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

Том 9, №4 (2017) http://naukovedenie.ru/vol9-4.php

URL статьи: http://naukovedenie.ru/PDF/01TVN417.pdf

Статья опубликована 09.07.2017

Ссылка для цитирования этой статьи:
Струков А.В., Ветлугин К.А. О методах количественного анализа кибербезопасности технических систем на основе логико-вероятностного подхода // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №4 (2017) http://naukovedenie.ru/PDF/01TVN417.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.052

Струков Александр Владимирович
Акционерное общество «Специализированная инжиниринговая компания «Севзапмонтажавтоматика»
Россия, Санкт-Петербург[1]
Ведущий специалист исследовательского отдела
Кандидат технических наук, доцент
E-mail: alexander_strukov@szma.com

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

О методах количественного анализа кибербезопасности технических систем на основе логико-вероятностного подхода

Аннотация. Авторами данной статьи рассмотрено содержание логико-вероятностного подхода к анализу кибербезопасности автоматизированных систем управления технологическими процессами. Сущность данного подхода состоит в том, что система как некоторая структура описывается как топология взаимосвязанных элементов. Взаимосвязи исследуемых элементов описываются функциями алгебры логики, образующими системы логических равенств. Обосновано использование методологии оценки надежности и риска для анализа кибербезопасности технических систем, даны рекомендации по выбору методов анализа технических рисков. Анализ риска современных технических систем представляет собой сложную комплексную задачу системного анализа, которая предполагает использование соответствующих программных средств. Приведены примеры методов количественного анализа риска в программной среде ПК «АРБИТР». Показано, что программная реализация технологии деревьев атак для описания потенциальных угроз и способов атак, реализующих эти угрозы, возможны путем сокращения функциональных возможностей программного комплекса, предназначенного для анализа надежности сложных систем. Приведен пример учета отказов по общей причине при анализе надежности резервируемых систем в задачах анализа функциональной безопасности. Также продемонстрирован пример программной реализации деревьев атак для web-доступной автоматизированной системы управления технологическим процессом.

[1] 199106, Россия, г. Санкт-Петербург, 26-я линия В.О., д. 15, корп. 2, лит. А Бизнес-центр «Биржа»

Ключевые слова: анализ надежности; оценка риска; кибербезопасность; дерево неисправностей; дерево событий; дерево атак; схема функциональной целостности; отказы по общей причине; функциональная безопасность

Введение

В настоящее время основным направлением развития кибербезопасности автоматизированных систем управления технологическими процессами (АСУТП) является исследование возможности и целесообразности использования теоретических разработок, методических приемов и практического опыта, накопленного в области информационной безопасности, анализа надежности и риска сложных технических систем. Наиболее часто специалисты в области кибербезопасности АСУТП обращают свое внимание на методический аппарат трех дисциплин: промышленной безопасности в вопросах оценки ущерба от риска аварий, функциональной безопасности в вопросах оценки эффективности средств защиты и информационной безопасности в вопросах реализации по защите непосредственно информационных ресурсов. Это позволяет определить кибербезопасность как процесс обеспечения функционирования АСУТП за счет снижения вероятности реализации опасных отказов, вызывающих недопустимый ущерб, при заданном уровне экономической эффективности технологического объекта с учетом возможного негативного антропогенного информационного воздействия на компоненты АСУТП.

Логико-вероятностный подход

По аналогии с определением логико-вероятностной теории безопасности (ЛВТ) профессора Рябинина И.А. [1], сущность логико-вероятностного подхода к анализу кибербезопасности выражается в формировании основных закономерностей развития знаний о возможных изменениях состояний технической системы не только в условиях штатной (нормальной) эксплуатации, но и при:

а) наличии внешних воздействий;

б) нарушениях правил эксплуатации;

в) преднамеренных зловредных действиях нарушителя (угроз, атак).

Отличительной чертой анализа кибербезопасности такого класса технических систем как автоматизированные системы управления технологическими процессами (АСУТП) является пересечение задач безопасности функционирования объекта управления (ОУ), функциональной безопасности аппаратно-программных средств защиты и информационной безопасности. При этом конечной целью и критерием выполнения задач кибербезопасности является обеспечение правильного и надежного функционирования ОУ.

Поэтому современный подход к анализу надежности АСУТП должен учитывать тот факт, что атрибутами надежности таких систем следует считать не только безотказность, ремонтопригодность и готовность, но и безопасность, конфиденциальность и целостность [2].

Расширенное понятие надежности (dependability – надежный, заслуживающий доверие) современных информационных и автоматизированных технических систем базируется на понимании того, что кроме феноменологических причин возникновения неисправностей в аппаратной части (естественные отказы элементов, человеческие ошибки) возможны неисправности программного обеспечения, вызванные преднамеренными вредоносными действиями. То есть неисправности возможны не только в домене физическом, но и в домене информационном.

Новый подход включает в себя анализ последствий кибератак с учетом их влияния на промышленную безопасность в смысле надежности и безопасности функционирования ОУ и на количественные экономические показатели. Такой подход к анализу кибербезопасности АСУТП является функциональным и риск-ориентированным и предполагает решение задач оценивания не только успешности/неуспешности самой кибератаки, но и сохранения устойчивого функционирования АСУТП и ОУ путем их адаптации к результатам кибервторжения (несанкционированного проникновения).

Первоочередной задачей ЛВТ кибербезопасности технических систем является разработка методов расчета показателей безопасности. Не отрицая необходимости разработки особенных, присущих только задачам информационной безопасности, методов анализа кибератак, и учитывая, что, конечной целью анализа является обеспечение именно надежного функционирования ОУ, следует при анализе опасностей, связанных с отказами АСУТП, оценивать технический риск, показатели которого определяются соответствующими методами теории надежности, представленными в таблице 1. При этом методы анализа надежности технических систем рекомендуется сочетать с методами моделирования аварий и количественной оценки риска аварий.

Таблица 1

Рекомендации по выбору методов анализа риска[2]

Метод	Вид деятельности				
	Предпроектные работы	**Проектирование**	**Ввод/вывод из эксплуатации**	**Эксплуатация**	**Реконструкция**
Проверочный лист	+	+	+	+	+
Анализ «Что будет, если…?»	**0**	+	++	++	+
Предварительный анализ опасностей (идентификации опасностей)	++	+	**0**	**0**	+
Анализ опасности и работоспособности	+	++	+	+	++
Анализ видов и последствий отказов	+	++	+	+	++
Анализ деревьев отказов и событий	**0**	++	+	+	++
Количественный анализ риска	++	++	+	+	+
Анализ барьеров безопасности	+	++	+	+	+

В таблице 1 приняты следующие обозначения:
«0» – наименее подходящий метод анализа;
«+» – рекомендуемый метод;
«++» – наиболее подходящий метод.

Важным и в настоящее время активно развивающимся элементом методического аппарата анализа риска и моделирования угроз является структурно-логический метод. Суть метода состоит в том, что система как некоторая структура описывается как топология взаимосвязанных элементов (оборудование, материалы, программное обеспечение, персонал), которые однозначно определяют состояния системы. Взаимосвязи элементов описываются

[2] Руководство по безопасности «Методические основы по проведению анализа опасностей и оценки риска аварий на опасных производственных объектах». Серия 27. Выпуск 16. – М.: ЗАО «Научно-технический центр исследований проблем промышленной безопасности, 2016. – 56 с.

функциями алгебры логики (ФАЛ), образующими системы логических равенств. На основе теоретического положения о том, что всякая система логических равенств замещается одним равенством и притом в весьма различных формах [3], формируются критерии нахождения исследуемой системы в безопасных, предопасных (критичных) и опасных (аварийных) состояниях.

Автоматизированное структурно-логическое моделирование в задачах анализа риска

Анализ риска современных технических систем представляет собой сложную комплексную задачу системного анализа, выполнение которого даже при наличии разработанного методического обеспечения невозможно или крайне затруднено без использования соответствующих программных средств.

К таким программным средствам относится программный комплекс (ПК) «АРБИТР» [4], разработанный в «Специализированной инжиниринговой компании «Севзапмонтажавтоматика» и аттестованный Ростехнадзором РФ, аттестационный паспорт № 222 от 21 февраля 2007 г.

Универсальной графической интерпретацией структурно-логического метода, реализованного в ПК АРБИТР, являются схемы функциональной целостности (СФЦ), позволяющие использовать методики построения блок-схем, деревьев неисправностей, деревьев событий, а также методику «галстук-бабочка» [4, 7], совмещающую на одном экранном интерфейсе перечисленные выше графические построения. Важно отметить, что свойство функциональной целостности включает в себя возможность отображения состава элементов системы, их взаимосвязей и позволяет определять условия реализации выходного эффекта. Это свойство имеет большое практическое значение, например, при выполнении первичного структурно логического моделирования на этапе построения деревьев неисправностей. Зачастую опытные разработчики или специалисты по эксплуатации АСУТП достаточно уверенно представляют блок-схему работоспособности анализируемой системы. Формирование списка минимальных сечений отказов (МСО) и доказательство его полноты и минимальности часто вызывает трудности.

В этом случае после разработки блок-схемы работоспособности в виде СФЦ решение обратной (инверсной) задачи позволяет получить гарантированно полный набор МСО.

На рис. 1 приведен фрагмент экранного интерфейса ПК АРБИТР, иллюстрирующий графическое представление опасного события и связанных с ним событий с помощью СФЦ, позволяющей реализовывать алгоритмы анализа дерева неисправностей и дерева событий в рамках единого интерфейса. В левой части схемы построено дерево неисправностей, модель которого описывает последовательность отказов и причин, приводящих к опасному событию. Для этих целей также может быть использован метод структурных схем надежности с инверсным критерием выходного события. Вершинное событие этой части схемы характеризуется рассчитанным значением вероятности (частоты) опасного события (реализации) события.

В правой части схемы построено дерево событий, модель которого описывает последовательность событий и отказов, приводящих к эскалации опасного события. В правой части СФЦ получена модель 8 сценариев развития аварии (эскалации). Каждому сценарию (фиктивные вершины №34-41) приписана мера последствий $w_i, i = 1, \dots, 8$ (столбец «Ущерб» в правой части экрана).

Значения ущерба для каждого сценария возникновения аварии могут, например, быть выражены в материальных потерях продукции или затратах на восстановление производства, или в некоторых условных единицах (у.е.).

По формуле взвешенного среднего может быть получена оценка W ущерба для исследуемой опасности

$$W = \sum_{i=1}^{8} p_i w_i, \quad (1)$$

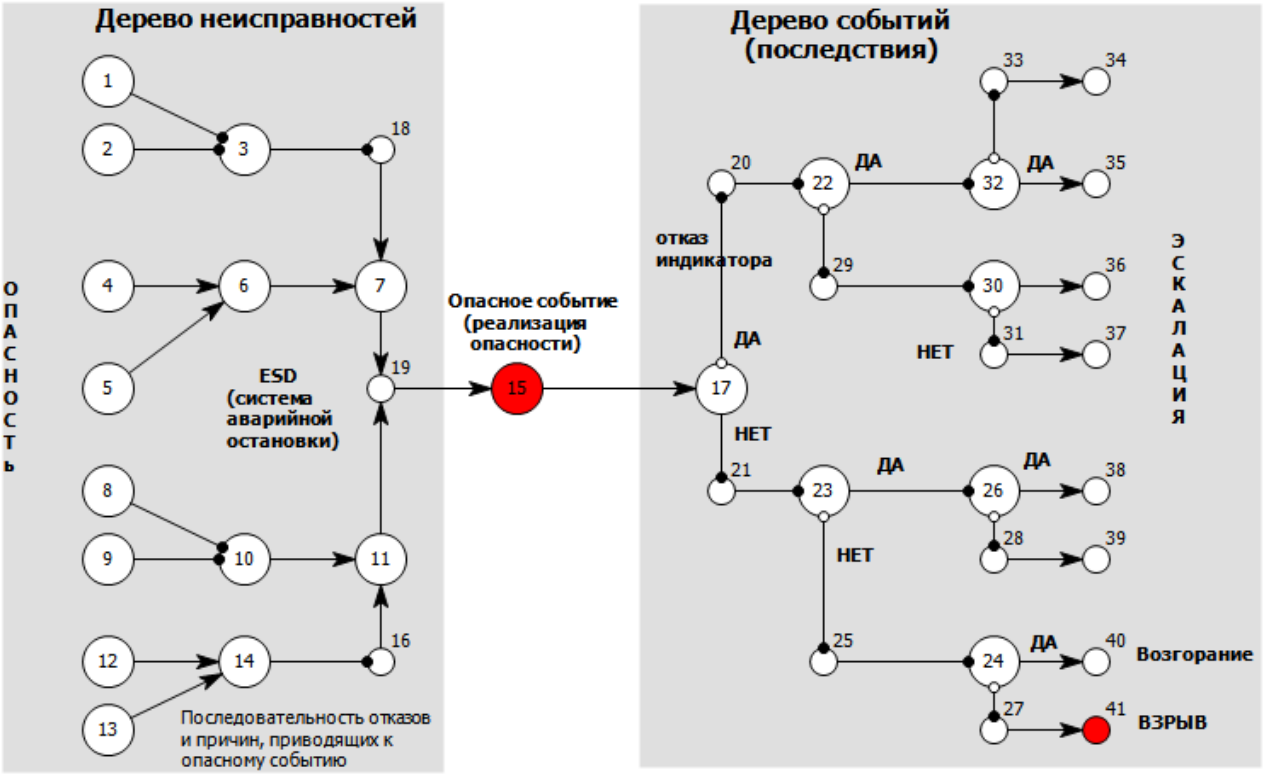

Рисунок 1. *Совместное применение методов анализа деревьев неисправностей и деревьев событий в программной среде ПК АРБИТР [5]*

Современной тенденцией развития компьютерных методов структурно-логического анализа кибербезопасности технических систем является использование технологии деревьев атак (ДА) для описания потенциальных угроз и способов атак, реализующих эти угрозы. ДА представляют собой мульти-уровневые диаграммы, состоящие из одного корня, листьев и потомков. При построении ДА используют булевы выражения для описания условий, при которых дочерние узлы обеспечивают реализацию родительских узлов. Наиболее часто при этом используют сокращенный набор логических операторов (гейтов), ограничиваясь операторами «ИЛИ», «И», «К из N». В то же время событию ДА могут быть приписаны не только вероятностные характеристики, но и детерминированные свойства (стоимость, объем оборудования и т.д.). В этом случае пользователь может задавать арифметические действия, которые должны выполняться над детерминированными свойствами событий. Например, при представлении логической функции вершинного события в виде ДНФ могут определяться действия над детерминированными характеристиками событий в конъюнкциях (сложение, нахождение минимума/максимума, среднего) и над детерминированными характеристиками отдельных конъюнкций в дизъюнкции.

Компьютерная реализация метода ДА может быть реализована, в частности, сокращением функциональных возможностей программы, предназначенной для анализа надежности сложных систем. Примером такой реализации можно назвать программу AttackTree компании Isograph[3]. Отечественным программным средством, реализующим методы ДА, является разрабатываемый ПК АРБИТР-АТ.

На рисунке 2 приведен фрагмент экранного интерфейса ПК АРБИТР-АТ, иллюстрирующий построение ДА для анализа кибербезопасности Web-доступной АСУТП [8] с использованием эквивалентированных вершин (вершины обозначены треугольниками), внутри которых могут быть реализованы алгоритмы получения количественных мер оценки, причем не только вероятностей реализации угрозы, но и детерминированных характеристик уязвимости, стоимости атаки и т.д.

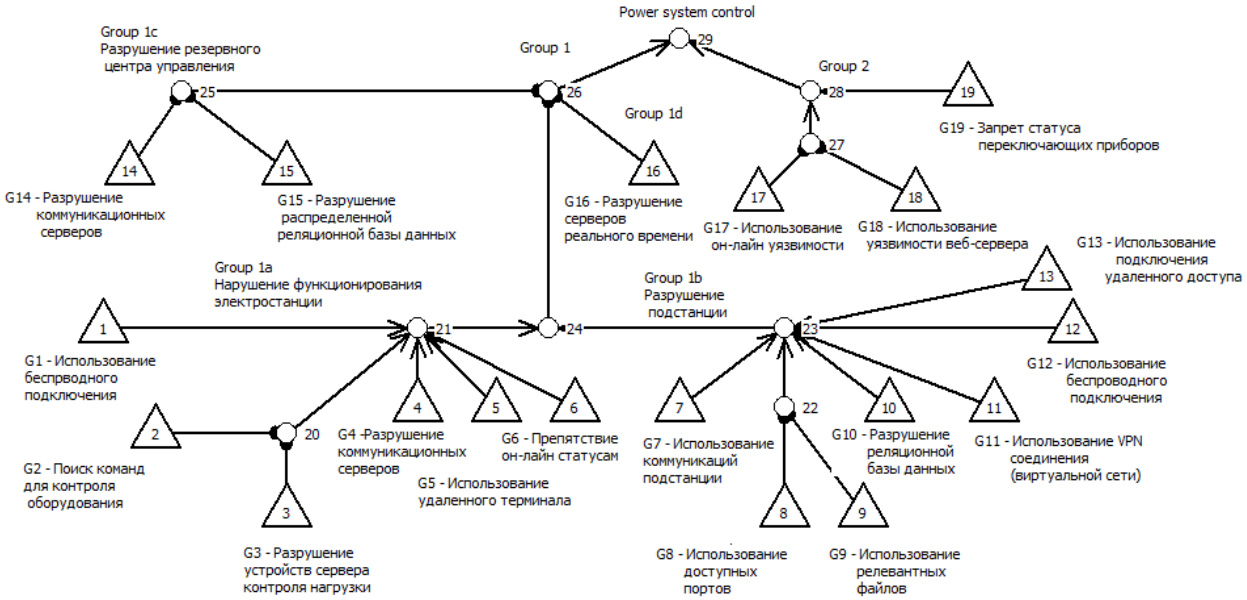

Рисунок 2. *Дерево атак для Web-доступной АСУТП (составлено авторами)*

Автоматизированное структурно-логическое моделирование в задачах анализа функциональной безопасности

Одной из задач анализа функциональной безопасности АСУТП является, в частности, анализ надежности систем безопасности с учетом отказов по общей причине (ООП).

В стандарте ГОСТ Р МЭК 61508-4-2007 (п.3.6.10)[4] дано следующее определение отказа по общей причины (Common cause failure – CCF) – отказ, который является результатом одного или нескольких событий, приводящих к одновременному отказу двух или более отдельных каналов в многоканальной системе, ведущих к отказу системы в целом.

Одним из способов введения ООП в модель надежности (безопасности) системы является явное отображение таких событий непосредственно на дереве неисправностей аналогично независимым отказам. Считается, что точный учет специфики конкретной задачи

[3] http://www.isograph.com/software/attacktree/ (Дата обращения 22.05.2017).

[4] ГОСТ Р МЭК 61508-4-2013 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения.

анализа риска может быть реализован только с использованием явного отображения всех событий и причин непосредственно на дереве [8].

На рисунке 3 представлена СФЦ дублированной системы, отказ которой моделируется с учетом ООП введением события №3 – отказа по общим причинам одновременно двух элементов CCF{1,2}.

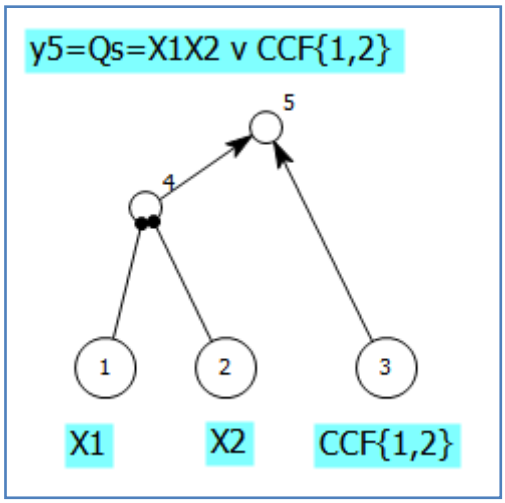

Рисунок 3. *СФЦ дублированной системы с учетом ООП (составлено авторами)*

Решение по логическому критерию «y_5» формирует логическую функцию «Отказ системы» вида

$$y_5 = X_1X_2 \vee CCF\{1,2\}, \quad (2)$$

где: X_1, X_2 – логические переменные, описывающие независимые отказы элементов №1 и №2;

CCF{1,2} – логическая переменная, описывающая отказ одновременный элементов №1 и №2 по общей причине.

Для перехода к вероятностной функции и вычисления вероятности отказа системы воспользуемся алгоритмом ортогонализации [8, 9]. Тогда уравнение (2) может быть записано в виде:

$$y_5 = X_1X_2\overline{CCF\{1,2\}} \vee CCF\{1,2\}, \quad (3)$$

где $\overline{CCF\{1,2\}}$ – операция инверсии.

Подставляя в (3) вероятности истинности логических переменных получим выражение для расчета вероятности отказа дублированной системы с учетом ООП:

$$Q_s = \Pr\{y_5 = 1\} = Q_1Q_2(1 - Q_{CCF}) + Q_{CCF}, \quad (4)$$

где: $\Pr\{X_1 = 1\} = Q_1$, $\Pr\{X_2 = 1\} = Q_2$ – вероятности независимых отказов элементов №1 и №2 дублированной системы соответственно;

$\Pr\{CCF\{1,2\} = 1\} = Q_{CCF}$ – вероятность отказа элементов №1 и №2 по общей причине.

Современная программная реализации методов оценки риска аварий с учетом ООП предполагает возможность автоматического виртуального построения расширенного дерева отказов без изменения графического изображения стандартного дерева неисправностей. Такой подход значительно упрощает процедуру анализа риска, размерность которой значительно увеличивается при учете ООП.

При использовании алгоритмов автоматического учета ООП следует внимательно относиться к тем допущениям и предположениям, которые легли в основу программно реализованного метода. Использование упрощенных методов допустимо только для очень простых по структуре систем и небольшого числа элементов.

Во-первых, следует учитывать особенности исходной информации об отказах элементов. Во-вторых, при вхождении в группу ООП элементов с разными показателями надежности необходимо использовать специфические подходы и методики.

Существуют два вида представления исходной информации об ООП.

В первом случае статистика отказов элемента включает в себя статистику ООП (режим «Adjust independent Q» в терминологии Isograph).

Во втором случае статистика отказов элемента не включает в себя статистику ООП (режим «No adjust independent Q» в терминологии Isograph).

Для примера рассмотрим простейшую модель β-фактора, в которой коэффициент β определяет долю отказов ООП от исходной известной интенсивности или вероятности отказов элемента.

В первом случае вероятность отказа по общей причине является частью общей вероятности отказа Q_{tot}, то есть $Q_{CCF} = \beta\, Q_{\text{tot}}$. Тогда вероятность независимого отказа равна $Q_i = (1-\beta)\, Q_{\text{tot}}$. Следовательно $Q_{\text{tot}} = Q_i + Q_{CCF}$.

Во втором случае принимается $Q_i = Q_{\text{tot}}$.

Покажем влияние различия задания исходных данных на простом примере расчета вероятности отказа дублированной системы.

Пусть заданы следующие исходные данные: $\beta = 0.05$ и $Q_1 = Q_2 = 0.01$.

Тогда в первом случае вероятность отказа по общей причине $Q_{CCF} = \beta \cdot Q_1 = \beta \cdot Q_2 = 0.05 \cdot 0.01 = 0.0005$.

Вероятность единичного (независимого) отказа элемента №1 или №2 будет $Q_{1i} = Q_{2i} = (1-\beta) \cdot Q_1 = (1-\beta) \cdot Q_2 = (1-0.05) \cdot 0.01 = 0.0095$.

Следовательно, вероятность отказа дублированной системы согласно (4) равна

$$Q_s = Q_{1i}Q_{2i}(1-Q_{CCF}) + Q_{CCF} = 0.0095^2(1-0.0005) + 0.0005 = 0.0005902. \quad (5)$$

Для второго случая вероятность отказа по общей причине также равна $Q_{CCF} = \beta \cdot Q_1 = \beta \cdot Q_2 = 0.05 \cdot 0.01 = 0.0005$. Но вероятности независимых отказов элемента № 1 или № 2 примут значения исходных (не пересчитанных) вероятностей отказов, то есть $Q_{i1} = Q_{i2} = 0.01$.

В этом случае вероятность отказа дублированной системы согласно (4) равна

$$Q_s = Q_{1i}Q_{2i}(1-Q_{CCF}) + Q_{CCF} = 0.01^2(1-0.0005) + 0.0005 = 0.00059995. \quad (6)$$

Анализ результатов, полученных по формулам (5) и (6), показывает:

- вероятность отказа дублированной системы с учетом ООП существенно определяется вкладом событий ООП. Несложно показать, что увеличение кратности резервирования практически не повлияет на величину вероятности

отказа. Этот факт наглядно подтверждается расчетами вероятности отказа на запрос систем безопасности типовых структур[5];

- если статистика ООП не входит в исходные данные об отказах элементов структуры, то расчет с прогнозированием ООП дает пессимистическую оценку надежности резервированных структур.

Практика эксплуатации ответственных АСУТП показывает, что такие пессимистические оценки ближе к реальным результатам эксплуатации, чем расчеты надежности без учета ООП.

Также из практических соображений следует рассматривать случаи, когда в группу ООП входят элементы с разными показателями надежности.

Если в группу ООП входят элементы с разными показателями надежности, то в качестве базового (расчетного) значения Q_{tot} принимается один из вариантов:

1. $Q_{tot} = \min\{Q_1, \dots, Q_n\}$, где $\min\{\dots\}$ – обозначение операции нахождения минимального значения переменных;
2. $Q_{tot} = \max\{Q_1, \dots, Q_n\}$, где $\max\{\dots\}$ – обозначение операции нахождения максимального значения переменных;
3. $Q_{tot} = \mathrm{E}\{Q_1, \dots, Q_n\}$, где $\mathrm{E}\{\dots\}$ – обозначение операции нахождения среднего значения переменных;
4. $Q_{tot} = \mathrm{G}\{Q_1, \dots, Q_n\}$, где $\mathrm{G}\{\dots\}$ – обозначение операции нахождения среднего геометрического значения переменных.

Рассмотрим пример резервированной системы, вероятности отказов элементов которой равны $Q_1 = 0.01$ и $Q_2 = 0.02$. В качестве модели ООП примем модель β-фактора, $\beta = 0.05$.

При условии, что статистика ООП входит в исходные данные о параметрах надежности элементов системы, рассмотрим варианты расчета параметров схемы.

1. $Q_{tot} = \min\{Q_1, Q_2\} = Q_1 = 0.01$.

В этом случае вероятность отказа по общей причине $Q_{CCF} = \beta Q_{tot} = 0.01 \cdot 0.05 = 0.005$ и вероятность независимого отказа относительно выбранного Q_{tot} равна $Q_{1i} = (1 - \beta) \cdot Q_{tot} = (1 - \beta) \cdot Q_1 = (1 - 0.05) \cdot 0.01 = 0.0095$.

Изменение вероятности отказа первого элемента Q_1, имеющего минимальное значение вероятности отказа, вследствие учета ООП можно записать в следующем виде

$$Q_{1i} = (1 - \beta)Q_1 = Q_1 - \beta Q_1 = Q_{CCF}. \quad (7)$$

Аналогично следует рассчитать вероятность независимого отказа второго элемента

$$Q_{2i} = Q_2 - Q_{CCF} = 0.02 - 0.0005 = 0.0195. \quad (8)$$

Расчет вероятности отказа системы по формуле (4) даст следующий результат

$$Q_S = Q_{1i}Q_{2i}(1 - Q_{CCF}) + Q_{CCF} = 0.0095 \cdot 0.0195 \cdot (1 - 0.0005) + 0.0005 = 0.000685. \quad (9)$$

Заметим, что без учета ООП вероятность отказа резервированной системы равна 0.0002.

[5] ГОСТ Р МЭК 61508-6-2013 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководства по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р 61508-3.

На рисунке 4 представлен фрагмент экранного интерфейса ПК АРБИТР, иллюстрирующий использование алгоритмов автоматического учета ООП. На вкладке «Группа 1 (ООП Бета модель)» показано, что в качестве Q_{tot} выбрано наименьшее значение вероятности отказа элементов в группе ООП. Флажок рядом с надписью «наименьшее» показывает, что исходные данные содержат статистику ООП. В нижней части вкладки в строке «Бета-фактор» отображается параметр $\beta = 0.05$.

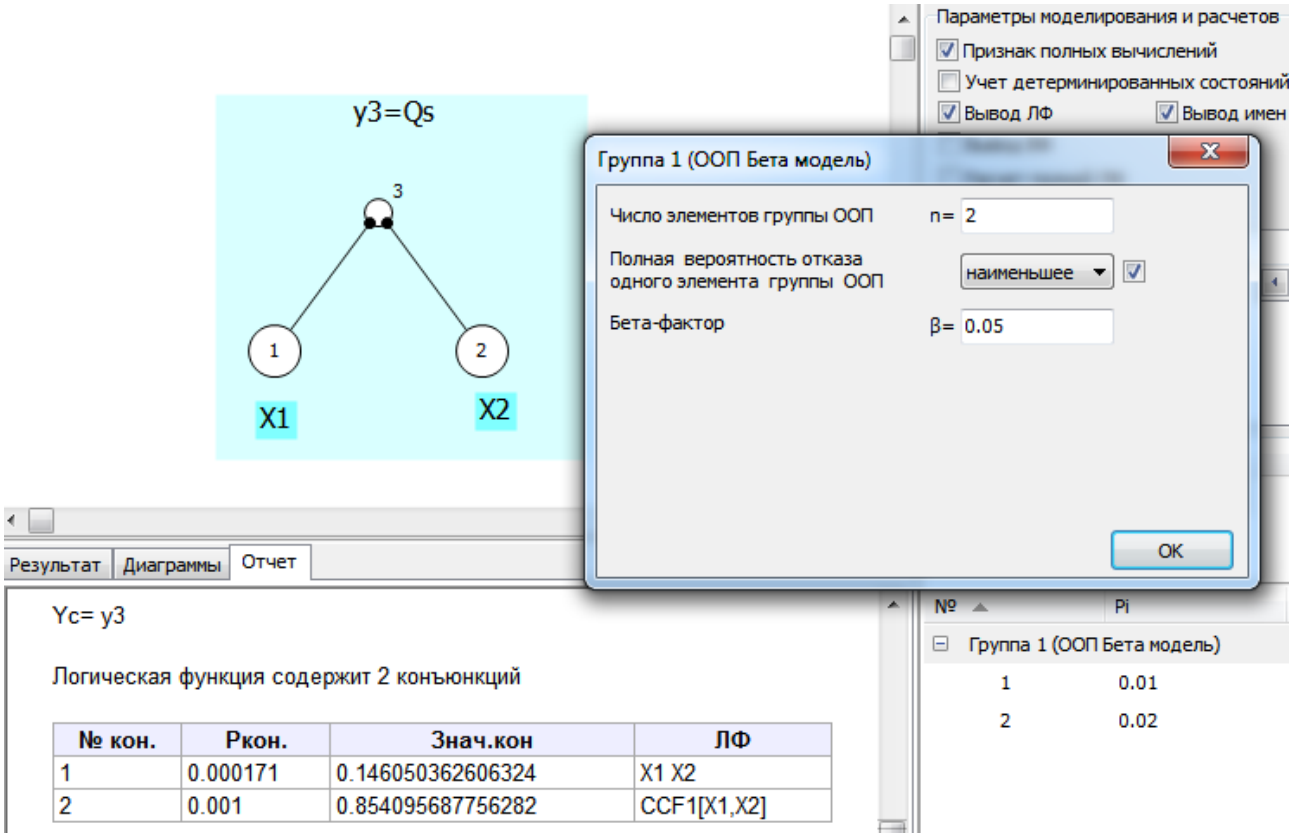

Рисунок 4. *Фрагмент экранного интерфейса ПК АРБИТР. Режим автоматического учета ООП (составлено авторами)*

На рисунке 4 в окне «Отчет» показана автоматически сформированная логическая функция (ЛФ), совпадающая с (1). Естественно, что и результат, полученный в ПК АРБИТР совпадает с аналитическим решением (9).

2. $Q_{tot} = \max\{Q_1, Q_2\} = Q_2 = 0.02.$

В этом варианте вероятность отказа по общей причине $Q_{CCF} = \beta \cdot Q_{tot} = 0.02 \cdot 0.05 = 0.001$ и вероятность независимого отказа относительно выбранного Q_{tot} равна $Q_{2i} = (1-\beta)Q_{tot} = (1-\beta)Q_2 = (1-0.05) \cdot 0.02 = 0.019.$

Вероятность независимого отказа первого элемента рассчитывается по аналогии с (8): $Q_{2i} = Q_1 - Q_{CCF} = 0.01 - 0.001 = 0.009.$

Расчет вероятности отказа системы по формуле (4) даст следующий результат

$$Q_s = Q_{1i}Q_{2i}(1-Q_{CCF}) + Q_{CCF} = 0.009 \cdot 0.019 \cdot (1-0.001) + 0.001 = 0.00117. \quad (10)$$

3. $Q_{tot} = \mathrm{E}\{Q_1, Q_2\} = 0.015.$

В этом варианте вероятность отказа по общей причине $Q_{CCF} = \beta \cdot Q_{tot} = 0.015 \cdot 0.05 = 0.00075.$

Вероятности независимых отказов первого и второго элементов рассчитываются по аналогии с (8): $Q_{1i} = Q_1 - Q_{CCF} = 0.01 - 0.00075 = 0.00925$, $Q_{2i} = Q_2 - Q_{CCF} = 0.02 - 0.00075 = 0.01925$.

Расчет вероятности отказа системы по формуле (4) даст следующий результат:

$$Q_s = Q_{1i}Q_{2i}(1 - Q_{CCF}) + Q_{CCF} = 0.00925 \cdot 0.01925 \cdot (1 - 0.00075) + 0.00075 = 0.0009279. \quad (11)$$

4. $Q_{tot} = \mathrm{G}\{Q_1, Q_2\} \cong 0.014142$.

В данном варианте вероятность отказа по общей причине $Q_{CCF} = \beta \cdot Q_{tot} = 0.014142 \cdot 0.05 \cong 0.0007071$.

Вероятности независимых отказов первого и второго элементов рассчитываются по аналогии с (8): $Q_{1i} = Q_1 - Q_{CCF} = 0.01 - 0.0007071 \cong 0.009293$, $Q_{2i} = Q_2 - Q_{CCF} = 0.02 - 0.0007071 \cong 0.019293$.

Расчет вероятности отказа системы по формуле (4) даст следующий результат

$$Q_s = Q_{1i}Q_{2i}(1 - Q_{CCF}) + Q_{CCF} \cong 0.0008863. \quad (12)$$

Сравнение результатов моделирования для 4-х вариантов задания базового (расчетного) значения Q_{tot} (формулы 9÷12) показывают их правильную физическую интерпретацию – чем выше значение базового (расчетного) значения Q_{tot}, тем выше вероятность отказа резервированной системы.

Заключение

В последнее время заметен рост внимания к проблемам анализа и оценки кибербезопасности не только информационных систем, но и такого широкого класса технических систем как АСУТП. И если до 2014 года обсуждение этих проблем не носило систематический характер, что во многом объясняется проведением подобных работ в рамках отдельных корпоративного заказов, то с момента опубликования требований к защите информации в АСУТП[6] появились работы, направленные не только на терминологические аспекты, но и на предложения по реализации тех или иных технических или организационных мер защиты информации. Возможно, что в ближайшее время будет устранен основной недостаток организации работ в этой сфере – отсутствие скоординированной активности в данной области [11].

Тем не менее, широкое обсуждение уязвимостей АСУТП на научно-практических конференциях, рекламные предложения разработчиков и производителей средств защиты информации не дают возможности заказчиками АСУТП оценить целесообразность и эффективность работ по обеспечению кибербезопасности, используя простой, но абсолютно понятный алгоритм – сравнение оценки затрат на кибербезопасность и оценки возможного ущерба от кибератак.

Рассматривая обеспечение кибербезопасности АСУТП как сложную мультидисциплинарную задачу, для автоматизированного моделирования и анализа риска необходимо применение программных средств, позволяющих реализовать методы количественной оценки риска аварий и анализа показателей функциональной безопасности.

[6] Приказ от 14.03.2014 № 31 Об утверждении требований 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).

ЛИТЕРАТУРА

1. Рябинин И.А. Надежность, живучесть, безопасность. Очерки разных лет // Изд-во Южно-российского государственного технического университета (Новочеркасского политехнического института), 2008. – 580 с.
2. Avizienis A., Laprie J.-C., Randell B. Fundamental Concepts of Dependability // Research Report No 1145, LAAS-CNRS, pp. 1-6.
3. Порецкий П.С. О способах решения логических равенств и об обратном способе математической логики // Собрание протоколов заседаний секции физико-математических наук общества естествоиспытателей при Казанском университете. Казань, 1884 / Т. 2. – XXIV. 170 С. (отдельный оттиск).
4. Можаев А.С. Аннотация программного средства «АРБИТР» (ПК АСМ СЗМА) // Вопросы атомной науки и техники. Серия «Физика ядерных реакторов». Раздел «Аннотации программных средств, аттестованных Ростехнадзором РФ»: науч.-техн. сб. – М.: РНЦ «Курчатовский институт», 2008. – Вып. 2/2008. – С. 105-116.
5. Можаева И.А., Нозик А.А., Струков А.В., Чечулин А.А. Современные тенденции структурно-логического анализа надежности и кибербезопасности АСУТП // Моделирование и анализ Безопасности и Риска в Сложных Системах: Труды Международной Научной Школы МА БР-2015. Санкт-Петербург, 17-19 ноября, 2015, ГОУ ВПО «СПбГУАП». СПб., 2015, С.140-145.
6. Ten C., Liu C., Govindarasu M. Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees // URL: https://pdfs.semanticscholar.org/c1f2/62911e2d3a4263324da70e6476b886c5b3e0.pdf (Дата обращения 22.05.2017).
7. Можаева И.А., Нозик А.А., Струков А.В. Особенности программной реализация методов количественного анализа риска аварий опасных производственных объектов на основе логико-вероятностного моделирования // Промышленность и безопасность. 2016. №8 (100). С. 34-37.
8. Швыряев Ю.В. и др. Вероятностный анализ безопасности атомных станций. Методика выполнения. М.: ИАЭ им. И.В. Курчатова, 1992. – 266 с.
9. Порецкий П.С. Решение общей задачи теории вероятностей при помощи математической логики // Собрание протоколов заседаний секции физико-математических наук общества естествоиспытателей при Казанском университете, Казань, 1887, Т.5, – С. 83-116. Переиздано: Труды СПИИРАН. 2015. Вып. 6 (43). С. 27-49.
10. Рябинин И.А. Струков А.В. Предисловие и вступительная статья к переизданию работы П.С. Порецкого «Решение общей задачи теории вероятностей при помощи математической логики» // Труды СПИ-ИРАН. 2015. Вып. 6 (43). С. 5-26.
11. Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУТП // Вопросы кибербезопасности. 2015. №2 (10). С. 56-59.

Strukov Aleksandr Vladimirovich
JSC «Specialized engineering company SEVZAPMONTAGEAUTOMATICA», Russian, Saint Petersburg
E-mail: alexander_strukov@szma.com

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

About methods for the quantitative analysis of cyber safety of technical systems bazed on the logical-probability approach

Abstract. The authors of this article reviewed the contents of the logical-probabilistic approach to the analysis of cyber security of automated control systems of technological processes. The essence of this approach is that the system as a certain structure describing as a topology of interconnected elements. The interrelation of the investigated elements describing by functions of the algebra of logic forming the system of Boolean equations. Authors justifies using of methodology of reliability assessment and risk analysis of technical systems cybersecurity, they also give recommendations on the choice of methods of analysis of the technical risks. Risk analysis of modern technical systems is a complex problem of system analysis, which involves the use of appropriate software tools. Examples of methods for quantitative risk analysis in the ARBITR software environment are introduced in this article. It means that a software implementation of the technologies of the attack trees to describe the potential threats and attack methods that implement these threats, is possible by reducing the functional capabilities of software intended for reliability analysis of complex systems. There is example of recording of common cause failure in the reliability analysis of redundant systems in the analysis of functional safety. The authors provides an example software implementation of attack trees for web-accessible automated control system of technological process.

Keywords: reliability analysis; risk assessment; cyber safety; fault tree; attack tree; event tree; scheme of functional integrity; common cause failures; functional safety