ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В СИСТЕМАХ УПРАВЛЕНИЯ АКТИВНЫМИ ФАЗИРОВАННЫМИ АНТЕННЫМИ РЕШЕТКАМИ

Д.К. Ульянов, *магистрант*
Московский технический университет связи и информатики
(Россия, г. Москва)

DOI:10.24412/2500-1000-2024-1-2-242-244

Аннотация. *В статье рассматриваются проблемы кибербезопасности в системах управления активными фазированными антенными решетками (АФАР). Выявлены возможные проблемы кибербезопасности, связанные с системами управления АФАР. Определены меры безопасности, направленные на укрепление целостности и функциональности ключевых систем в условиях потенциальных киберугроз.*

Ключевые слова: *АФАР, кибербезопасность, данные, система.*

Активные фазированные антенные решетки (АФАР) представляют собой антенные системы, играющие ключевую роль в области связи, радиолокации и других сфер. Данные системы зависят от сложных механизмов управления для обеспечения их нормального функционирования. Однако, как и любая другая технология, системы управления АФАР подвержены уязвимостям в области кибербезопасности. Рассмотрим возможные проблемы кибербезопасности, связанные с системами управления АФАР [1]. К ним целесообразно отнести:

- несанкционированный доступ, когда злоумышленники пытаются получить доступ к системам управления АФАР, как физическим, так и удаленным способом, что может привести к манипуляциям конфигурацией антенн, нарушению систем связи или радиолокации;
- перехват и манипулирование данными, передаваемыми между устройствами управления и АФАР, что может привести к неправильному лучеобразованию или изменениям схем связи;
- DoS-атаки и последующий отказ оборудования систем управления АФАР, что может привести к простою, повлиять на критически важные приложения, зависящие от АФАР, такие как системы экстренной связи или военные радары [2].

Актуальность исследования уязвимостей кибербезопасности, связанных с системами управления Активных Фазированных Антенных Решеток (АФАР), представляет собой важный аспект в применении передовых технологий и взаимосвязанных систем. АФАР играют ключевую роль в критически важных системах связи и радиолокации, что делает их потенциальными объектами для кибератак.

С ростом зависимости организаций от технологических систем возрастает и неотложность обеспечения их защиты от несанкционированного доступа, манипуляции данными и других киберугроз. Нарушение целостности и функциональности систем управления АФАР может иметь значительные последствия, начиная от снижения уровня конфиденциальности данных до нарушения работы систем связи и радиолокации. Внедрение мер безопасности обеспечивает надежность Активных Фазированных Антенных Решеток (АФАР), повышает устойчивость инфраструктур, зависящих от антенных систем.

В исследовании [3] авторы представляют новую архитектуру беспроводной передачи данных под названием «переключаемый фазированный массив» (ПФМ) с целью усиления безопасности физического уровня. ПФМ действует в качестве платформы для трех различных техник передачи:

1) передача с использованием обычного фазированного массива;
2) техника передачи подмножества антенн;
3) техника бесшумного переключения антенн.

ПФМ состоит из обычного черного передатчика с фазированным массивом, за которым следуют антенны с схемой переключения включения-выключения.

Предложенное решение сохраняет цель перемешивания точек созвездия как по амплитуде, так и по фазе в нежелательных направлениях, сохраняя при этом четкое созвездие в целевом направлении. ПФМ отличается от ранее использованных методов следующим образом:

1) ПФМ не ограничивается использованием фазовой модуляции и может принимать любой тип модуляции, включая;

2) нет необходимости модулировать сигнал в радиочастотной (РЧ) области, где остаются неизменными схемы обычного передатчика с фазированным массивом;

3) на больших расстояниях ПФМ перемешивает созвездие сигнала;

4) ПФМ легко интегрируется с существующей инфраструктурой фазированных передатчиков;

5) ПФМ разрывает связь между скоростью передачи данных и скоростью переключения;

6) ПФМ выполняет различные техники цифровой модуляции. Результаты показывают, что ПФМ и его варианты представляют собой простые и очень эффективные решения для улучшения безопасности физического уровня связи на миллиметровых волнах.

Рассмотрим предложенные меры безопасности, направленные на укрепление целостности и функциональности ключевых систем в условиях потенциальных киберугроз.

1. Шифрование выступает в качестве надежного механизма защиты конфиденциальности и целостности данных, передаваемых в системах управления АФАА. Реализация конечного шифрования гарантирует, что конфиденциальная информация остается защищенной и устойчивой к несанкционированному доступу **Ошибка! Источник ссылки не найден.**[3]. Однако выбор алгоритмов шифрования должен соответствовать стандартам отрасли и регулярно обновляться для сопротивления эволюции киберугроз.

2. Системы обнаружения вторжений (СОВ) играют ключевую роль в выявлении и реагировании на аномальную активность в сетях управления АФАА. Непрерывный мониторинг подозрительного поведения повышает способность системы обнаруживать и своевременно смягчать потенциальные кибервторжения [5]. Однако эффективность СОВ зависит от качественных баз данных сигнатур и алгоритмов обнаружения аномалий. Регулярные обновления и настройки необходимы для адаптации к новым угрозам.

3. Протоколы аутентификации снижают риск несанкционированного доступа к системам управления АФАА. Использование многократной аутентификации добавляет дополнительный уровень безопасности, гарантируя, что только авторизованный персонал может взаимодействовать с конфигурациями системы [2]. Однако требуется регулярное обновление и ротация учетных данных аутентификации.

Предложенные меры безопасности соответствуют лучшим практикам отрасли и предоставляют комплексный подход к решению потенциальных уязвимостей в системах управления АФАА. Шифрование обеспечивает конфиденциальность и целостность данных, системы обнаружения вторжений активно мониторят подозрительную активность, а протоколы аутентификации гарантируют, что только авторизованные лица имеют доступ и могут манипулировать механизмами управления. Однако важно отметить, что кибербезопасность является областью постоянного развития, и постоянное внимание, обновления и соблюдение новых лучших практик необходимы для поддержания устойчивости систем управления АФАА перед постоянно меняющимися киберугрозами.

Библиографический список1. Visser H.J. Array and phased array antenna basics. – John Wiley & Sons, 2006.

2. Швець В.А., Харченко В.П. Antenna array as a constructive element of increasing cybersecurity of network satellite system receivers. 2018.

3. Alotaibi N.N., Hamdi K.A. Switched phased-array transmission architecture for secure millimeter-wave wireless communication // IEEE Transactions on Communications. – 2016. – Т. 64. № 3. – С. 1303-1312.

4. Барабанов А., Марков А., Цирлов В. Сертификация систем обнаружения вторжений //Открытые системы. СУБД. – 2012. – № 3. – С. 31-33.

5. Садирова Х. Протоколы аутентификации в обеспечении сетевой безопасности // Conference on Digital Innovation: Modern Problems and Solutions. 2023.

CYBER SECURITY CHALLENGES IN ACTIVE PHASED ARRAY ANTENNAS CONTROL SYSTEMS

D.K. Ulyanov, *Graduate Student*
Moscow Technical University of Communication and Informatics
(Russia, Moscow)

Abstract. *The article discusses cybersecurity problems in active phased array antenna (APA) control systems. Possible cybersecurity problems associated with APAA control systems have been identified. Security measures have been identified to strengthen the integrity and functionality of key systems in the face of potential cyber threats.*

Keywords: *APAA, cybersecurity, data, system.*