Тельминов О.А.

Модель угроз для системы управления колесной платформой с многоагентной многоуровневой нейросетевой реализацией

Аннотация: Предлагается формирование модели угроз для системы управления колесной платформой, учитывающей программную и аппаратную реализацию.

Ключевые слова: система управления, модель угроз, искусственные нейронные сети

Система управления колесной платформой состоит из нейросетевого программного обеспечения с развитой иерархией, которое выполняется на процессоре с выделенными ускорителями для традиционных формальных и передовых спайковых нейросетей. Для обеспечения кибербезопасности такой системы на первом этапе необходимо разработать модель угроз, которая закладывает общую основу для управления рисками безопасности. В модели определяется, какие ресурсы и от какого типа нарушителя защищать в системе; возможные атаки; меры обеспечения требуемого уровня доверия и устойчивости к инцидентам. Таким образом, выстраиваются вектора атаки – прозрачные цепочки вида угроза/нарушитель – возможные воздействия на элементы системы – меры предотвращения или снижения последствий – тесты.

1. Описание системы управления колесной платформой

Система управления колесной платформой состоит из цифрового двойника такой платформы и моделей соратников, соперников, окружающей среды (таблица 1). Для цифрового двойника и каждой из моделей работает программный агент, в совокупности образуя многоагентную систему управления. Цифровой двойник платформы получается с помощью нейросети Behavior Cloning (BC) путем наблюдения за PINN, которая реализует физико-математическую модель движения платформы. Прорабатывается вопрос двухсторонней связи между цифровым двойником и системой управления. При этом BC состоит из трех уровней: стратегического, тактического и рефлексного, которые

различаются по быстродействию и объему вычислительных затрат, обратно пропорциональных друг другу. Обученная на сервере ВС далее запускается на платформе на периферийном устройстве с возможностью дообучения на борту. Периферийное устройство состоит из управляющего CPU и двух типов нейроускорителей – для традиционных формальных сетей и для спайковых сетей. Первый тип используется для реализации массированных матричных вычислений, второй – для более разреженной событийной обработки. В периферийном устройстве оптимизированы узкие места работы с памятью на всех этапах: DMA, кэш-память, переключение контекста тредов, векторно-матричные вычисления в памяти на кроссбарах с применением традиционных элементов и элементной базы на новых физических принципах, ассоциативную память для нейросетей и другие. Модернизированные для этой цели элементы электронной компонентной базы и ключевые узлы на их основе запланированы к моделированию в соответствующей САПР с применением моделей одной из отработанных технологий микроэлектроники. В качестве примера мобильного робота используется колесная платформа, что является развитием имеющегося задела [1-3].

Таблица 1 – Функции, выполняемые программными агентами с помощью цифрового двойника и моделей объектов реального мира

Объект	Агент
Объект управления	Цифровой двойник: интегрирует данные других агентов, прогнозирует его состояние, поведение, реакции и воздействует на платформу
Объект влияния	Модель прогнозирует его состояние, поведение, реакции
Окружающая среда	Многомасштабные модели прогнозируют ее ландшафт, погодные условия, препятствия
Соратники	Модель прогнозирует их состояние, поведение, реакции
Соперники	Модель прогнозирует потенциальные угрозы от них, помехи и конкурирующие действия

2. Модель угроз для системы управления

Целью разработки модели угроз является определение, анализ и оценка угроз безопасности информации, в части (1) компрометации обучающих выборок и моделей на этапах обучения и дообучения нейросетей на стратегическом, тактическом и рефлексном уровнях; (2) модификации процессов взаимодействия агентов системы управления, соратников, соперников и окружающей среды; (3) нарушения целостности, устойчивости и доверенности вычислительного процесса; (4) искажение входных данных о состоянии и параметрах движения платформы. С этой целью может быть использована, например, отечественная методика оценки угроз [4].

К объектам защиты можно отнести следующие пункты. Информационными ресурсами являются обучающие выборки, в том числе построенные с помощью PINN, а также результаты симуляций для обучения ВС, параметры нейросетевых моделей, логи функционирования нейросетей и телеметрия сопряженных устройств. В части программного обеспечения следует отметить нейросетевые фреймворки, агентов, микрокоды CPU, нейроускорителей и других аппаратных решений (где применимо). К аппаратной части относятся указанные выше составляющие и их элементы, сенсорные элементы на колесной платформе, интерфейсы связи. Каналы связи представлены внутренней шиной периферийного вычислительного устройства, а также бортовыми модулями связи с удаленными объектами, в том числе для телеметрии.

Имеется несколько потенциальных источников угроз. Внешние злоумышленники воздействуют на платформу через каналы связи. К внутренним нарушителям относятся разработчики или операторы с избыточными правами. Технические и программные сбои могут вызываться ошибками при работе аппаратной и программной части вычислителя, а также при функционировании программных агентов. При изготовлении аппаратной части на недоверенных фабриках, например, за рубежом, возможно размещение закладок в составные части вычислителя для нейросетей. Аналогичная ситуация вероятна и при недоверенной разработке программного обеспечения для вычислителя, в том числе и нейросетевых программных агентов. Важным источником угроз являются электромагнитные помехи,

дрейф параметров и деградация компонентов, в том числе и мемристоров с ограниченным числом резистивных переключений.

К возможным уязвимостям программной части следует отнести отсутствие контроля целостности при удаленном обновлении программного обеспечения и нейросетевых моделей, утечку данных телеметрии и обмена. В аппаратной части возможна утечка через побочные электромагнитные излучения и наводки, вероятны уязвимости через закладки, дефекты и незащищенную загрузку микропрограмм. Для нейросетевых моделей свойственны такие уязвимости, как «отравление» данных, подмена модели и внедрение backdoor-паттернов в веса нейросетей. При сетевом взаимодействии возможны перехват и подмена данных в каналах связи, атаки на сообщения между агентами.

На основании рассмотренного сформулированы перечень угроз информации и потенциальные последствия их реализации. Предложен ряд программных, аппаратных и организационных мер, обеспечивающих кибербезопасность системы управления. В дальнейшем планируется разработка комплексной методики защиты информации для рассматриваемой системы управления.

Литература:

1. *Тельминов О.А.* Концепция многоагентной нейроподобной когнитивной системы управления мобильным робототехническим комплексом / VI Международная конференция по нейронным сетям и нейротехнологиям (NeuroNT'2025). Сборник докладов. Санкт-Петербург (4-5 мая 2025 г.). – СПб.: СПбГЭТУ «ЛЭТИ», 2025. – С. 122-126.

2. *Тельминов О.А.* Особенности нейроподобной реализации многоагентного управления роботом в распределенных системах / XVIII Всероссийская мультиконференция по проблемам управления (МКПУ–2025): материалы мультиконференции. Тула (15 сентября-20 сентября 2025 г.): в 4 т. Т. 2. Управление в распределенных и сетевых системах (УРСС – 2025) / под ред. академика РАН И.А. Каляева. – Тула: Изд-во ТулГУ, 2025. – С. 296-299.

3. *Тельминов О.А.* Варианты нейроподобной реализации многоагентного управления роботом / Российский форум «Микроэлектроника 2025» 11-я Научная конференция «ЭКБ и микроэлектронные модули». Сборник тезисов. Научно-

технологический университет «Сириус» (21-27 сентября 2025 г.). – М.: ТЕХНОСФЕРА, 2025. – С. 706.

4. Методический документ: Методика оценки угроз безопасности информации. ФСТЭК России, 2021 [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения 01.09.2025).