МИНОБРНАУКИ РОССИИ

Федеральный исследовательский центр «Информатика и управление» РАН
Национальный комитет РАН по распознаванию образов
и анализу изображений
Институт информационных технологий Министерства науки и образования
Азербайджанской Республики
Институт проблем передачи информации им. А. А. Харкевича РАН
Белорусский государственный университет
Национальный исследовательский Томский государственный университет
Федеральный исследовательский центр «Карельский научный центр РАН»
Ошский государственный университет
Юго-Западный государственный университет

ОПТИКО-ЭЛЕКТРОННЫЕ ПРИБОРЫ И УСТРОЙСТВА В СИСТЕМАХ РАСПОЗНАВАНИЯ ОБРАЗОВ И ОБРАБОТКИ ИЗОБРАЖЕНИЙ

Распознавание – 2023

Сборник материалов XVII Международной
научно-технической конференции

12–15 сентября 2023 года

Курск
ЮЗГУ
2023

• на первом этапе определить временные интервалы в простейших случаях построения циклограмм управления оборудованием;

• на втором этапе провести анализ параллельных программ функционирования МР, закладываемых в ЭВМ стратегического уровня;

• на третьем этапе решить задачу синтеза оптимальных циклограмм управления мобильными роботами и т. д.

Таким образом, разделенная на иерархические уровни цифровая система управления бортовым оборудованием мобильного робота, включающая ряд параллельно функционирующих подсистем, обеспечивает решение целевых задач за счет генерации оптимальных циклограмм согласованного функционирования бортового оборудования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Fadali M.S., Visioli A. Digital control engineering: Analysis and design. Elsevier Inc., 2013. P. 239–272.

2. Digital control of continuous production with dry friction at actuators / E. Larkin, A. Privalov, A. Bogomolov, T. Akimenko // Smart Innovation, Systems and Technologies. 2022. Vol. 232. P. 427–436.

3. Dirk Th. The linkage tree genetic algorithm // Parallel Problem Solving from Nature. 11th International Conferences, Krakov, Poland, September 11-15. 2010. Berlin, Heidelberg: Springer-verlag, 2010. P. 264–273. DOI 10.1007/978-3-642-15844-5_27.

4. Ларкин Е. В., Богомолов А. В., Акименко Т. А. Моделирование иерархической системы управления группой мобильных роботов // Известия Тульского государственного университета. Серия: Технические науки. 2023. № 2. С. 29–35. DOI 10.24412/2071-6168-2023-2-29-36

УДК 004.056

Р. М. Алгулиев[1], Р. М. Алыгулиев[1], Л. В. Сухостат[1]
e-mail: r.alguliev@gmail.com, r.aliguliyev@gmail.com, lsuhostat@hotmail.com

[1]Институт информационных технологий, г. Баку, Азербайджанская Республика

ОЦЕНКА КРИТИЧНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ОСНОВЕ ГРАФА АТАК

В работе предлагается метод определения критических устройств киберфизических систем с применением байесовского графа атак.

Применение информационных технологий к киберфизическим системам (КФС) и их доступность в сети Интернет делает их привлекательной

мишенью для деструктивных кибератак злоумышленников [1]. Статистика кибератак за последние несколько лет показывает рост числа кибератак на КФС, при этом в большинстве случаев целью атакующего является получение контроля над подсистемой управления.

Наиболее важной задачей является сохранение способности КФС корректно функционировать даже в условиях различных кибератак, поскольку успешное их осуществление может привести к негативным последствиям и экологическим катастрофам, а также к гибели людей.

Злоумышленники нацеливаются на наиболее уязвимые компоненты КФС, которые могут стать отправной точкой для эффективного исследования уязвимостей системы безопасности.

Существующие методы не могут всесторонне анализировать распространенные многоэтапные кибератаки в среде КФС. Мощным инструментом для оценки киберустойчивости КФС является байесовский граф атак. Он предоставляет информацию о причинно-следственных связях между уязвимостями. Уязвимость определяется количественно с использованием общей системы оценки уязвимостей (Common Vulnerability Scoring System, CVSS) и оценок Национальной базы данных уязвимостей.

Цель этой работы – оценить критичность устройств КФС с применением байесовского графа атак. CVSS рассматривается для количественного анализа уязвимостей. Оценки сложности эксплойта берутся как веса ребер графа [2]. В работе рассматриваются следующие метрики оценки уязвимостей: вектор доступа (access vector, AV), базовая оценка (base score, BS), метрика воздействия (γ), оценка возможности реализации (ε) и оценка сложности реализации уязвимости (ξ). Они рассчитываются для *i*-й уязвимости как

$$I_i = 10{,}41 \cdot (1 - (1 - IC_i) \cdot (1 - II_i) \cdot (1 - IA_i)), \quad (1)$$

где IC – конфиденциальность, II – целостность и IA – доступность.

$$BS_i = roundTo1Decimal(((0{,}6 \cdot I_i) + (0{,}4 \cdot E_i) - 1{,}5) \cdot f(I_i)), \quad (2)$$

где

$$f(I_i) = \begin{cases} 0, & \text{если } I_i = 0; \\ 1{,}176 & \text{в противном случае.} \end{cases} \quad (3)$$

Оценка сложности реализации уязвимости определяется как [3]

$$\xi = 10 - \frac{\varepsilon}{AV}, \quad (4)$$

где ε – оценка возможности использования AV.

Чем меньше ξ, тем легче злоумышленнику скомпрометировать этот узел КФС (табл.).

Информация об уязвимостях КФС

Тип устройства	Уязвимость	Уровень КФС	BS	γ	ε	AV	ξ
FTP Сервер	CVE-2014-4877	DMZ	9,3	10,0	8,6	1,0	1,4
Historian	CVE-2019-0211	DMZ	7,2	10,0	3,9	0,395	0,1
Web-сервер	CVE-2014-4881	Уровень управления	5,4	6,4	5,5	0,64	1,4
Инженерная рабочая станция	CVE-2019-0708	Уровень управления	10,0	10,0	10,0	1,0	0,0
Рабочая станция оператора	CVE-2014-4684	Уровень управления	6,0	6,4	6,8	1,0	3,2
ПЛК	CVE-2021-22681	Уровень управления	7,5	6,4	10,0	1,0	0,0

В результате удалось выявить наиболее критичные устройства КФС. Доказана необходимость совершенствования мер безопасности при защите инженерных рабочих станций КФС, наиболее часто подвергающихся кибератакам, как показали последние исследования.

Данная работа выполнена при поддержке Научного фонда Государственной нефтяной компании Азербайджанской Республики (SOCAR) (Контракт No. 3LR-AMEA).

СПИСОК ЛИТЕРАТУРЫ

1. Fawzi H., Tabuada P., Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks // IEEE Transactions on Automatic Control. 2014. Vol. 59, no. 6. P. 1454–1467.

2. Efficient attack graph analysis through approximate inference / L. Muñoz-González, D. Sgandurra, A. Paudice, E. C. Lupu // ACM Transactions on Privacy and Security. 2017. Vol. 20, no. 3. P. 1–30.

3. Analysis of stepping-stone attacks in internet of things using dynamic vulnerability graphs / M. Gamarra, S. Shetty, O. Gonzalez [et al.] // Modeling and Design of Secure Internet of Things. 2020. Vol. 12. P. 273–294.