Институт компьютерных технологий и информационной безопасности ИТА ЮФУ, заведующий кафедрой безопасности информационных технологий. E-mail: abramoves@sfedu.ru

В настоящее время ученое сообщество дает нам отдельные определения беспилотных летательных аппаратов (БПЛА) и киберфизических систем. Эти определения полностью самодостаточны и не пересекаются между собой. Однако технический прогресс не стоит на месте, и узость данных определений не позволяет исследователям в полной мере применять некоторые определения из-за проблем в терминологии. Настоящая статья позволит преодолеть имеющиеся разногласия в терминологии и переносить свойства киберфизических систем на беспилотные летательные аппараты.

Ключевые слова: БПЛА, киберфизическая система, концептуальная модель, модели угроз, модели атак, модель kill-chain для КФС, уязвимости БПЛА, негативные последствия

ВВЕДЕНИЕ

В 2006 г. Хелен Джилл ввела термин для обозначения комплексов, состоящих из природных объектов, искусственных подсистем и контроллеров, – «киберфизические системы» [5].

Киберфизическая система (КФС) – это система, основанная на интеграции вычислений с физическими процессами. Встраиваемые компьютеры совместно с сетями осуществляют мониторинг и контроль за физическими процессами обычно путем передачи данных через узлы системы, где физические процессы влияют на вычисления, и наоборот. Это означает, что КФС может быть

* Статья получена 18 августа 2024 г.

определена как система, которая выполняет функции сбора, хранения, анализа, обработки и предоставления данных от устройств, взаимодействующих с физическими процессами и объектами, а также их тесную интеграцию с информационными технологиями в рамках надежной среды передачи данных.

1. ОПИСАНИЕ И КЛАССИФИКАЦИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Беспилотные летательные аппараты – это летательные аппараты, представляющие собой автономные роботизированные системы, задачей которых является выполнение полетов, потенциально опасных для человека, по заранее заданной программе с возможностью автоматической или ручной корректировки полетного задания, а также оперативное принятие решений в зависимости от меняющихся условий полета и окружающего пространства [1].

В наши дни классификация беспилотных летательных аппаратов (или дронов) в России ведется в соответствии с ГОСТ Р 59517–2021 «Беспилотные авиационные системы. Классификация и категоризация» [2]. Этот стандарт позволяет классифицировать БПЛА по четырем параметрам и разделяет их на три категории.

Однако в вопросах компоновки БПЛА производители не ограничены никакими стандартами, в результате чего отсутствуют требования к оснащению БПЛА со стороны авиационных регуляторов. Возможно это связано с тем, что БПЛА уже имеют множество конфигураций, аэродинамических схем и их компонентов, а также с тем, что внедрение жестких стандартов и классификаций может ограничить развитие технологий БПЛА.

Таким образом, на основании ГОСТ Р 59517–2021 БПЛА могут классифицироваться по следующим параметрам:

- 1) максимальная взлетная масса;
- 2) достигаемая в полете кинетическая энергия;
- 3) эксплуатационное назначение;
- 4) условия видимости.

Беспилотные летательные аппараты разделяются на три категории:

- 1) открытая категория (А);
- 2) специальная категория (В);
- 3) сертифицируемая категория (С).

Согласно российской классификации БПЛА можно систематизировать следующим образом [3]:

– микро- и мини-БПЛА ближнего радиуса действия (взлетная масса до 5 кг, дальность действия 25...40 км);

- легкие БПЛА малого радиуса действия (взлетная масса 5...50 кг, дальность действия 10...70 км);
- легкие БПЛА среднего радиуса действия (взлетная масса 50...100 кг, дальность действия 70...150 (250) км);
- средние БПЛА (взлетная масса 100...300 кг, дальность действия 150...1000 км);
- среднетяжелые БПЛА (взлетная масса 300...500 кг, дальность действия 70...300 км);
- тяжелые БПЛА среднего радиуса действия (взлетная масса более 500 кг, дальность действия 70...300 км);
- тяжелые БПЛА большой продолжительности полета (взлетная масса более 1500 кг, дальность действия около 1500 км);
- беспилотные боевые самолеты (взлетная масса более 500 кг, дальность действия около 1500 км).

Международной ассоциацией по беспилотным системам AUVSI (Association for Unmanned Vehicle Systems International) была предложена универсальная классификация БПЛА, которая объединяет в себе вышеназванные критерии [4].

Универсальная классификация БПЛА по летным параметрам

Universal classification of UAVs by flight parameters

Универсальная классификация БПЛА по летным параметрам						
Группа	Категория		Взлетная масса, кг	Дальность полета, км	Высота полета, м	Продолжительность полета, ч
	рус.	англ.				
Малые БПЛА	НаноБПЛА	Nano	< 0,025	< 1	100	1
	МикроБПЛА	Micro	< 5	< 10	250	1
	Мини-БПЛА	Mini	5...150	< 10	150...300	< 2
Тактиче-ские	Легкие БПЛА для контроля переднего края обороны	Close Range (CR)	25...150	10...30	3000	2...4
	Легкие БПЛА с малой дальностью полета	Short Range (SR)	50...250	30...70	3000	3...6

Продолжение таблицы
Continuation of the Table

Универсальная классификация БПЛА по летным параметрам						
Группа	Категория		Взлетная масса, кг	Дальность полета, км	Высота полета, м	Продолжительность полета, ч
	рус.	англ.				
	Средние БПЛА	Medium Range (MR)	150...500	70...200	5000	6...10
	Средние БПЛА с большой продолжительностью полета	Medium Range Endurance (MRE)	500...1500	>500	8000	10...18
	Маловысотные БПЛА для проникновения в глубину обороны	Low Altitude Deep Penetration (LADP)	250...2500	>250	50...9000	0,5...1
	Маловысотные БПЛА с большой продолжительностью полета	Low Altitude Long Endurance (LALE)	15...25	>500	3000	>24
	Средневысотные БПЛА с большой продолжительностью полета	Medium Altitude Long Endurance (MALE)	1000...1500	>500	5000...8000	24...48
Стратегические	Высотные БПЛА с большой продолжительностью полета	High Altitude Long Endurance (HALE)	2500...5000	>2000	20 000	24...48
Спецназначение	БПЛА, оснащенные ударной частью	Lethal (LET) (Offensive)	—	300	4000	3...4
	БПЛА – ложные цели	Decoys (DEC)	150...500	0...500	50...5000	<4

Окончание таблицы

End of the Table

Универсальная классификация БПЛА по летным параметрам						
Группа	Категория		Взлетная масса, кг	Дальность полета, км	Высота полета, м	Продолжительность полета, ч
	рус.	англ.				
	Стратосферные БПЛА	Stratospheric (STRA)	>2500	>2000	>20 000	>48
	Экзостратосферные БПЛА	Exo-stratospheric (EXO)	–	–	>30 500	–

Российская классификация отличается от предложенной UVS International по ряду параметров: некоторые классы зарубежной классификации отсутствуют в РФ, легкие БПЛА в России имеют значительно большую дальность и т. д.

2. БАЗОВЫЕ СИСТЕМЫ БПЛА

Технологии развития БПЛА находятся на стыке прикладных наук и высокотехнологичных отраслей. Создание аэродинамических схем летательных аппаратов, разработка специальных материалов для изготовления конструкций фюзеляжа, изготовление нанотехнологичных процессоров, сенсоров – все эти направления должны слаженно работать, чтобы создаваемые БПЛА могли отвечать всем предъявляемым к ним требованиям. В настоящее время уровни технологического и промышленного развития, материаловедения, а также развития цифровых технологий позволили создавать автономные высокоточные БПЛА с высокими летно-техническими и массогабаритными характеристиками. При изготовлении БПЛА используются композитные материалы, которые позволяют значительно повысить маневренность и прочность, уменьшить вес производимого БПЛА, способствуют поглощению вибраций и уменьшению производимого уровня шума при полете. Характеристики материалов, из которых создаются БПЛА, при различных параметрах окружающей среды позволяют БПЛА совершать полеты на больших высотах и с высоким уровнем перегрузки практически в любую погоду. Основным и самым высокотехнологичным элементом системы БПЛА является электронная система управления.

Электронная система управления любого БПЛА состоит из вычислительной мощности и сенсоров, включающих в себя следующее:

- 1) процессор с модулями оперативной и энергонезависимой памяти, необходимые для функционирования систем БПЛА;
- 2) модуль определения положения в пространстве, состоящий из многоосевых MEMS-сенсоров, таких как магнетометры, акселерометры, гироскопы и т. д.;
- 3) модуль аналоговых или цифровых барометрических датчиков для определения высоты и воздушной скорости;
- 4) модуль управления двигателями и энергоснабжением;
- 5) модуль управления сервоприводами для управления полетом и режимами двигателей;
- 6) модуль приема спутниковой навигации GPS для точного геопозиционирования;
- 7) модуль радиосвязи для ручного управления и передачи данных телеметрии.

Систему управления БПЛА также могут дополнять другие системы, например:

- радиолокационные системы;
- лидары;
- ультразвуковые датчики расстояний;
- системы стабилизации фото- и видеоборудования.

Устройство стандартного БПЛА вертолетного типа (квадрокоптер) и его основные узлы представлены на рис. 1.

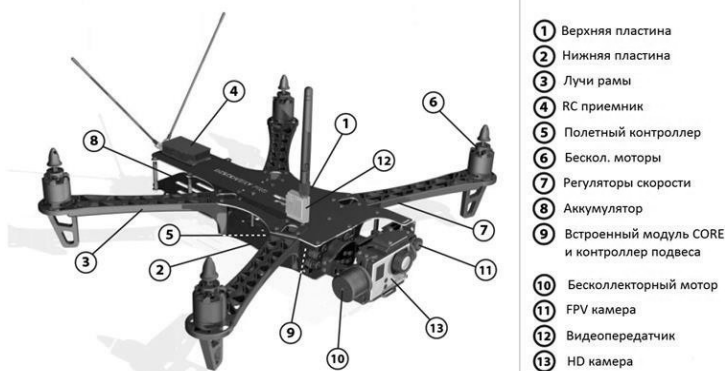


Рис. 1. Устройство стандартного БПЛА

Fig. 1. The structure of a standard UAV

3. КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ КФС

Концептуальная модель киберфизической системы [6] включает в себя пять уровней:

- 1) физический;
- 2) сетевой;
- 3) хранилище данных;
- 4) обработка и аналитика;
- 5) уровень приложений.

На рис. 2 представлена концептуальная модель киберфизической системы.

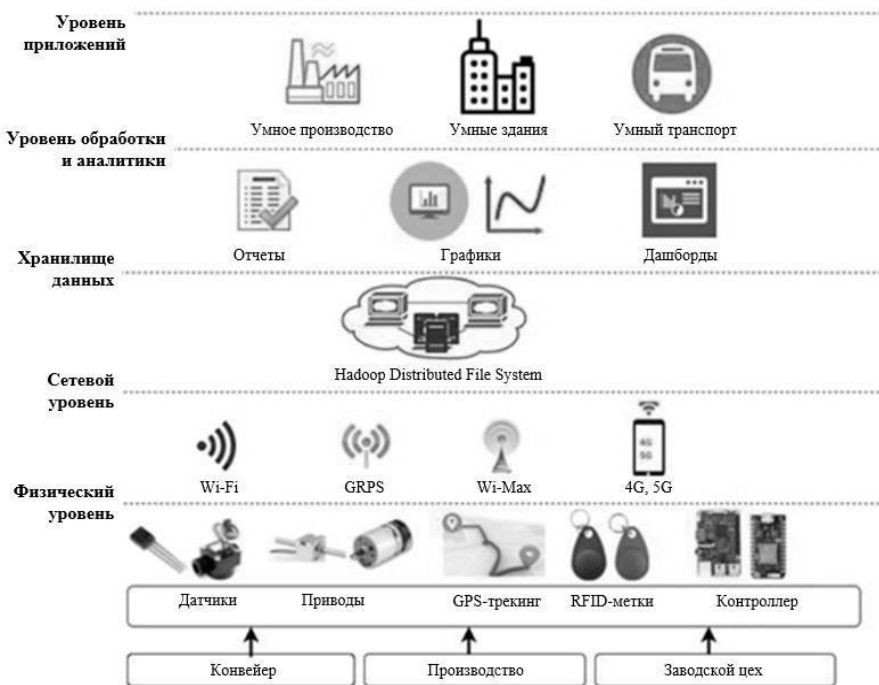


Рис. 2. Концептуальная модель киберфизической системы

Fig. 2. Conceptual model of a cyberphysical system

Физический уровень

Этот уровень состоит из приводов, датчиков, вычислительных элементов и отслеживающих устройств. В режиме реального времени контроллер спосо-

бен собирать с датчиков данные и обрабатывать их локально и/или передавать в облачное хранилище для обработки.

Сетевой уровень

Киберфизические системы могут получать доступ к киберпространству по различным сетевым протоколам, например:

- Wi-Fi,
- WiMAX,
- GPRS,
- технологии 3G/4G/LTE.

Другие облегченные протоколы, такие как MQTT, CoAP, AMQP, WebSocket и Node, используются для передачи данных с периферийных устройств в облако для их хранения и обработки [6]. Каждый протокол имеет свои плюсы перед другими в зависимости от пропускной способности, скорости, надежности, задержки, масштабируемости и безопасности.

Хранилище данных

Киберфизические системы обрабатывают большой объем данных, собранных с объектов, расположенных на физическом уровне. Такие данные хранятся на локальном сервере или в облаке. Данные могут храниться в кластере из трех различных подчиненных узлов с использованием распределенной системы хранения для резервирования

Уровень обработки и аналитики

Уровень обработки и аналитики применяется для обработки данных. С использованием SQL-запросов можно генерировать отчеты, графики, осуществлять мониторинг в режиме реального времени. Методы интеллектуального анализа данных, такие как кластеризация данных, классификация и регрессия, могут быть использованы для планирования и построения прогнозов. Также на этом уровне процессы мониторинга и управления могут быть направлены обратно на физический уровень для приведения в действие некоторых устройств.

Уровень приложений

Этот уровень является пользовательским интерфейсом для операторов, производителей, сторонних поставщиков. Также приложения имеют удобный интерфейс, позволяющий взаимодействовать с уровнями КФС на основе привилегированного доступа и приоритета.

4. ПРИМЕНЕНИЕ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

В настоящее время применение КФС охватывает большинство производственных сфер. Но наиболее востребованными они являются в области строительства, транспорта, производства и энергосбережения. Например, умная

электрическая сеть (Smart Grid) способна объединять несколько производственных электростанций с множеством нагрузок и в режиме реального времени производить динамическую балансировку нагрузки и ценообразование. Киберфизические системы в сфере производства представлены умными станками и машинами, технологиями 3D-печати и аддитивного производства в целом. Если роботы до последнего времени были оправданы на производстве только для стандартизированных повторяющихся операций, то гибридные системы, способные адаптироваться к изменениям, могут значительно расширить область действий автоматизированных систем.

На рис. 3 представлены сферы, в которых уже успешно применяются киберфизические системы.



Рис. 3. Сферы применения киберфизических систем

Fig. 3. Application areas of cyber-physical systems

5. КЛАССИФИКАЦИЯ КФС

В настоящее время сложно обозначить единую классификацию киберфизических систем. В обобщенном виде основные атрибуты (признаки) классификации КФС можно представить следующим образом.

1. Сложность в соответствии с функциональными возможностями и используемыми компонентами.
2. Связность в соответствии с используемыми интерфейсами и протоколами передачи данных.
3. Критичность в соответствии с зависящими от системы бизнес-процессами.
4. Социальный аспект в соответствии с характером взаимодействия системы с пользователями и операторами.

Эти атрибуты в большей степени применимы к концепции рассмотрения БПЛА как киберфизической системы. Именно по этой причине в дальнейшем будем использовать вышеуказанную классификацию.

Рассмотрение БПЛА как КФС позволяет определять их как совокупность датчиков, систем, вычислительных мощностей, а не как отдельный, неделимый объект. Подобная концепция в дальнейшем даст возможность определять элементы подобной КФС как уязвимости (точки входа) и при рассмотрении БПЛА использовать парадигмы, применимые к киберфизическим системам.

6. БПЛА КАК КИБЕРФИЗИЧЕСКАЯ СИСТЕМА

БПЛА является многосоставной системой и может включать в себя тысячи различных датчиков и сенсоров, которые обмениваются между собой информацией, аккумулируют ее и передают на управляющее устройство. Одиночные БПЛА или группу БПЛА можно рассматривать как информационную систему со своими структурно-функциональными характеристиками.

В БПЛА встроена киберфизическая система, состоящая из датчиков и/или исполнительных механизмов. Датчики предоставляют данные (или информацию) исполнительному механизму, который может управлять БПЛА. Собранные данные используются для анализа и принятия важных решений, связанных с полетной миссией.

Исходя из вышеописанного беспилотные летательные аппараты можно характеризовать как сложную систему, выполняющую сбор, хранение, обработку данных, поступающих от физических устройств (сенсоров, датчиков и т. д.), а также их тесную интеграцию с информационными технологиями в рамках надежной среды передачи данных (каналы управления и навигации).

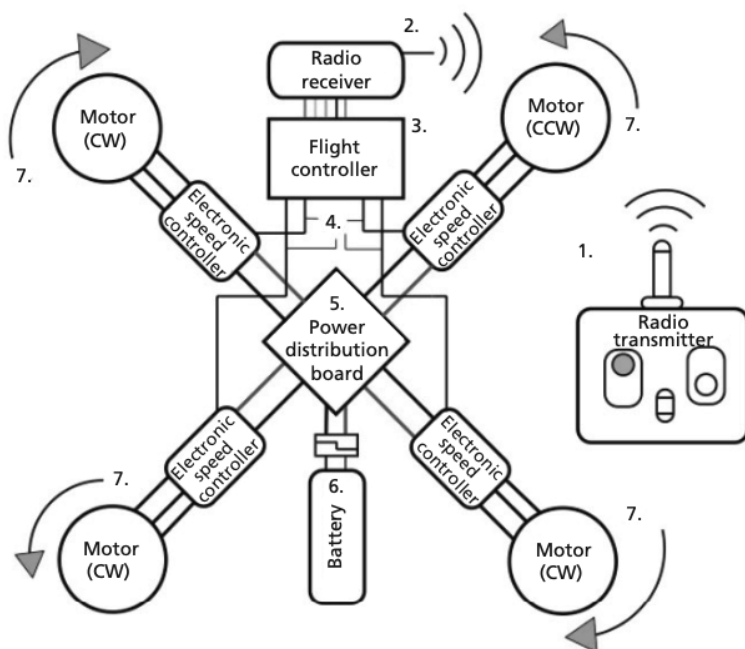


Рис. 4. Используемая в исследованиях структурная схема БПЛА [8]

Fig. 4. Structural diagram of the UAV used in the research [8]

Таким образом, в ряде случаев БПЛА можно рассматривать как киберфизическую систему, что позволит в дальнейшем применять к БПЛА ряд определений, свойственных КФС, и методики исследования информационной безопасности, в том числе модели угроз, модели атак, разрабатываемые для КФС.

7. СРАВНЕНИЕ КИБЕРНЕТИЧЕСКОЙ И КИБЕРФИЗИЧЕСКОЙ МОДЕЛИ KILL-CHAIN

После того как мы представили БПЛА в виде киберфизической системы, мы можем рассматривать и применять модели кибератак для киберфизических систем непосредственно к БПЛА.

Как один из примеров, рассмотрим сравнение кибернетической и киберфизической модели kill-chain, которая представлена на рис. 5 [7].



Рис. 5. Сравнение кибернетической и киберфизической модели kill-chain

Fig. 5. Comparison of cybernetical and cyberphysical kill-chain models

В соответствии с типовой моделью kill-chain для киберсистем все этапы атаки проводятся на одном уровне – физическом. Модель kill-chain для киберфизической системы организована на трех различных уровнях – физическом, уровне управления и киберуровне.

После определения БПЛА как киберфизической системы мы можем рассматривать различные модели кибератак (и модели защиты от них), соответствующие киберфизическим системам.

8. КИБЕРУГРОЗЫ БЕЗОПАСНОСТИ БПЛА. ИСТОЧНИКИ И РЕАЛИЗАЦИЯ

Чаще всего взлом производится с целью перехвата или подмены информации, передаваемой с помощью БПЛА. Современное ПО позволяет существенно снизить риск ошибок, а также повысить уровень автономности. Однако БПЛА имеет уязвимые места за счет факторов, оказывающих пагубное влияние на всю систему в целом.

Рассмотрим некоторые из них:

- 1) разрушающее радиоэлектронное воздействие на информационно-управляющую систему;
- 2) несанкционированный доступ к основным узлам на программном уровне и, как следствие, нарушение технологических циклов работы;
- 3) нарушение (срыв) управления из-за деструктивного воздействия вредоносного программного обеспечения (ПО);
- 4) человеческий фактор (свободный доступ к элементам БРЭО, ошибки программистов);

5) использование штатных операционных систем и аппаратных средств с имеющимися недеklarированными возможностями.

Но самым слабым местом любого БПЛА являются беспроводные каналы связи. Любые сигналы и команды, посылаемые GPS-навигатором, можно перехватывать, заглушить или подменить.

Атаки на БПЛА через уязвимость в канале связи можно разделить на три категории:

- 1) усиление или создание радиопомех, запуск в систему стороннего вредоносного ПО;
- 2) перехват трафика;
- 3) имитация и подмена сигналов GPS.

Исходя из вышеизложенного можно сделать вывод, что беспилотные летательные аппараты в дальнейшем можно позиционировать как киберфизические системы, а также применять к БПЛА угрозы безопасности, относящиеся к КФС.

СПИСОК ЛИТЕРАТУРЫ

1. Беспилотные летательные аппараты // Российские беспилотники. – URL: <https://russiandrone.ru/publications/bespilotnye-letatelnye-apparaty/> (дата обращения: 30.08.2024).
2. ГОСТ Р 59517–2021. Беспилотные авиационные системы. Классификация и категоризация. – М.: Стандартинформ, 2021.
3. Российская универсальная классификация // Арсенал-Инфо. – URL: <https://arsenal-info.ru/b/book/3398882726/15> (дата обращения: 30.08.2024).
4. Классификация UVS International // Арсенал-Инфо. – URL: <https://arsenal-info.ru/b/book/3398882726/14> (дата обращения: 30.08.2024).
5. NSF Workshop on Cyber-Physical Systems, October 16–17, 2006. – Austin, Texas, 2006.
6. *Смышляева А.А., Резникова К.М., Савченко Д.В.* Современные технологии в Индустрии 4.0 – киберфизические системы // Отходы и ресурсы. – 2020. – Т. 7, № 3. – Ст. 2. – DOI: 10.15862/02INOR320.
7. A multi-layered and kill-chain based security analysis framework for cyber-physical systems / A. Hahn, R.K. Thomas, I. Lozano, A. Cardenas // International Journal of Critical Infrastructure Protection. – 2015. – Vol. 11. – P. 39–50. – DOI: 10.1016/j.ijcip.2015.08.003.
8. How to analyze the cyber threat from drones: background, analysis frameworks, and analysis tools / K. Best, J. Schmid, S. Tierney, J. Awan, N. Beyene, M. Holliday, R. Khan, K. Lee. – RAND Corporation, 2020. – DOI: 10.7249/RR2972.

Васильев Евгений Алексеевич, аспирант кафедры безопасности информационных технологий. Основное направление научных исследований – безопасность БПЛА, методы радиоэлектронной борьбы. E-mail: evva@sfsedu.ru

Абрамов Евгений Сергеевич, заведующий кафедрой безопасности информационных технологий. Основное направление научных исследований – обнаружение атак, методы компьютерной криминалистики. E-mail: abramoves@sfsedu.ru

DOI: 10.17212/2782-2230-2024-3-63-77

UAV as a cyberphysical system *

E.A. Vasiliev¹, E.S. Abramov²

¹ *Institute of Computer Technologies and Information Security, ITA SFSU, 2 Chekhova Street, Taganrog, 347922, Russian Federation, postgraduate student of the Department of Information Technology Security. E-mail: evva@sfsedu.ru*

² *Institute of Computer Technologies and Information Security, ITA SFSU, 2 Chekhova Street, Taganrog, 347922, Russian Federation, Head of the department of the Department of Information Technology Security. E-mail: abramoves@sfsedu.ru*

Currently, the scientific community gives us separate definitions of UAVs and cyberphysical systems. These definitions are completely self-sufficient and do not intersect with each other. However, technical progress does not stand still and the narrowness of these definitions does not allow researchers to fully apply some definitions due to problems in terminology. This article will help overcome the existing differences in terminology and transfer the properties of cyber-physical systems to unmanned aerial vehicles.

Keywords: UAV, cyberphysical system, conceptual model, threat models, attack models, kill-chain model for CFS, UAV vulnerabilities, negative consequences

REFERENCES

1. *Bespilotnye letatel'nye apparaty* [Unmanned aerial vehicles]. *Rossiiskie bespilotniki* [Russian drones]. Available at: <https://russiandrone.ru/publications/bespilotnye-letatelnye-apparaty/> (accessed 30.08.2024).
2. GOST R 59517–2021. *Bespilotnye aviatsionnye sistemy. Klassifikatsiya i kategorizatsiya* [State standard R 59517–2021. Unmanned aircraft systems. Classification and categorization]. Moscow, Standartinform Publ., 2021.

* Received 18 August 2024.

3. Rossiiskaya universal'naya klassifikatsiya [Russian universal classification]. *Arsenal-Info*. (In Russian). Available at: <https://arsenal-info.ru/b/book/3398882726/15> (accessed 30.08.2024).
4. Klassifikatsiya UVS International [Classification UVS International]. *Arsenal-Info*. (In Russian). Available at: <https://arsenal-info.ru/b/book/3398882726/14> (accessed 30.08.2024).
5. *NSF Workshop on Cyber-Physical Systems*, October 16–17, 2006, Austin, Texas.
6. Smyshlyaeva A.A., Reznikova K.M., Savchenko D.V. Sovremennye tehnologii v Industrii 4.0 – kiberfizicheskie sistemy [Modern technologies in Industry 4.0 – cyber-physical systems]. *Otkhody i resursy = Russian Journal of Resources, Conservation and Recycling*, 2020, vol. 7, no. 3, art. 2. DOI: 10.15862/02INOR320.
7. Hahn A., Thomas R.K., Lozano I., Cardenas A. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection*, 2015, vol. 11, pp. 39–50. DOI: 10.1016/j.ijcip.2015.08.003.
8. Best K., Schmid J., Tierney S., Awan J., Beyene N., Holliday M., Khan R., Lee K. *How to analyze the cyber threat from drones: background, analysis frameworks, and analysis tools*. RAND Corporation, 2020. DOI: 10.7249/RR2972.

Для цитирования:

Васильев Е.А., Абрамов Е.С. БПЛА как киберфизическая система // Безопасность цифровых технологий. – 2024. – № 3 (114). – С. 63–77. – DOI: 10.17212/2782-2230-2024-3-63-77.

For citation:

Vasiliev E.A., Abramov E.S. BPLA kak kiberfizicheskaya sistema [UAV as a cyber-physical system]. *Bezopasnost' tsifrovyykh tekhnologii = Digital Technology Security*, 2024, no. 3 (114), pp. 63–77. DOI: 10.17212/2782-2230-2024-3-63-77.