УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ПРИМЕНЕНИИ ПОТРЕБИТЕЛЬСКИХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Клейменкин Д.В.
студент,
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,
Шахты, Россия
Моторко Е.А.
студент,
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,
Шахты, Россия
Бугакова А.В.
к.т.н., доцент
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,
Шахты, Россия

Аннотация

Данная статья посвящена технологии обеспечения информационной безопасности при использовании потребительских беспилотных летательных аппаратов (БПЛА). Так как БПЛА представляют собой тип подключенного устройства, собирающего и отправляющего данные для анализа, то это создает проблемы с безопасностью и возможностью взлома устройств. Необходимо рассмотреть, какие правила устанавливает правительство для обеспечения

безопасного полета. Проанализированы способы увеличения защищенности БПЛА от угрозы взлома.
Ключевые слова: беспилотный летательный аппарат, информационная безопасность, анализ данных, взлом устройства.

INFORMATION SECURITY IN THE APPLICATION OF CONSUMER DRONES

Kleimenkin D.V.
student,
Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,
Shakhty, Russia
Motorko E.A.
student,
Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,
Shakhty, Russia
Bugakova A.V.
Candidate of Technical Sciences, Associate Professor
Institute of Service Sphere and Entrepreneurship (Branch) of DSTU in Shakhty,
Shakhty, Russia

Abstract

This paper focuses on information security technology for consumer unmanned aerial vehicles (UAVs). Since drones are a type of connected device that collects and sends data for analysis, this creates security issues and the possibility of the devices being hacked. It is necessary to look at what regulations the government has put in place to ensure safe flying. Ways to increase the security of UAVs from the threat of hacking are analyzed.

Keywords: drone, information security, data analytics, device hacking.

Беспилотные летательные аппараты (БПЛА) вошли в повседневную жизнь как для частных, некоммерческих потребителей, в том числе для бытовых нужд, так и в качестве коммерческих устройств. В 2023 году рынок БПЛА, используемых во всех секторах, достигает 141 миллиард долларов, при этом объем рынка коммерческих БПЛА составляет не менее 17 миллиардов долларов.

Востребованность на рынке БПЛА обуславливается:

– ростом рынка беспилотных систем. Рынок БПЛА и систем мониторинга местности в реальном времени стремительно развивается. Этот рост обусловлен увеличением потребности в мониторинге и сборе данных о местности в различных отраслях, таких как сельское хозяйство, городское планирование, геология, экология и другие.

– эффективностью и экономией ресурсов. БПЛА обеспечивает эффективную и точную мониторинговую информацию, что позволяет клиентам оптимизировать свои операции и экономить ресурсы. Это особенно важно для сельского хозяйства, где можно увеличить урожайность и уменьшить затраты на воду и удобрения.

– безопасной и долгосрочной устойчивостью. В ряде сфер, таких как лесной и природный ресурс, мониторинг играет решающую роль в предотвращении лесных пожаров, охране природы и контроле за преступностью. Наш продукт обеспечивает безопасность и долгосрочную устойчивость в таких областях.

– гибкостью и адаптацией. Различные системы мониторинга могут быть легко настроены под конкретные потребности клиентов и масштабирована для разных местностей и условий. Эта гибкость делает продукт востребованным в разных отраслях и ситуациях.

– технологическим преимуществом. БПЛА использует передовые технологии, такие как высокоразрешающие камеры, датчики и программное

обеспечение для обработки данных. Это дает ему конкурентное преимущество на рынке.

– экологической устойчивостью. Использование БПЛА вместо традиционных средств мониторинга может снизить негативное воздействие на окружающую среду, так как они не требуют большого количества топлива и не выбрасывают вредные выбросы.

Классификация БПЛА указана в таблице 1.

Таблица 1 – Классификация БПЛА [1]

Класс БПЛА	Взлетная масса, кг	Дальность действия, км
Микро- и мини БПЛА ближнего радиуса действия	5	25-40
Легкие БПЛА малого радиуса действия	5-50	10-120
Легкие БПЛА среднего радиуса действия	50-100	70-150(250)
Средние БПЛА	100-300	150-1000
Среднетяжелые БПЛА	300-500	70-300
Тяжелые БПЛА среднего радиуса действия	>500	70-300
Тяжелые БПЛА большой продолжительности полета	>1500	1500
Беспилотные боевые самолеты	500	1500

БПЛА могут быть взломаны или использоваться для взлома других электронных устройств. Проблемы кибербезопасности будут становиться только более актуальными по мере увеличения количества БПЛА в небе и того, как злоумышленники становятся умнее выявлять любые слабые места в системе безопасности.

Существует несколько различных способов взлома БПЛА [2]. После обнаружения злоумышленник потенциально может передать по нисходящей линии видео или другие изображения, которые беспилотник транслирует на свою базовую станцию.

Например, БПЛА передает ложные координаты GPS. Беспилотник «думает», что следует своей первоначальной схеме полета, но на самом деле его ведут в другое место. БПЛА также может быть использован для того, чтобы врезаться в автомобиль, человека или даже другой беспилотник. Может быть

дано указание приземлиться рядом с злоумышленником, чтобы его можно было украсть вместе с полезной нагрузкой, которая может, например, включать камеру, установленную на БПЛА, и изображения, сохраненные на карте памяти.

БПЛА могут быть взломаны на расстоянии до двух километров. Перехватывая командно-контрольный сигнал между оператором и беспилотником, злоумышленник может получить полный контроль над его системами. Радиосигнал часто не зашифрован, что упрощает его декодирование с помощью анализатора пакетов, поэтому взломать сигнал БПЛА технически не сложно. Сигнал также может быть просто заглушен, в результате чего беспилотник не сможет самостоятельно ориентироваться.

Для того, чтобы обеспечить безопасность БПЛА в [3] предлагаются следующие методы [3]:

1. Регулярное обновление прошивки БПЛА. Основные производители БПЛА выпускают исправления при появлении новых угроз безопасности, поэтому регулярное обновление должно помочь беспилотнику опережать злоумышленников.

2. Использование надежного пароля для приложения базовой станции. Использование комбинации букв, цифр и специальных символов для создания надежного пароля поможет избежать взлома сигнала БПЛА злоумышленником [4].

3. При использование смартфона или ноутбука в качестве контроллера, обеспечить его безопасность и не допустить заражения вредоносными программами. Использовать антивирусное программное обеспечение и не загружать сомнительные программы или приложения.

4. Перейти на виртуальную частную сеть (VPN), чтобы злоумышленники не могли получить доступ к коммуникация при подключении к сети Интернет.

5. Установление ограничения в единицу для количества устройств, которые могут подключаться к базовой станции. Это предотвратит перехват сигнала злоумышленниками для управления другими устройствами.

6. Убедиться, что БПЛА имеет режим «Возвращение домой» (RTH). Это позволит восстановить беспилотник в случае угона. Однако, RTH зависит от работы GPS, и он не застрахован от подмены GPS [5].

Ответственность для владельцев беспилотников [6].

Если владелец беспилотника не соблюдает правила использования воздушного пространства, его могут привлечь к административной ответственности. За нарушение права на неприкосновенность частной жизни ответственность уголовная. Санкция – от штрафа в размере до 200 000 до лишения свободы на срок до двух лет. А еще потерпевший имеет право потребовать возместить убытки и моральный вред, если они возникли из-за распространения видео. Если при полете не было оформлено разрешение, но оно требовалось, и в результате беспилотник причинил человеку тяжкий вред или человек погиб – по неосторожности причинение тяжкого вреда здоровью или смерть человека ответственность будет уголовной. Санкция – до пяти лет лишения свободы, если пострадал один человек. Если погибли два или более лиц – свободы можно лишиться на срок до семи лет.

Библиографический список

1. Сашников Т. К. К вопросу обеспечения информационной безопасности беспилотных авиационных систем с летательными аппаратами малого и лёгкого класса в специализированных АСУ // T-Comm. 2013. №6. URL: https://cyberleninka.ru/article/n/k-voprosu-obespecheniya-informatsionnoy-bezopasnosti-bespilotnyh-aviatsionnyh-sistem-s-letatelnymi-apparatami-malogo-i-lyogkogo-klassa (дата обращения: 25.11.2023).

2. Basan E, Basan A, Nekrasov A, Fidge C, Sushkin N, Peskova O (2021) GPS-spoofing attack detection technology for UAVs based on Kullback-Leibler divergence. Drones 6(1):8

3. Altawy, Riham & Youssef, Amr. (2016). Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. ACM Transactions on Cyber-Physical Systems. 1. 1-25. 10.1145/3001836.

4. Susan Morrow. Beware of the drone! Privacy and security issues with drones [Электронный ресурс] – Режим доступа – URL: https://resources.infosecinstitute.com/topics/general-security/privacy-and-security-issues-with-drones/ (Дата обращения 27.11.2023)

5. Security and drones — what you need to know / Kaspersky [Электронный ресурс] – Режим доступа – URL: https://me-en.kaspersky.com/resource-center/threats/can-drones-be-hacked (Дата обращения 27.11.2023)

6. Порядок использования воздушного пространства РФ беспилотными воздушными судами (БВС, БПЛА, беспилотники, дроны) / Министерство транспорта РФ. Федеральное Агентство Воздушного Пространства [Электронный ресурс] – Режим доступа – URL: https://favt.gov.ru/poryadok-ispolzovaniya-bespilotnyh-vozdychnih-sudov/ (Дата обращения 27.11.2023)

Оригинальность 83%