Интернет-журнал «Науковедение» ISSN 2223-5167 http://naukovedenie.ru/

Том 9, №3 (2017) http://naukovedenie.ru/vol9-3.php

URL статьи: http://naukovedenie.ru/PDF/18TVN317.pdf

Статья опубликована 18.05.2017

Ссылка для цитирования этой статьи:
Ветлугин К.А., Исаева М.Ф. Использование структурно-логического моделирования при оценке риска информационной безопасности и анализе защищенности и надёжности автоматизированных систем управления производственными и технологическими процессами на объектах, представляющих опасность для жизни и здоровья людей // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №3 (2017) http://naukovedenie.ru/PDF/18TVN317.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.056.5

Ветлугин Константин Александрович
ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I»
Россия, Санкт-Петербург[1]
Аспирант
E-mail: k.a.vetlugin@yandex.ru

Исаева Мария Феликсовна
ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I»
Россия, Санкт-Петербург
Аспирант
E-mail: isaeva@pgups.ru

Использование структурно-логического моделирования при оценке риска информационной безопасности и анализе защищенности и надёжности автоматизированных систем управления производственными и технологическими процессами на объектах, представляющих опасность для жизни и здоровья людей

Аннотация. В данной статье поднимаются проблемы анализа защищенности и надежности автоматизированных систем управления производственными и технологическими процессами на объектах, представляющих опасность для жизни и здоровья людей и окружающей природной среды. В качестве эффективного инструмента анализа защищенности и надежности предлагается моделирование атак с помощью структурно-логического подхода. Таким образом, можно рассмотреть различные сценарии развития ситуации при реализации атаки, а также произвести оценку рисков информационной безопасности, основываясь на полученной модели. В статье также приведены разные методы построения структурно-логических моделей такие, как метод «галстук-бабочка» и деревья атак, рассмотрены их характеристики, определяющие конечную модель сценариев атаки. Приведены примеры коммерческих и свободно распространяемых программных средств, позволяющих создавать деревья атак и деревья событий. Показан пример реализации дерева событий, отображающих разные сценарии развития аварии. Авторы рассматривают способы минимизации рисков нежелательных событий, которые могут привести к ущербу для организации, а также приводят

[1] 190031, Россия, Санкт-Петербург, Московский пр., д. 9

ряд технических и организационных подходов, снижающих вероятность реализации атаки за счет устранения имеющихся уязвимостей. В заключение авторы рекомендуют использовать систему поддержки принятия решений для выбора наиболее подходящего способа минимизации рисков.

Ключевые слова: структурно-логическое моделирование; метод «галстук-бабочка»; деревья атак; оценка рисков; уязвимость; угроза информационной безопасности; оценка защищенности

Железнодорожный транспорт является одним из самых безопасных видов транспорта, однако железная дорогая представляет повышенную опасность как для жизни и здоровья людей, так и для окружающей среды. Кроме того, железная дорога является объектом стратегического значения, что в свою очередь повышает требования к уровню надежности и защищенности систем, функционирующих и внедряемых на сети российских железных дорог.

В современных реалиях безопасное функционирование автоматизированных систем управления производственными и технологическими процессами невозможно без соответствующих средств защиты информации (СЗИ). Перед организациями, эксплуатирующими автоматизированные системы управления производственными и технологическими процессами, встает вопрос целесообразности внедрения тех или иных СЗИ. При выборе СЗИ в первую очередь необходимо руководствоваться существующей нормативной и законодательной базой.

Одним из основных документов, предъявляющих требования к обеспечению безопасности информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды является приказ Федеральной службы по техническому и экспортному контролю от 14.03.2014 № 31[2]. Требования данного документа направленны на обеспечение функционирования автоматизированной системы в штатном режиме, а также на снижение рисков незаконного вмешательства в процессы функционирования автоматизированных систем управления критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов, безопасность которых обеспечивается в соответствии с законодательством Российской Федерации о транспортной безопасности.

При выборе СЗИ необходимо не только руководствоваться законодательством в области информационной безопасности, но и учитывать специфику автоматизированной системы управления, так как в разных автоматизированных системах могут присутствовать разные уязвимости, что приводит к проявлению разных угроз информационной безопасности.

Как говорилось ранее, внедрение и эксплуатация автоматизированных систем требуют использования соответствующих СЗИ, которые зачастую имеют очень высокую стоимость. Более того для обслуживания СЗИ организациям необходимо нанимать новый персонал и формировать структурные подразделения, ответственные за поддержание работоспособности таких систем, что приводит к увеличению расходов. В результате, у организаций возникает

[2] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (http://fstec.ru).

необходимость оценивать выгоду от внедрения СЗИ и производить выбор на множестве альтернатив СЗИ.

Одним из способов определения целесообразности внедрения СЗИ является оценка рисков информационной безопасности, которая позволяет получить комплексную характеристику, учитывающую вероятность реализации угрозы и её ущерб. Оценка и минимизация рисков - это важные элементы управления информационной безопасностью организации.

Наиболее часто риск определяют как произведение ущерба от реализации угрозы информационной безопасности и вероятности её реализации. Математически можно также определить обобщенный показатель риска R_{total}, который представляет собой сумму индивидуальных рисков R_i, которые вычисляются как произведение потенциального ущерба от реализации угрозы L_i и вероятности её реализации $p(L_i)$.

$$R_i = L_i \times p(L_i) \quad (1)$$

$$R_{total} = \sum_i R_i \quad (2)$$

Для получения значений L_i и $p(L_i)$ могут быть использованы статистические и экспертные данные, а также средства математического моделирования. В качестве примеров математических методов можно упомянуть сценарное логико-вероятностное моделирование, метод «галстук-бабочка» (bow-tie analysis), а также метод основанный на построении деревьев атак.

Название метода «галстук-бабочка» обусловлено внешним видом структурно-логической схемы, формируемой при использовании этого метода. В случае анализа защищенности автоматизированной системы в центе такой структурно-логической схемы будет находиться реализация угрозы информационной безопасности (инцидент информационной безопасности), слева - уязвимости, которые могут быть использованы для реализации угрозы, а справа - возможные последствия (варианты ущерба) от реализации угрозы. Метод «галстук-бабочка» является весьма распространенным инструментом для анализа рисков. В нем также используется такое понятие как «барьер», которое обозначает внедряемое средство защиты информации, снижающее вероятность использования какой-либо уязвимости либо минимизирующий ущерб в случае успешной реализации атаки.

Метод, основанный на деревьях атак (attack trees), получил широкое применение на практике, поскольку он является интуитивно понятным и наглядным инструментом для анализа угроз. Цель деревьев атак - определить и проанализировать возможные атаки на автоматизированную систему в структурированном виде.

В простейшем виде дерево атак представляет собой связный ациклический граф:

$$T = (V, E), \quad (3)$$

где: V - множество вершин (возможные уязвимости системы), E - множество связей между вершинами (V_i, V_j), которое отображает этапы проведения атаки.

На практике при формировании деревьев атак используются разные дополнительные параметры, такие как:

- вероятность использования уязвимости (реализации угрозы);
- стоимость атаки;
- величина ущерба от реализации угрозы;

- необходимость специального оборудования;
- прочее.

Таким образом, сценарии атак могут быть представленными разными видами деревьев в зависимости от специфики объекта зашиты. Например, дерево атаки может быть:

- мультиграфом (при возможности попасть из одной вершины в соседнюю разными способами, характеризующими вероятность реализации угрозы/величину ущерба/стоимость атаки и т.д.);
- ориентированным/неориентированным графом;
- взвешенным/невзвешенным графом;
- прочее.

Помимо вышеперечисленного, вершины, имеющее одного предка, могут состоять в отношении конъюнкции/дизъюнкции, что указывает на необходимость использования двух и более уязвимостей для реализации атаки (отношение конъюнкции) или хотя бы одной уязвимости из множества возможных (отношение дизъюнкции).

На сегодняшний день существует множество программных средств, позволяющий моделировать сценарии кибер-атак, в том числе строить деревья атак. Наиболее известными программными средствами для построения деревьев атак являются AttackTree+ от компании Isograph и SecurITree от канадской компании Amenaza Technologies. Также существуют проекты построения деревьев атак с открытым исходным кодом такие, как ADTool, разработанный Университетом Люксембурга, SeaMonster и Ent.

Примером отечественной разработки служит программный комплекс АРБИТР (ПК АСМ СЗМА), который используется не только для решения практических задач в разных организациях, а также успешно внедрен в учебным процесс кафедры «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения Императора Александра I.

Деревья атак являются частным случаем деревьев событий, модели которых могут быть построены с помощью ПК АРБИТР. Дерево событий - логическая диаграмма, используемая для анализа факторов, влияющих на аварию, поломку или нежелательное событие [3].

Пример дерева событий, реализованного в ПК АРБИТР, представлен на рисунке 1.

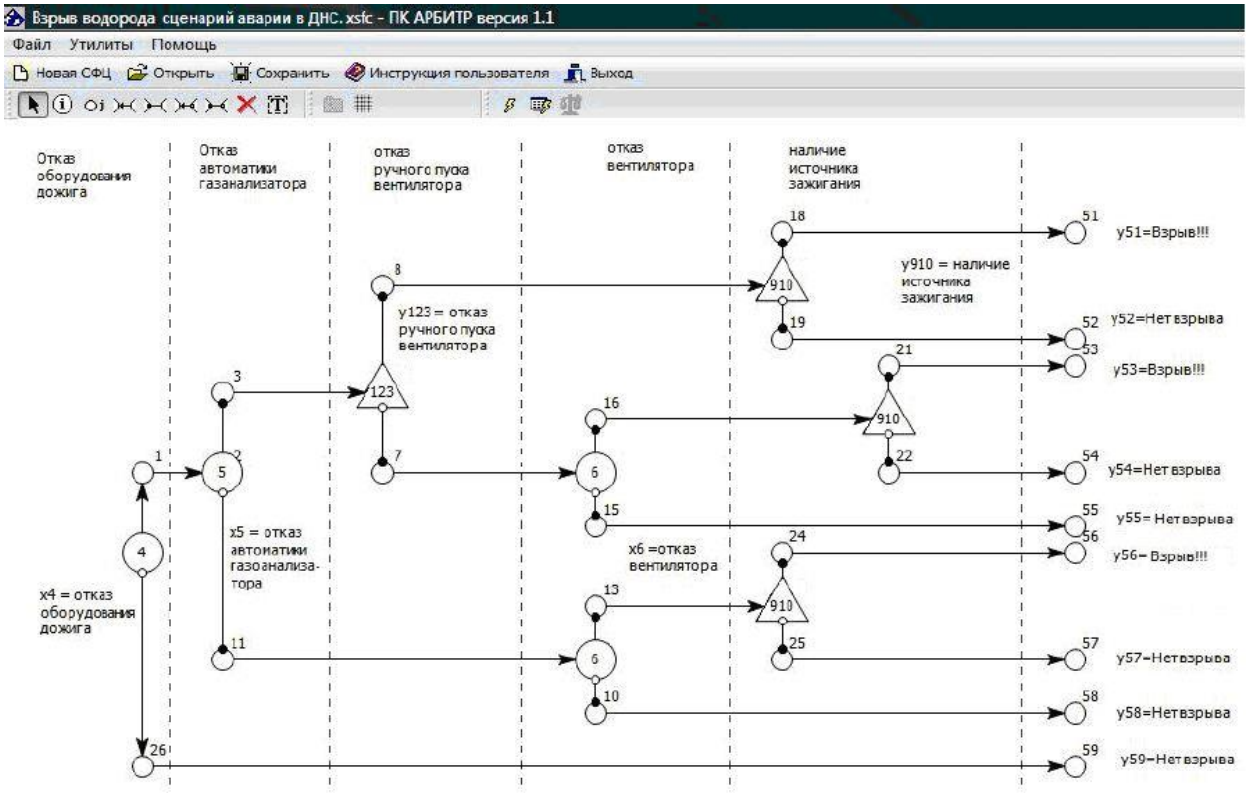

Рисунок 1. *Сценарий развития аварии [3]*

На рисунке 1 вершины дерева событий изображены кружками и треугольниками с цифрами внутри фигур. В графическом редакторе ПК АРБИТР фигуры с цифрами внутри обозначают функциональные и эквивалентированные вершины схемы функциональной целостности. Функциональная вершина - это графическая модель отдельного элемента-события исследуемой системы. Её аналитическими аналогами в логических моделях выступают простые логические переменные, а в вероятностных моделях - характеристики, определяющие вероятности свершения соответствующих собственных случайных событий. Эквивалентированная вершина является эквивалентом (подграфом) другой схемы функциональной целостности. Эквивалентированная вершина может иметь собственную структуру и служить для сокращения размерности основного графа [8].

После построения структурно-логической модели, описывающий всевозможное сценарии развития атаки, и оценки рисков информационной безопасности возникает необходимость выбора средств минимизации рисов. Минимизации рисков можно добиться двумя способами:

- снизить вероятность реализации атаки;
- уменьшить величину ущерба от реализации атаки.

Снижения вероятности атаки достигается внедрением дополнительных СЗИ, которые устраняют имеющиеся уязвимости. В качестве СЗИ могут быть внедрены:

- антивирусное программное обеспечение (автоматизированные рабочие места пользователей);
- межсетевые экраны;
- криптографические средства защиты;
- модуль доверенной загрузки;

- прочее.

Уменьшение вероятности атаки также может быть достигнуто организационными средствами защиты информации:

- обучение и организация работы с персоналом;
- организация внутриобъектового и пропускного режимов и охраны;
- проведение внутреннего и внешнего аудитов информационной безопасности;
- прочее.

Уменьшение величины ущерба от реализации атаки зачастую достигается экономическими методами, например, страхование как способ переноса риска нежелательного события на другую организацию.

При выборе средств по минимизации рисков могут использоваться системы поддержки принятия решений (СППР). Особо острая необходимость в СППР может возникнуть при большом количестве сценариев всевозможных атак, которые визуализируются структурно-логическими схемами внушительных размеров. В таких условиях выбор оптимального решения практически невозможен без применения СППР.

В заключение необходимо отметить, что существуют множество других методов оценки рисков информационной безопасности, но моделирование угроз с помощью структурно-логического подхода (например, деревья атак) позволяет проследить динамику и сценарии развития атак и визуализировать полученные результаты.

ЛИТЕРАТУРА

1. Ветлугин К.А., Корниенко А.А., Струков А.В. Сценарный логико-вероятностный подход к анализу надежности и защищенности инфокоммуникационных систем // Сборник материалов V Международной научно-практической конференции. - 2015. С. 330-332.
2. Ададуров С.Е., Глухов А.П., Диасамидзе С.В., Еремеев М.А., Корниенко А.А., Яковлев В.А. Информационная безопасность и защита информации на железнодорожном транспорте: учебник: в 2 ч. / С.Е. Ададуров и др.; под ред. А.А. Корниенко. - М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - 440 с.
3. Гладкова И.А., Струков А.А., Струков А.В. «Сценарное логико-вероятностное моделирование опасной ситуации с использованием ПК ПРБИТР». Сб. докладов II международной научно-практической конференции ИКМ МТМТС 2013, СПб, ОАО «ЦТСС», 2013, С. 50-54.
4. Alexander V. Strukov Reliability assessment for three-state element systems using ARBITR software // International Journal of Risk Assessment and Management, Vol. 18, Nos. 3/4, 2015. P. 266-275.
5. Диасамидзе С.В., Корниенко А.А. Аудит и управление информационной безопасностью: учеб. пособие / А.А. Корниенко, С.В. Диасамидзе. - СПб.: Петербургский гос. университет путей сообщения, 2011. - 83 с.

6. Anatoly Kornienko, Mark Polyanichko, Dmitry Efanov. Methodological aspects of detection and resolution of conflicts of train control systems information security software // IEEE EWDTS 2016, Yerevan, October, 14-17, 2016. - P. 209-213.
7. С.Е. Ададуров, С.В. Диасамидзе, А.А. Корниенко, А.А. Сидак Международная кибербезопасность на железнодорожном транспорте: методологические подходы и нормативная методическая база // Вестник ВНИИЖТ. - 2015, №6. С. 9-15.
8. Поленин В.И., Рябинин И.А., Свирин С.К., Гладкова И.А. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства/ Под научным редактированием Можаева А.С. СПб.: NIKA, 2011.
9. Ветлугин К.А., Струков А.В. Алгоритмы автоматизированного структурно-логическогомоделирования надежности и безопасности информационных и телекоммуникационных систем / К.А. Ветлугин, А.В. Струков: учеб. пособ. - СПб.: ФГБОУ ВО ПГУПС, 2016. - 47 с.
10. А.А. Нозик, А.В. Струков, И.А. Можаева. Особенности программной реализации методов количественного анализа риска аварий ОПО на основе логико-вероятностного моделирования // Промышленность и безопасность, №8(106), 2016. - С. 42-47.

Vetlugin Konstantin Alexandrovich
Emperor Alexander I St. Petersburg state transport university, Russian, Saint Petersburg
E-mail: k.a.vetlugin@yandex.ru

Isaeva Mariia Feliksovna
Emperor Alexander I St. Petersburg state transport university, Russian, Saint Petersburg
E-mail: isaeva@pgups.ru

Using structural-logical modeling in the risk assessment of information security, in security and reliability analysis of automated control systems of production and technological processes on the objects presenting danger to life and health of people

Abstract. Problems of security analysis and reliability of automated control systems of production and technological processes on the objects presenting danger to life and health of people and the natural environment are introduced in this article. Attack modeling using the structural-logical approach is considered as an effective tool of security analysis and reliability. Thus, it is possible to consider different scenarios of situation development while the attack is implemented, as well as to assess information security risk, based on the obtained model. The article also lists the different methods of construction of structural-logical models such as the method of bow-tie analysis and attack trees, their characteristics are examined, which determine the final model attack scenarios. Examples of commercial and freely distributable software that lets you create attack trees, and event trees are presented. Sample implementation of the event tree that shows different scenarios of the accident is shown. The authors examine ways to minimize risks of undesirable events that can cause damage to the organization as well as lead a number of technical and organizational approaches that reduce the probability of attack by removing existing vulnerabilities. In conclusion, the authors recommend the use of a decision support system for selecting the most appropriate method of risk mitigation.

Keywords: structural-logical modeling; bow-tie analysis; attack trees; risk assessment; vulnerability; threat of information security; security assessment