DOI:

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ОБЛАЧНОГО СЕРВИСА В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ АСУ ТП

Самошина А.И., Промыслов В.Г., Камешева С.Б., Галин Р.Р.

Институт проблем управления им. В.А. Трапезникова РАН, Россия, г. Москва ул. Профсоюзная д.65

aniamayorova13@mail.ru, v1925@mail.ru, kameshevasaniya@gmail.com, riant.r.galin@yandex.ru

Аннотация: Целью данной работы является разработка программного модуля расчета зон безопасности. Для разработки модуля применена математическая модель, основанная на теории графов. Эта модель позволяет описать отношения между объектами/субъектами политики безопасности. Модуль разрабатывается для облачного сервиса моделирования АСУ ТП omole.ws.

Ключевые слова: безопасность, АСУ, модель, процесс, алгоритм.

Введение

Работа посвящена актуальной проблеме обеспечение информационной безопасности автоматизированной системы управления (АСУ ТП) атомной электростанции (АЭС). Так как АЭС играют важную роль в производстве электроэнергии для многих стран. Они снабжают электроэнергией промышленность, центры, государственные учреждения и жилые районы. Тем не менее история показывает, что даже небольшая атака на АЭС может привести к катастрофическим последствиям для граждан страны, экономики, инфраструктуры и безопасности. В последнее время повышенное внимание уделяется области ядерной кибербезопасности из-за атак или инцидентов, направленных на срыв работы АЭС. Это подчеркивает важность проведения оценок безопасности на АЭС в части, связанной с киберзащитой.

Безопасность цифровых систем, используемых на АЭС, изучается в последнее время из-за резкого увеличения использования информационных и коммуникационных устройств, интеграции устройств цифровых систем управления и взаимосвязи между системами на АЭС. Одной из практик, которая может нанести ущерб атомной промышленности, является использование коммерческого программного обеспечения. Этот тип программного обеспечения не обеспечивает адекватный уровень защиты от внешних угроз и часто рассматривается как прямой способ проникновения в сеть объекта. В большинстве случаев, считается, что АЭС полностью изолирована от интернета и поэтому эта отрасль защищена от кибератак, но это заблуждение. Большая часть коммерческого программного обеспечения обеспечивает подключение к интернету через виртуальные сети такие как VPN. Эти сети в большинстве случаев остаются незарегистрированными и остаются без внимания.

Отсюда следует, что критичность применения АСУ заключается в наличии опасности нарушения нормального режима их функционирования в случае полного или частичного отказа, что может привести к катастрофическим последствиям для людей, других систем и/или окружающей среды.

Дискреционные модели используются для моделирования проблем безопасности информационных систем в сложных системах, таких как АЭС. Облачные сервисы используются для моделирования безопасности таких опасных ситуаций в системах. В данной статье представлены исследования с использованием облачного сервиса omole.ws [9].

1 Зона безопасности АСУ ТП АЭС

1.1 Оформление начальных элементов

В данной работе рассматривается типовая архитектура АСУ ТП АЭС. Любая система имеет свою иерархическую структуру, также и АСУ ТП АЭС (рис.1).

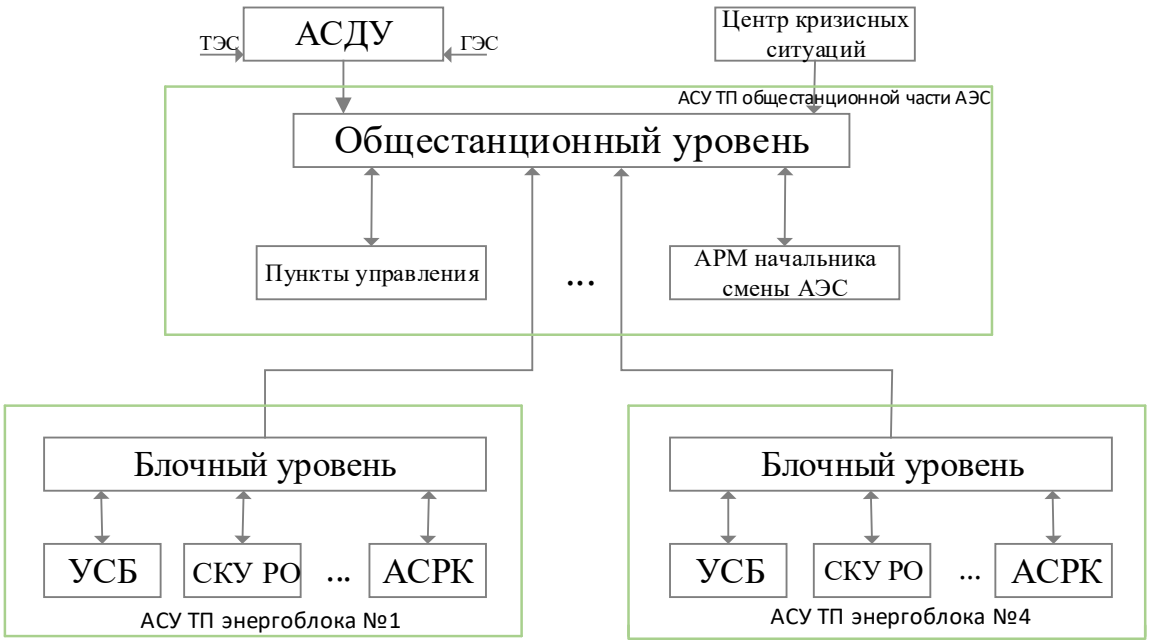

Рис.1 – Иерархическая структура АСУ ТП АЭС.

Исходя из структуры видно, что она имеет свои уровни. Эти уровни важны для безопасности системы в целом. Для удобства защиты такой большой системы удобнее разбить ее не только на уровни, но и на зоны.

Зоной безопасности можно назвать совокупность подзон, к которым предъявлены общие требования безопасности [1-3].

Уровнем безопасности называется определенный комплекс операций, соответствующий одному из типов доступа read, write, take, grant в системе доступной для выполнения субъектом/объектом действий над другими субъектами/объектами. Уровни назначаются, исходя из операций, относящиеся к передаче прав или передачи информации.

2 Алгоритм расчета зон безопасности АСУ ТП АЭС

Существует много математических моделей расчета зон безопасности и самыми распространенными являются методы обхода графа BFS (breadth-first search – поиск в ширину) и DFS (depth-first search – поиск в глубину). Оба метода представляют из себя обход каждой вершины графа. Рассмотрим основные различия между методами BFS и DFS (представлены в таблице 1).

Таблица 1 – Основные различия между BFS и DFS

	BFS	DFS
Алгоритм	Вершинный	Краевой
Структура данных	Очередь	Стек
Метод обхода	Первоначально обходят самые старые вершины, которые еще не посетили	Первоначально обходят вершины по краю
Пространство памяти	Неэффективно	Эффективно
Построение дерева	Широкое и короткое	Узкое и длинное

После рассмотрения сравнения алгоритмов обхода графа видно, что алгоритм DFS больше подходит для расчета зон безопасности АСУ ТП АЭС. Данный граф проходит граф от стартовой вершины до конечной вершины, затем другие вершины до тех пор, пока все не будут рассмотрены.

Алгоритм обхода графа методом DFS представлен на рис.2. [5].

Рис.2 - Алгоритм обхода DFS.

При рассмотрении алгоритма DFS можно сделать вывод, что ребра в графе разделаются на 4 вида:
1 ребра, которые относятся к дереву:

$$\begin{cases} \boldsymbol{arr}(\boldsymbol{u}) < \boldsymbol{arr}(\boldsymbol{v}) \\ \boldsymbol{dep}(\boldsymbol{u}) > \boldsymbol{dep}(\boldsymbol{v}) \end{cases}$$

2 обратные ребра:

$$\begin{cases} \boldsymbol{arr(u) > arr(v)} \\ \boldsymbol{dep(u) < dep(v)} \end{cases}$$

3 ребра на опережение:

$$\begin{cases} \boldsymbol{arr(u) < arr(v)} \\ \boldsymbol{dep(u) > dep(v)} \end{cases}$$

4 ребра, у которых при рассмотрении вершины, вершина не является ни потомком и ни предком:

$$\boldsymbol{arr(v) < dep\ (v) < arr(u) < dep(u)}$$

Алгоритм DFS так же может применяться для:

1. решения головоломок;
2. нахождения компонентов, которые подключены;
3. поиска сильно связанных компонентов;
4. поиска срезанных вершин графа.

Алгоритм DFS для выделения зон безопасности путем обхода графа реализован в облачном сервисе omole.ws в разделе "islands". После выбора зон, в раскрывающемся меню вы можете просмотреть все зоны и пошагово посмотреть, как работает этот алгоритм. В отличие от аналогичных систем, где вы должны сделать весь анализ самостоятельно, в omole.ws можно удобно рассмотреть выделение зон. Это облегчает выделение зон безопасности АСУ ТП АЭС. На рис. 3 показан граф с использованием алгоритма расчета зон безопасности (островов).

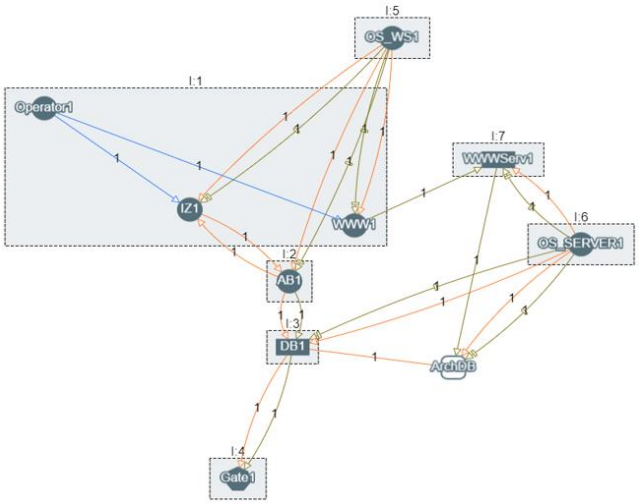

Рис. 3. Отдел АСУ ТП АЭС с выделением островов (зон).

Помимо того, что все четко видно, вы также можете получить готовую документацию во время анализа. Реализованный алгоритм в облачном сервисе omole.ws позволяет загрузить полученную документацию в различных форматах документов. Этот документ содержит описание компонентов, граф с выбранным алгоритмом и таблицу деления на уровни и зоны.

Заключение

В данной работе был проведен сравнительный анализ различных алгоритмов расчета зон безопасности АСУ ТП АЭС. Проведен анализ услуг по моделированию АСУ ТП информационной безопасности. В результате был рассмотрен алгоритм расчета зон безопасности путем обхода графа с использованием метода DFS. Модуль расчета зоны безопасности реализован и подключен к облачному сервису omole.ws.

Литература

1. *Крыжановская Ю.А., Кашко В.В.,* «Разработка комплекса обучающих программ для курса «математические основы защиты информации и информационной безопасности», 2016, сс. 106-111.
2. *K.V. Rudakov,* “Mathematical Foundations for Processing High Data Volume”, Machine Learning, and Artificial Intelligence. Pattern Recognit. Image Anal. 29, (2019) pp. 339–343.
3. *Iskhakov, R. Meshcheryakov, S. Iskhakov, A. Krainov,* “Increase in security of authentication services through additional identification using optimal feature space”, Proceedings of the 4th International

Scientific Research Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM-2017, Tomsk, Russia): Atlantis Press, 2017. Vol. 72. pp. 443-446.
4. *I.I. Galiev, A.N. Chernyaev,* "Choice of APCS for NPP Based on a Set of Reliability and Risk Criteria." At Energy 124, (2018) pp. 154–158.
5. *N.I. Sidnyaev',* "Analytical Calculation for Reliability Validation of Nuclear Power Plants". At Energy 126, (2019) pp. 29–33.
6. *T. Hagerup,* "Space-Efficient DFS and Applications to Connectivity Problems: Simpler, Leaner, Faster". Algorithmica 82, (2020) pp. 1033–1056.
7. *P. Biswas, A. Paul, A. Gogoi, P.Bhattacharya, "*An Efficient Approach for Constructing Spanning Trees by Applying BFS and DFS Algorithm Directly on Non-regular Graphic Sequences". In: Shetty N., Prasad N., Nalini N. (eds) Emerging Research in Computing, Information, Communication and Applications. Springer, New Delh, (2016), pp. 427-436.
8. *T. Everitt, M. Hutter,* "Analytical Results on the BFS vs. DFS Algorithm Selection Problem. Part I: Tree Search". In: Pfahringer B., Renz J. (eds) AI 2015: Advances in Artificial Intelligence. AI 2015. Lecture Notes in Computer Science, vol 9457. Springer, Cham.
9. Omole.ws, Methodical manual. Электронный ресурс, URL: https://omole.ws, Дата обращения: 3 марта 2020.
10. Digital Security Office. Электронный ресурс, URL: https://www.securitylab.ru/ software/270345.php, Дата обращения: 15 февраля 2020.
11. *Refsdal, B. Solhaug, K. Stolen,* Cyber-Risk Management, Springer International Publishing (2015) P. 145.
12. NetAPT. Электронный ресурс, URL: https://www.network-perception.com, Дата обращения: 20 февраля 2020.
13. *Z. Lu, W. Wang, C. Wang,* Modeling and Evaluating Denial of Service Attacks for Wireless and Mobile Applications. Springer International Publishing, (2015) P. 145.
14. Microsoft SDL. Электронный ресурс, URL: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling, Дата обращения: 25 февраля 2020.
15. Threat Modeler. Электронный ресурс, URL: https://threatmodeler.com, Дата обращения: 25 февраля 2020.