Джабраилзаде Нурлан, Магистр
Национальная Авиационная академия
Jabrayilzade Nurlan**,** Master's Degree
National Aviation Academy

МЕТОДЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ БПЛА

Аннотация. Статья посвящена анализу актуальных угроз кибербезопасности, с которыми сталкиваются беспилотные летательные аппараты (БПЛА) в современных условиях. Рассматриваются основные векторы атак, включая перехват управления, GPS-спуфинг, внедрение вредоносного программного обеспечения и утечку конфиденциальных данных. Особое внимание уделено методам защиты, таким как шифрование данных, многофакторная аутентификация, использование блокчейн-технологий, системы обнаружения вторжений и альтернативные навигационные решения. Также обсуждаются перспективы применения искусственного интеллекта для повышения устойчивости БПЛА к киберугрозам.

Abstract. This article analyzes the current cybersecurity threats faced by unmanned aerial vehicles (UAVs) in modern operational environments. It examines key attack vectors, including command interception, GPS spoofing, malware injection, and leakage of confidential data. Special attention is given to protection methods such as data encryption, multi-factor authentication, blockchain technologies, intrusion detection systems, and alternative navigation solutions. The paper also discusses the potential of artificial intelligence to enhance UAV resilience against cyberattacks.

Ключевые слова: Аутентификация, блокчейн, беспилотные летательные аппараты, кибербезопасность, шифрование

Keywords: Authentication, blockchain, cybersecurity, encryption, unmanned aerial vehicles

Введение: Беспилотные летательные аппараты (БПЛА) сыграли значительную роль в развитии технологий и современного общества. Эти устройства становятся неотъемлемой частью таких отраслей, как сельское хозяйство, геодезия, логистика, охрана правопорядка, а также военные и разведывательные операции. БПЛА обладают уникальными возможностями: высокой маневренностью, способностью выполнять задачи без участия человека и работать в опасных или труднодоступных местах, что делает их ценными как для гражданского, так и для военного применения. В последние годы беспилотники широко используются для наблюдения, доставки, картографирования, разведки и даже спасательных операций, что подтверждает их значимость.

Однако с ростом их распространения и внедрения в различные сферы деятельности возникает ряд новых проблем, связанных с безопасностью эксплуатации. Учитывая, что большинство современных БПЛА полагаются на беспроводные технологии для связи, навигации и передачи данных, их системы становятся уязвимыми для разнообразных типов кибератак. Вредоносный код, перехват сигналов управления, подделка данных о местоположении и другие формы вмешательства могут не только нарушить работу аппарата, но и привести к катастрофическим последствиям, включая утрату контроля над аппаратом, угрозу безопасности людей и утечку конфиденциальной или стратегически важной информации.

Актуальность исследования: С каждым годом использование БПЛА расширяется, что сопровождается увеличением числа угроз, связанных с их эксплуатацией, особенно в области информационной и кибербезопасности. Беспилотные аппараты, будучи интегрированными в системы управления, передачи данных и навигации, становятся уязвимыми для различных типов атак. С учетом того, что большинство современных БПЛА используют беспроводные каналы связи для управления и передачи данных, они могут стать объектами различных вмешательств – от перехвата управляющих сигналов до внедрения вредоносного программного обеспечения. Например, GPS-спуфинг (фальсификация данных о местоположении), атаки на каналы управления и атаки с использованием уязвимостей в программном обеспечении могут привести к сбоям в работе аппарата, утрате контроля или краже данных.

Особенно актуальными являются угрозы для БПЛА, использующихся в военных или разведывательных целях, где утечка конфиденциальных данных может иметь стратегические последствия. Применение беспилотников в гражданских целях также вызывает обеспокоенность, так как утечка данных, например, во время мониторинга окружающей среды или доставки товаров, может нарушить законность и права частных лиц. Поэтому вопросы кибербезопасности БПЛА требуют пристального внимания как со стороны ученых и инженеров, так и со стороны государственных и частных организаций, которые используют эти устройства.

Цели и задачи исследования: Цель данного исследования – всесторонний анализ существующих угроз безопасности БПЛА, выявление их уязвимостей и разработка эффективных методов защиты. В рамках исследования будут рассмотрены различные аспекты угроз безопасности БПЛА, включая уязвимости в системах связи и управления, методы защиты данных, а также способы аутентификации пользователей и устройств. Важным элементом работы является исследование применения современных технологий, таких как шифрование данных, системы обнаружения вторжений и блокчейн-технологии, которые могут значительно повысить устойчивость БПЛА к кибератакам.

Задачи исследования:

1. Обзор существующих угроз безопасности БПЛА и классификация типов атак, которым подвергаются эти устройства.
2. Оценка эффективности существующих методов защиты БПЛА от киберугроз.
3. Разработка рекомендаций по улучшению киберзащиты БПЛА, включая как программные, так и аппаратные решения.
4. Исследование применения инновационных технологий для повышения безопасности БПЛА в условиях реальной эксплуатации.

Угрозы безопасности БПЛА

Современные угрозы кибербезопасности представляют собой разрушительное воздействие на системы управления БПЛА, так как эти аппараты активно используют беспроводные технологии для связи и передачи данных. Рассмотрим основные угрозы, с которыми сталкиваются БПЛА:

1. **Перехват управления**

Одним из самых опасных видов угроз для БПЛА является перехват управления. БПЛА используют беспроводные каналы связи для получения команд от оператора. Если эти каналы не защищены должным образом, они становятся уязвимыми для атак. Например, с помощью технологий глушения (jamming) злоумышленник может заблокировать связь между аппаратом и оператором, что приведет к сбоям в его работе. Более сложные атаки, такие как spoofing (обман) и man-in-the-middle (атака "человек посередине"), позволяют перехватить сигнал и изменить команды, поступающие к БПЛА. Это может привести к тому, что аппарат начнет действовать по указаниям атакующего, а не оператора.

2. **GPS-спуфинг (фальсификация GPS-сигналов)**

Большинство БПЛА используют GPS для навигации и определения местоположения. Однако эти системы уязвимы для атак типа GPS-спуфинг, когда злоумышленник посылает поддельные GPS-сигналы, чтобы ввести БПЛА в заблуждение относительно его реального местоположения. Это может привести к сбоям в работе устройства, его перехвату или даже к катастрофе. Спуфинг может оставаться незамеченным длительное время, что усложняет своевременное реагирование на такие атаки.

3. **Утечка конфиденциальной информации**

БПЛА часто используются для сбора и передачи конфиденциальной информации, такой как фотографии, видеозаписи, топографические карты и другие данные. Если передача данных не защищена должным образом, злоумышленники могут перехватить или модифицировать информацию, что представляет серьезную угрозу для безопасности, особенно если эти данные имеют стратегическое или разведывательное значение.

4. **Вредоносное ПО**

Вредоносное ПО (вирусы, трояны, шпионские программы) может быть установлено на БПЛА через зараженные устройства или внешние носители, такие как флешки. Вредоносные программы могут нарушить работу системы управления, повредить аппаратные компоненты или украсть данные. Современные БПЛА подключаются к различным беспроводным сетям, включая Wi-Fi, Bluetooth и мобильные сети, что создает дополнительные каналы для распространения вирусов и других вредоносных программ.

Методы защиты БПЛА

Для защиты БПЛА от киберугроз необходимо применять комплексные методы, которые включают как программные, так и аппаратные решения. Рассмотрим наиболее эффективные методы защиты:

1. **Шифрование данных**

Шифрование данных является одним из ключевых методов защиты БПЛА от атак. Использование криптографических алгоритмов, таких как AES (Advanced Encryption Standard) и RSA, позволяет защитить каналы связи между БПЛА и операторами от перехвата и подделки данных. Шифрование также необходимо для защиты GPS-сигналов от подделки и фальсификации.

2. **Многофакторная аутентификация**

Внедрение многофакторной аутентификации (MFA) позволяет повысить уровень безопасности управления БПЛА. Этот метод включает несколько уровней проверки, таких как пароли, биометрические данные и аппаратные токены. Это предотвращает несанкционированный доступ, даже если злоумышленники получат учетные данные оператора.

3. **Блокчейн-технологии**

Блокчейн является одной из инновационных технологий, которая может существенно повысить безопасность БПЛА. Блокчейн использует криптографические методы, которые делают невозможным изменение данных без изменения всей цепочки. Это можно использовать для аутентификации команд управления, защиты от вмешательства злоумышленников, а также для обеспечения прозрачности и надежности данных, передаваемых между БПЛА и наземными станциями.

4. **Системы обнаружения вторжений (IDS)**

Системы IDS помогают выявлять аномалии в поведении БПЛА и его компонентов. Эти системы анализируют трафик и мониторят работу устройства на предмет вторжений, таких как попытки захвата управления или внедрения вредоносного ПО. Такие системы позволяют оперативно реагировать на угрозы, предотвращая их развитие.

5. **Альтернативные системы навигации**

В случае уязвимости GPS-каналов важно использовать альтернативные системы навигации, такие как инерциальные навигационные системы (INS). Эти системы работают независимо от внешних сигналов, что делает их более устойчивыми к атакам, связанным с фальсификацией GPS-сигналов.

Инновационные технологии для повышения безопасности БПЛА

С развитием технологий киберугроз появляется необходимость применения инновационных решений для повышения уровня защиты БПЛА. Одной из таких технологий является искусственный интеллект (ИИ), который может использоваться для мониторинга и анализа поведения аппаратов в реальном времени. ИИ способен выявлять аномалии в действиях БПЛА и предсказывать возможные угрозы, что позволит операторам своевременно реагировать на изменения в работе аппарата.

Заключение

С развитием беспилотных летательных аппаратов (БПЛА) и их широким применением в различных отраслях, включая сельское хозяйство, оборону, логистику, безопасность и многие другие, возрастает и важность защиты этих технологий от киберугроз. Современные БПЛА, как и другие устройства, использующие беспроводные технологии для связи и

управления, становятся уязвимыми для множества видов атак, таких как перехват управления, фальсификация GPS-сигналов, внедрение вредоносного программного обеспечения и утечка конфиденциальной информации. Эти угрозы могут не только нарушить работу аппарата, но и привести к гораздо более серьезным последствиям, таким как утрата контроля над устройством, угроза безопасности людей и потеря стратегически важной информации.

Необходимость в комплексной защите БПЛА от кибератак становится всё более актуальной с учетом их стратегической важности и роли в различных сферах. В данном контексте важно развивать не только эффективные технические решения для защиты данных и систем, но и внедрять инновационные технологии, такие как искусственный интеллект и блокчейн, которые могут значительно повысить безопасность БПЛА. Методы шифрования, многофакторной аутентификации, а также системы обнаружения вторжений (IDS) оказываются важными элементами в предотвращении кибератак и обеспечении надежности эксплуатации беспилотных аппаратов.

Одним из важнейших аспектов исследования является создание многоуровневых и интегрированных решений, которые обеспечат защиту на всех уровнях – от передачи данных до аппаратных компонентов. Внедрение технологий защиты на всех этапах эксплуатации БПЛА позволит повысить их устойчивость к внешним угрозам и минимизировать риски, связанные с безопасностью. Важным шагом вперед в этом направлении является использование альтернативных навигационных систем, таких как инерциальные навигационные системы (INS), а также развитие инновационных подходов в области искусственного интеллекта и машинного обучения для анализа и прогнозирования угроз.

В заключение, можно утверждать, что безопасность БПЛА – это не просто техническая задача, а важная составляющая их успешного и безопасного применения в различных областях. Эффективная защита этих аппаратов требует комплексного подхода, включающего как современные методы криптографической защиты, так и инновационные разработки в области кибербезопасности, что позволит обеспечить их безопасность и надежность в условиях множества актуальных угроз.

Список литературы:

1. Исрафилов А. Современные вызовы в области кибербезопасности беспилотных авиационных систем. // КиберЛенинка, 2024.

2. Renu Y., Sarveshwaran V. A Review of Cyber Security Challenges and Solutions in Unmanned Aerial Vehicles (UAVs). // Inteligencia Artificial, 2025, 28 (75), 199–219.

3. Yu A., Kolotylo I., Hashim H.A., Eltoukhy A.E.E. Electronic Warfare Cyberattacks, Countermeasures and Modern Defensive Strategies of UAV Avionics: A Survey. // arXiv preprint, 2025.

4. Mekdad Y., Aris A., Babun L., et al. A Survey on Security and Privacy Issues of UAVs. // arXiv preprint, 2021.

5. Hassija V., Chamola V., Agrawal A., et al. Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey. // arXiv preprint, 2021.

6. Cyber4Drone: A Systematic Review of Cyber Security and Forensics of Drones. // MDPI Drones, 2023.

7. A Comprehensive Review Of Cyber Security In Unmanned Aerial Vehicles. // IOSR Journal of Computer Engineering, 2025, 27 (2), 25–34.

8. UAS Cyber Security and Safety Literature Review. // FAA ASSURE, 2021.

9. A Survey on Cybersecurity Attacks and Defenses for Unmanned Aerial Vehicles. // Journal of Systems Architecture, 2023.

10. The Cybersecurity Risks Threatening Drones: Innovative Solutions and Future Directions. // Preprints, 2025.