**НЭНСИ ФРИДРИХ (NANCY FRIEDRICH),** маркетолог по решениям для аэрокосмической и оборонной промышленности, Keysight Technologies

# ПЕРСПЕКТИВЫ РАЗВИТИЯ РЭБ: САМООБУЧЕНИЕ КАК ДВИЖЕНИЕ ВПЕРЕД

Для того чтобы не отстать от противника, вооруженные силы должны постоянно развиваться, используя более гибкие, масштабируемые способы обнаружения, анализа и подавления противдействующих сигналов.

Военно-воздушные силы США недавно отправили в отставку свой первый самолет типа Compass Call. Созданный в 1982 году, он выпускался в различных модификациях, специализированных на обнаружении, перехвате и подавлении радиосвязи противника. Системы этого самолета могли нарушать радиосвязь и препятствовать координации действий воинских подразделений. Такие возможности позволяли ему оставаться в строю почти четыре десятилетия. Однако за это время системы радиоэлектронного противодействия стремительно развивались, что привело к созданию более сложных систем РЭБ. Изменяющиеся технологии и рыночные тенденции способствовали появлению новых угроз, поставив перед современными вооруженными силами задачу их своевременной идентификации.

Как правило, РЭБ (радиоэлектронная борьба) определяется как противодействие в сложной электромагнитной обстановке, в результате чего все радиочастотные системы считаются элементами РЭБ. Электромагнитные воздействия охватывают разные аспекты среды РЭБ, от радиолокационных систем и генераторов помех до военных систем связи. Целью может быть любая система, работающая через эфир. Для обеспечения связи, обнаружения и защиты системы РЭБ используют электромагнитные волны. Подавление этих функций означает нарушение работы систем связи или навигации противника. Кроме того, системы радиоразведки могут собирать информацию и отыскивать цели.

Даже слабые противники могут применять серийно выпускаемое оборудование, например, средства подавления системы глобального позиционирования (GPS). Так, атака на системы навигации способна нарушить координацию действий. Но, что еще страшнее, кибернетические системы противника могут исказить информацию о местоположении, времени или навигации. Подобные действия приводят к различным проблемам — от простого замешательства до грандиозных катастроф. Противник может не производить видимых атак, а просто вносить ошибки в работу систем связи и другого оборудования.

## НОВЫЕ МАСШТАБЫ РЭБ

В любом радиоэлектронном конфликте победителем выйдет тот, кто сможет быстрее ориентироваться в электромагнитной обстановке, используя для этого технологические преимущества. Тем не менее количество и сложность угроз

постоянно возрастает, что в первую очередь определяется наличием технологий. Несколько десятилетий назад в этой области доминировало весьма ограниченное число игроков. Технологические возможности и затраты, необходимые для достижения превосходства в области РЭБ, не позволяли другим создавать конкурентоспособные системы. Однако по мере удешевления и роста доступности серийно выпускаемой электроники, в РЭБ включились противники всех масштабов. В наше время даже мелкие агрессоры могут располагать конкурентоспособным арсеналом угроз, что делает среду РЭБ более опасной и непредсказуемой. С понижением входного барьера, каждый, обладающий достаточным мастерством и знаниями, может обзавестись оборудованием, способным создавать угрозу.

Системы программной радиосвязи (SDR) тоже сильно изменили арену РЭБ. Изначально под SDR понимались перестраиваемые средства связи, реализованные полностью программно. Аналогово-цифровое преобразование выполнялось непосредственно во входном тракте. Однако современные системы SDR зачастую принимают более сложные формы и позволяют изменять рабочую частоту, модуляцию, диапазон и сетевой протокол без смены оборудования. С ростом скорости цифровой обработки сигнала (ЦОС) и аналого-цифрового преобразования (АЦП), все большая часть обработки сигнала выполняется в цифровой форме. С помощью таких технологий вооруженным силам легче обновлять системы противодействия. Стремительное развитие серийно выпускаемого оборудования двойного назначения и программных радиосистем приведет к значительному многообразию и сложности будущих угроз.

Считается, что в будущем наиболее сильное влияние на РЭБ окажут технологии искусственного интеллекта (ИИ). С добавлением ИИ системы противодействия начнут еще и обучаться в процессе выполнения каждой боевой задачи, что, вероятно, в будущем сделает их преобладающими.

## УГРОЗЫ ОБРЕТАЮТ НОВЫЕ ФОРМЫ

Благодаря развитию технологий целевые сигналы постоянно усложняются. В прошлом они были статическими — всегда проявлялись и вели себя одинаково. Современные постановочные сигналы систем РЭБ гибко меняют поведение в зависимости от сценария. Например, если противник подавляет реактивную угрозу, то сигнал может быть установлен на другую несущую или изменить характер возникновения. Поэтому сегодня противники должны предвидеть вероятность изменения постановочного сигнала и быть готовыми к соответствующей реакции.

Как правило, такие угрозы называют когнитивными или адаптивными. И хотя люди считают эти термины синонимами, существует много уровней адаптивности. Большинство из них не связано с возможностями когнитивных систем РЭБ. Используя алгоритмы самообучения, когнитивные системы РЭБ могут начать взаимодействие со средой, не имея информации о потенциале противника, и быстро оценить текущий сценарий. Выполняя некоторые действия, вызывающие реакцию со стороны систем противника, когнитивные системы могут оценивать эту реакцию, а затем сформировать эффективный ответ, подходящий для конкретной системы противника.

В отличие от этого адаптивные решения способны быстро оценить новый сценарий и среагировать на него оригинальным способом. Например, адаптивный радар может проанализировать обстановку и соответствующим образом изменить характер передачи, применяя новую форму сигнала для каждой передачи или меняя алгоритм обработки импульсов. Такая гибкость может, например, улучшить разрешение цели.

Многим системам РЭБ для изменения формы сигнала требуется лишь небольшое изменения программы, что повышает непредсказуемость формы и поведения сигнала. Вооруженные силы стремятся отделить адаптивные импульсы РЛС от других сигналов, независимо от того, кому они принадлежат — союзнику или противнику. По мере того как угрозы становятся все более адаптивными, оппоненты должны реагировать на них как можно быстрее.

## ВЛИЯНИЕ САМООБУЧЕНИЯ

С появлением искусственного интеллекта (ИИ) интеллектуальные машины стали работать и реагировать на события подобно людям. Эти машины могут выполнять интеллектуальные операции, используя такие функции, как распознание сигналов. Самообучение поднимает ИИ на следующую ступень, позволяя непрерывно обучаться на основе полученных данных и соответствующим образом адаптироваться. Такие компьютеры обучаются очень быстро. Системы РЭБ, использующие самообучение, обучаются на каждой боевой операции, определяя способы повышения эффективности, что позволяет им получать преимущество в будущих столкновениях.

Причем данная эволюция происходит без вмешательства человека, поскольку компьютер сам решает, как изменить свое поведение. В процессе тестирования и применения эти системы обучаются на основе приобретенного опыта. В результате они меняют свое будущее поведение, а значит, компьютер сам принимает решение о последующих шагах. Благодаря непредсказуемости такой системы, даже создавшие ее люди не могут точно спрогнозировать ее поведение.

Используя самообучение, системы РЭБ будут адаптироваться и менять свое поведение или способ действий с нарастающей скоростью. Например, если радар пытается отследить самолет, контрмеры противника могут ему в этом помешать. Самообучаясь, радар постарается применить другие методы обнаружения в стремлении достичь успеха. Современные машины обладают уровнем интеллекта, на порядок превосходящим знания человека — специалиста в области РЭБ, поскольку они обучаются на постоянно накапливаемых данных.

## ПОСТОЯННО МЕНЯЮЩЕЕСЯ БУДУЩЕЕ

В связи с изобилием новых современных вариативных угроз вооруженные силы сражаются за контроль над электромагнитной обстановкой. Доминирование в спектре позволяет им обнаруживать, обманывать и срывать операции противника, одновременно защищая соб-

ственную армию. Для достижения такого доминирования вооруженные силы должны постоянно совершенствовать применяемые угрозы и меры противодействия. Чтобы не отстать от постоянно меняющегося характера сигналов систем РЭБ, военным нужны гибкие масштабируемые решения. Риск, ослабленный сегодня, завтра может уже не представлять опасности, вынуждая вооруженные силы постоянно готовиться к новым угрозам и даже к новым противникам.

Неполные, несогласованные данные не позволяют получить ясную картину постановочных сигналов и создать методологию проверки противодействия этим угрозам. Такая проблема порождается традиционными системами имитации эмиттеров в системах РЭБ. Они используют базы данных известных помех, для которых обычно имеются соответствующие меры противодействия. Сейчас подобные классифицированные списки известных целей быстро устаревают и уже неэффективны. Эти системы не могут идентифицировать и устранять угрозы в ЭМ среде и оперативно принимать необходимые меры противодействия.

И даже если такие системы могут обрабатывать новые сигналы, они используют для этого очень медленные процессы. Из обнаруженного возмущения в эфире военные извлекают информацию о типе сигнала — частоту или период повторения импульсов (PRI), отсылают сведения в лабораторию и вырабатывают меры противодействия. Пройдут месяцы, прежде чем эта информация будет готова к применению в системе.

В ходе будущих военных действий противник будет иметь более полную картину происходящего. Исходя из достигнутого в последнее десятилетие, можно сделать вывод, что в следующие 10–20 лет произойдет быстрое развитие технологий. Согласно прогнозам, нарастание самообучающихся машин и искусственного интеллекта подстегнет непрерывную эволюцию систем РЭБ. Они начнут использовать мощные вычислительные среды, применяя, например, несколько параллельно работающих устройств для ускорения сбора информации. Технологии обнаружения тоже будут играть важную роль, собирая информацию о зоне конфликта. Новые методы кодирования уже привели к появлению сложных, взаимосвязанных и коррелированных датчиков.

Эти технологические инновации позволят создать умные, быстро адаптирующиеся помеховые сигналы и методы достижения контроля в спектральной обстановке. Но, несмотря на постоянное развитие технологий и появление новых типов угроз, кое-что остается неизменным: вооруженные силы, достигшие и сохранившие доминирование в спектре, получат преимущество и в области РЭБ.