Предложенный метод решения задачи, являющийся функцией параметров распределения ресурсов ОТС, и разработанный на его основе математический аппарат теоретико-игрового подхода, позволяет обосновать точки КУ на множестве условий взаимодействия ОТС.

Литература:

1. *Берзин Е.А.* Оптимальное распределение ресурсов и теория игр. – М.: Радио и связь, 1983. – 216 с.

2. *Нейман Дж. фон, Моргенштейн О.* Теория игр и экономическое поведение. – Москва: Наука, 1970. – 708 с.

Мамченко М.В.

Подход к оценке изменения критических характеристик робототехнических систем во времени

Аннотация: Для обеспечения безопасного функционирования робототехнических систем предлагается подход к оценке изменения их критических характеристик во времени, позволяющий формировать значения предкритических состояний и отказа для аппаратных и программных компонентов, которые, в свою очередь, могут использоваться для сравнения состояний активов робототехнической системы как в реальном времени, так и после завершения эксплуатации активов.

Ключевые слова: робот, робототехническая система, обработка информации, критические характеристики, безопасность

Введение

В процессе эксплуатации робототехнических систем (РТС) наиболее актуальным вопросом является обеспечение их безопасности, особенно – информационной. В научной литературе вопрос обеспечения информационной безопасности роботов является достаточно изученным: например, разработаны модели информационной безопасности РТС, соответствующие средства

моделирования и подходы к их построению, модели угроз, методы, способы и алгоритмы безопасного управления, в том числе группового, выявления инцидентов и нарушений безопасности, анализа рисков, обеспечения безопасности связи и отдельных элементов, интерфейсов и подсистем роботов; оценено влияние человеческого фактора на состояние информационной защищенности РТС [1–6]. Однако слабо исследованным является направление, связанное с оценкой состояния элементов и характеристик роботов и РТС, которые являются критически важными для обеспечения их безопасного функционирования, и разработкой соответствующих методов, моделей, подходов и (или) алгоритмов.

Для обеспечения безопасного функционирования РТС в работе предлагается подход к оценке изменения критических характеристик во времени, позволяющий формировать значения предкритических состояний и отказа для аппаратных и программных компонентов, которые, в свою очередь, могут использоваться для сравнения состояний активов системы как в реальном времени, так и после завершения эксплуатации ее активов.

1. Суть подхода

Понятие «критическая характеристика» без привязки к конкретному анализируемому объекту определим с использованием ГОСТ Р 50779.82-2018: непосредственно влияющая на выполнение основной функции характеристика, выявленная на основе логических заключений и опыта, которая должна соответствовать указанным требованиям, чтобы избежать опасных условий или негативных последствий при эксплуатации объекта. Для целей работы «расширим» определение критической характеристики робота к определению «актив» – для РТС.

Суть подхода заключается в определении состояния, в которое перейдет актив РТС. Для этого необходимо сформировать массивы состояний, характеризующие степень ее устойчивости при различных внешних воздействиях и при их отсутствии. Данная задача решается в пять нижеуказанных этапов.

Этап 1

На концептуальном уровне рассмотрим РТС как киберфизическую систему, в которой разнородные физические устройства, вычислительные системы и программные средства взаимодействуют в реальном времени. Необходимо определить и отслеживать оценки изменения технических параметров активов РТС на основе результатов наблюдений за определенные интервалы времени, например $T_1 \in [t_{11}; t_{12}]$ и $T_2 \in [t_{21}; t_{22}]$, при этом T_1 должен быть коротким промежутком времени, а T_2 – большим временным промежутком, значительно превышающим T_1 ($T_1 \ll T_2$).

Этап 2

Описанные критически важные активы, влияющие на безопасность, представим в виде совокупности аппаратной части и программных средств

$$ACT = \left(a_{r_j} \cap a_{p_j}\right), \quad (1)$$

где ACT – множество критически важных активов;

$a_{r_j} \in \left\{a_{r_1},\ a_{r_2}, \dots, a_{r_n}\right\}$ – множество значений параметров аппаратных средств;

$a_{p_j} \in \left\{a_{p_1},\ a_{p_2}, \dots, a_{p_n}\right\}$ – множество значений параметров программных средств.

Этап 3

С помощью вероятностного подхода сформируем значения вероятности отказа аппаратных и программных средств активов при неблагоприятных воздействия на временном интервале T_1, при этом пограничные условия для отказа зададим на основе статистических методов отдельно для аппаратных (2) и программных (3) средств

$$\left\{a_{r_j} \in \{A_r\} |\ A_p \cup Q, q_k^{T_1} \in \{Q\}\right\}, \quad (2)$$

$$\left\{a_{p_j} \in \{A_p\} \middle|\ A_r \cup Q, q_k^{T_1} \in \{Q\}\right\}, \quad (3)$$

где A_r – множество значений параметров аппаратных средств;

A_p – множество значений параметров программных средств для соответствующего множества A_r;

A_p – множество значений параметров программных средств;

A_r – множество значений параметров программных средств для соответствующего множества A_p;

Q – множество дестабилизирующих воздействий на активы РТС.

Этап 4

Условия для нахождения переходной матрицы состояния активов системы при появлении деструктивных воздействий для аппаратных (4) и программных (5) средств определим следующим образом

$$\left\{ \exists! \in \left\{ S_{a_{r_j}} \right\} \middle| \sum_{j=1}^{n} P_{ij} = 1, q_k^{T_1} \right\}, \quad (4)$$

$$\left\{ \exists! \in \left\{ S_{a_{p_j}} \right\} \middle| \sum_{j=1}^{n} P_{ij} = 1, q_k^{T_1} \right\}, \quad (5)$$

где $S_{a_{r_j}}$ – множество оценок значений параметров аппаратных средств;

$S_{a_{p_j}}$ – множество оценок значений параметров программных средств;

P_{ij} – вероятность выполнения задач при неблагоприятных воздействиях для каждого актива системы.

Этап 5

Следующим этапом является формирование значений предкритических состояний и отказа аппаратных средств на временно промежутке T_2 для аппаратных (6) и программных (7) компонентов РТС

$$\left\{ P_{a_{r_j}}(T_2) \in \left\{ S_{a_{r_j}} \right\} \middle| K_{g_j} \in \{1,0\}, q_K^{T_2} \in \{Q\} \right\}, \quad (6)$$

$$\left\{ P_{a_{p_j}}(T_2) \in \left\{ S_{a_{p_j}} \right\} \middle| K_{g_j} \in \{1,0\}, q_K^{T_2} \in \{Q\} \right\}, \quad (7)$$

где $P_{a_{r_j}}$ – вероятность соответствия оценок значений параметров аппаратных средств для предкритического состояния или отказа их;

$P_{a_{p_j}}$ – вероятность соответствия оценок значений параметров программных средств для предкритического состояния или отказа их;

K_{g_j} – коэффициент готовности аппаратных и программных средств при длительном временном интервале T_2.

Сформированные таким образом данные могут использоваться для сравнения состояний активов РТС в реальном масштабе времени, а также спустя определенный длительный интервал времени – в ходе или по завершению эксплуатации активов системы [7].

Заключение

Разработанный подход к оценке изменения критических характеристик робототехнических систем во времени позволяет сформировать значения предкритических состояний и отказа для их аппаратных и программных компонентов, которые, в свою очередь, могут использоваться для сравнения состояний активов системы как в реальном времени, так и после завершения эксплуатации активов.

Литература:

1. *Степенкин А.А.* Доверительная модель информационной безопасности среды многоагентных робототехнических систем // Вопросы кибербезопасности. – 2020. – №6(40). – С. 23-31. – DOI: 10.21681/2311-3456-2020-06-23-31.

2. *Умников Е.В., Грачев Д.В.* Структура системы обеспечения информационной безопасности при имитационном моделировании робототехнических комплексов // Известия Института инженерной физики. – 2021. – №3(61). – С. 81-86.

3. *Антохин Е.А., Воронин Л.Л., Москвитина Е.В.* Актуальные вопросы обеспечения информационной безопасности робототехнических комплексов военного назначения // Colloquium-Journal. – 2020. – №25-1(77). – С. 33-37.

4. *Мещеряков Р.В., Исхаков С.Ю.* О проблемах анализа данных в системах управления инцидентами безопасности роботов /

Информационные технологии и системы: труды Восьмой Всероссийской научной конференции с международным участием. – Ханты-Мансийск: АУ «Югорский НИИ информационных технологий», 2020. – С. 108-114.

5. *Петренко В.И., Тебуева Ф.Б., Павлов А.С., Стручков И.В.* Анализ рисков нарушения информационной безопасности в роевых робототехнических системах при масштабировании численности агентов // Прикаспийский журнал: управление и высокие технологии. – 2022. – №2(58). – С. 92-109. – DOI: 10.54398/20741707_2022_2_92.

6. *Холмогоров В.Н., Порохненко К.А.* Информационная безопасность интерфейса RS-232 при реализации робототехнических систем // Наука настоящего и будущего. – 2020. – Т. 1. – С. 204-205.

7. *Mamchenko M.V., Romanova M.A., Trefilov P.M.* Defining the Critical Characteristics of Unmanned Vehicles in a Smart City // IFAC-PapersOnLine. – 2021. – Vol. 54(13). – P. 488-492. – DOI: 10.1016/j.ifacol.2021.10.496.

Рожнов А.В.

Обоснование развития информационно-аналитической системы при реализации гибридных моделей технологии анализа среды функционирования в задачах прогнозного моделирования

Аннотация: Предлагается к обсуждению ряд поисковых вопросов реализации взаимоувязанных новых элементов гибридных моделей в ходе мезосистемной интеграции и рассмотрения базовых вариантов развития информационно-аналитической системы. Основное внимание фокусируется на особенностях и обозримой перспективе решения задач прогнозного моделирования посредством возможностей применения технологии анализа среды функционирования сложных систем на основе «3D» – ситуационного центра.

Ключевые слова: анализ среды функционирования, гибридные модели, единая технология, информационно-аналитическая система, мезосистемная интеграция,