DOI: 10.25728/mlsd.2022.0912

УЧЕТ ВОЗМОЖНЫХ ОШИБОЧНЫХ ДЕЙСТВИЙ ОПЕРАТОРА ПРИ ПРОВЕДЕНИИ АНАЛИЗА БЕЗОПАСНОСТИ СЛОЖНЫХ ТРАНСПОРТНЫХ СИСТЕМ

Резчиков А.Ф., Цвиркун А.Д., Дранко О.И., Степановская И.А.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная, д.65
rw4cy@mail.ru
Цесарский Л.Г.
Филиал ПАО "Корпорация "Иркут" "Центр комплексирования",
Россия, г. Москва, ул. Смольная, д. 24Д
lev.tsesarskiy@ic.irkut.com
Кушников В.А.
ФГБУН ФИЦ «Саратовский научный центр Российской Академии Наук»,
Россия, г. Саратов, ул. Рабочая, д.24
kushnikoff@iptmuran.ru
Богомолов А.С.
ФГБУН ФИЦ «Саратовский научный центр Российской Академии Наук»,
Россия, г. Саратов, ул. Рабочая, д.24
bogomolov@iptmuran.ru

Аннотация. В работе предложен порядок учета «человеческого фактора» при проведении анализа безопасности сложной транспортной системы. Для этого предлагается рассматривать оператора в качестве элемента компонентов СТС и разработать модель нарушенного функционирования оператора, как часть модели нарушенного функционирования компонентов СТС и, следовательно, модели СТС в целом.

Ключевые слова: анализ, безопасность, модель, система, оператор, отказ, ошибка.

Введение

Необходимость осуществления постоянного контроля текущего уровня риска при функционировании СТС с использованием проактивного и упреждающего моделирования вызывает потребность моделирования возникновения рисков в СТС [1]. Модель возникновения рисов в СТС, используя модельноориентированный подход, должна строиться на основании моделей безопасности компонентов СТС, а те в свою очередь на основании моделей безопасности свих составных элементов [2]. Каждый компонент СТС имеет в своем составе операторов.

Как сказано в [1], «В авиации будут иметь место отказы и эксплуатационные ошибки, несмотря на самые эффективные и тщательно разработанные меры, применяемые для их предотвращения. Никакая деятельность человека или созданная им система не гарантирована от полного отсутствия факторов опасности и эксплуатационных ошибок». Можно сказать, что это относится не только к авиации. Из этого следует, что оценка безопасности полета без учета правильности действий экипажа является неполной. Дело даже не в том, что по данным различных источников из-за "ошибочных действий» операторов происходит более 70 процентов нарушений функционирования сложных систем [3]. Основой модели безопасности СТС является полный перечень возможных видов нарушения функционирования. Если этот перечень не учитывает такое важнейшее звено в контуре управления системой, как оператор, то его нельзя считать полным, и, следовательно, неполной является модель безопасности системы. Таким образом, модели безопасности компонентов СТС и СТС в целом должны учитывать оператора, или, по общепринятому выражению, учитывать «человеческий фактор» (ЧФ).

1 Оператор в сложной транспортной системе

В качестве примера СТС рассмотрим авиационную транспортную систему (АТС). В состав АТС традиционно включают воздушное судно, систему технического обслуживания и ремонта, систему управления воздушным движением (УВД), аэродромные службы обеспечения полетов, в том числе оборудование, материалы, персонал, технические средства, программное обеспечение, нормативная и эксплуатационная документация. Все эти составные части включают операторов. В рамках данной работы в качестве операторов системы (компонента СТС) будем рассматривать штатных специалистов, обеспечивающих функционирование системы (компонента СТС) в соответствии с технической документацией. Предложения по проведению анализа безопасности АТС представлены,

например, в [2]. Для обеспечения полноты и объективности оценки безопасности целесообразно использовать модельноориентированный подход [2].

2 Модель нарушенного функционирования оператора СТС

В настоящее время существуют различные модели, описывающие ошибочные действия оператора, основанных на экспериментальном материале и опыте эксплуатации. Некоторые модели основаны на встраивании оператора в среду управления [3]. Другие используют планомерный анализ фактов, их классификацию и ранжирование с формированием базы данных ошибок оператора. Характерным примером такого подхода является изложенный в [4], иллюстрация которого представлена на рис.1.

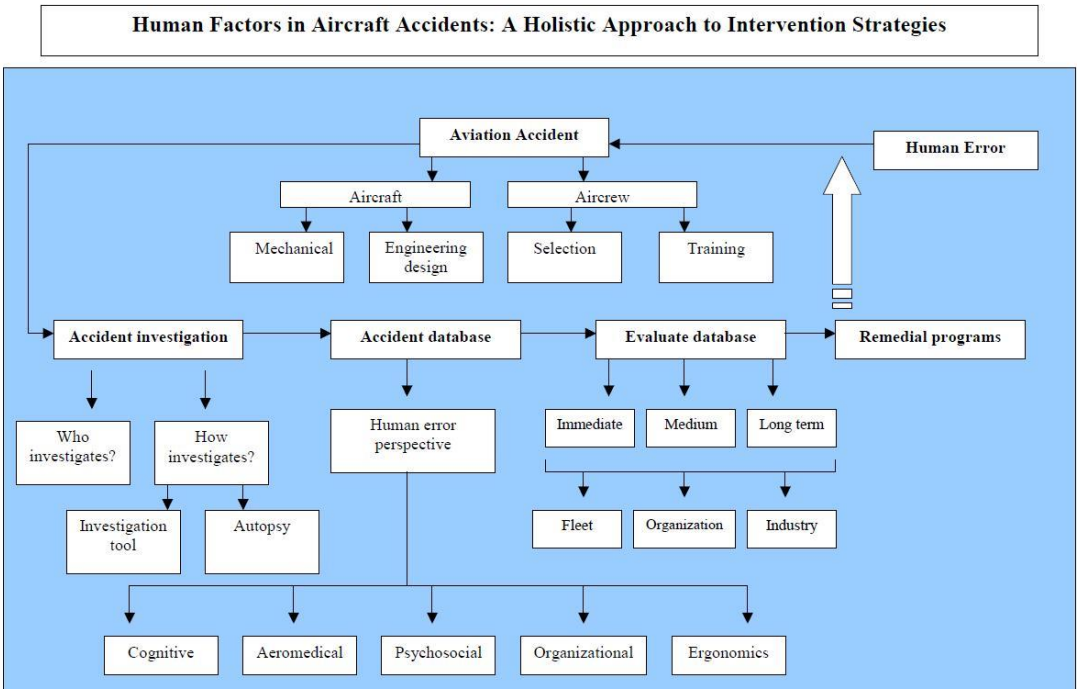

Рис.1. Схема анализа факторов, влияющих на авиационный инцидент

В рамках данного подхода проводится целостный анализ факторов, влияющих на риск возникновения авиационного инцидента в целом, и по причине человеческого фактора в частности. В процессе анализа эксплуатационных данных формируется база данных инцидентов, определяется вклад в инцидент ошибок человека, осуществляется классификация ошибочных действий по различным факторам: когнитивным, медицинским, психологическим, организационным, эргономическим. Систематическое выполнение изложенного процесса позволяет постепенно находить различного рода решения, снижающие риски происшествий по причине ЧФ. Однако, подобный подход не позволяет осуществлять управление безопасностью АТС на всем жизненном цикле, т.к. процесс не встроен в модель безопасности АТС, как интегрированной совокупности компонентов [2].

В [1] прямо отмечено, что при построении системы управления безопасностью полета необходимо исходить из понимания того, что отказов элементов АТС и ошибки операторов являются неотъемлемой частью процесса функционирования АТС. Из этого можно сделать вывод, что целесообразно включить в модель надежности и безопасности АТС модель нарушенного функционирования оператора, которую можно было бы интегрировать с моделями нарушенного функционирования элементов систем АТС.

Модель нарушенного функционирования элемента системы описана в [2], ее структура показана на рис.2, ниже дано ее формальное описание.

Рис.2. Модель нарушенного функционирования элемента системы

Пусть $Э_1, \ldots, Э_n$ – элементы системы. Каждый элемент системы рассматривается как преобразователь входных сигналов в выходные, взаимосвязи между элементами в процессе функционирования системы таковы, что на входы каждого элемента $Э_i$ попадают выходы соединенных с ним элементов системы. Структура модели элемента $Э_i$ представлена на рис. 3.

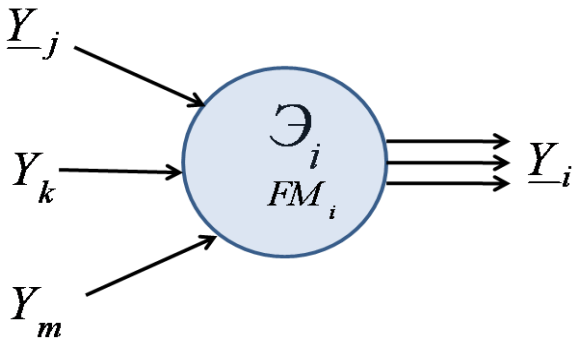

Рис.3. Структура модели нарушенного функционирования элемента системы

Конкретизируем теперь обозначения для различных видов сигналов элементов, обозначая через $\overline{X}_i, \overline{Y}_i$ соответственно множества входных и выходных сигналов элемента, не являющихся нарушенными, через $\underline{X}_i, \underline{Y}_i$ – соответственно множества нарушений входных и выходных сигналов элемента, FM_i– множество видов отказов элемента, NM_i – множество видов ненарушенного функционирования элемента $Э_i, i = \overline{1,n}$.

Примем гипотезу, что причиной нарушения функционирования элемента $Э_i$ являются отказы FM_i самого этого элемента и нарушения выходных сигналов элементов, связанных с $Э_i$. В ситуации на рис. 3 входные сигналы, полученные элементом $Э_i$ от элементов $Э_k$ и $Э_m$ не являются нарушенными, причиной нарушенного выходного сигнала элемента $Э_i$ может быть отказ самого элемента $Э_i$, нарушенный входной сигнал элемента $Э_j$ или эти две причины в комплексе.

Таким образом может быть установлено соответствие каждого нарушенного выходного сигнала из множества $\underline{Y}_j$ по крайней мере одному элементу множеств

$$FM_i \times \underset{j \in O(Э_i)}{\times} \overline{Y}_j,$$
$$NM_i \times \underset{j \in O(Э_i)}{\times} \underline{Y}_j,$$
$$FM_i \times \underset{j \in O(Э_i)}{\times} \underline{Y}_j,$$

где $O(Э_i) \subseteq \{0, \ldots, n\}$ – множество индексов элементов, связанных с $Э_i$ таким образом, что их выходы попадают на вход $Э_i$ и через $Э_0$ обозначена окружающая среда системы; элементы, не связанные с другими элементами из множества $\{Э_1, \ldots, Э_n\}$, считаются связанным с $Э_0$.

Таким образом, модель нормального функционирования элемента $Э_j$ может быть задана отображением вида

$$F_i^0 : NM_i \times_{j \in O(Э_i)} \overline{Y_j} \to \overline{Y_i}, \quad (1)$$

а модель нарушенного функционирования элемента $Э_i$ может быть задана отображениями вида

$$F_i^1 : FM_i \times_{j \in O(Э_i)} \overline{Y_j} \to \underline{Y_i}, \quad (2)$$

$$F_i^2 : NM_i \times_{j \in O(Э_i)} \underline{Y_j} \to \underline{Y_i}, \quad (3)$$

$$F_i^3 : FM_i \times_{j \in O(Э_i)} \underline{Y_j} \to \underline{Y_i}. \quad (4)$$

Распространим описанную модель нарушенного функционирования на действия оператора системы. Соответствующая модель представлена на рис.4. Под механическими сигналами понимается воздействие на органы управления, логические – принятие решение и т.п. Такой подход позволяет использовать для параметрического описания модели нарушенного функционирования оператора метод приведения [2]. В этом случае возможные ошибочные действия экипажа являются, наряду с нарушениями функционирования элементов систем, причинами функциональных отказов систем, а оператора можно рассматривать в качестве элемента системы. Отметим, изложенный подход не отвергает анализ ошибок оператора с позиции медицинских, психологических и других факторов. Эти модель сохраняют свою значимость при анализе причин ошибок оператора.

Вероятность ошибочных действий оператора в рамках изложенной модели определяется, как и для элементов системы, нарушениями внутренних состояний (FM_i) и нарушениями входных сигналов ($\underline{Y_i}$). Вероятности событий $\underline{Y_i}$ определяются в рамках анализ безопасности смежных с оператором систем (система экранной индикации, пульты, информационные панели, системы звуковой и речевой информации).

Рис.4. Модель нарушенного функционирования оператора системы

Для определения вероятностей событий FM_i можно использовать анализ результатов эксплуатации, летных и стендовых испытаний, математическое моделирование, материалы различных справочников. При этом важно не рассматривать числовое значение как самоцель и помнить, что для нашей задачи вполне устраивает точность в пределах одного, а часто и двух порядков. Кроме того, анализ имеющихся материалов [5] позволяет сделать вывод, подтверждаемый опытом эксплуатации, что значения вероятностей различного рода ошибок оператора в зависимости от условий лежат в диапазоне 10^{-5} - 10^{-2}. Для хорошо обученных операторов диапазон можно уменьшить до 10^{-5} - 10^{-3}. Этих данных достаточно, чтобы с помощью предлагаемого подхода достичь целей проведения анализа безопасности АТС. Ниже приведен пример, иллюстрирующий изложенный подход.

3 Пример учета возможных ошибочных действий оператора при проведении анализа безопасности системы

Рассмотрим пример оценки безопасности системы с учетом действий оператора на основании изложенной выше модели. На рис. 5 представлена рассматриваемая схема человеко-машинной системы.

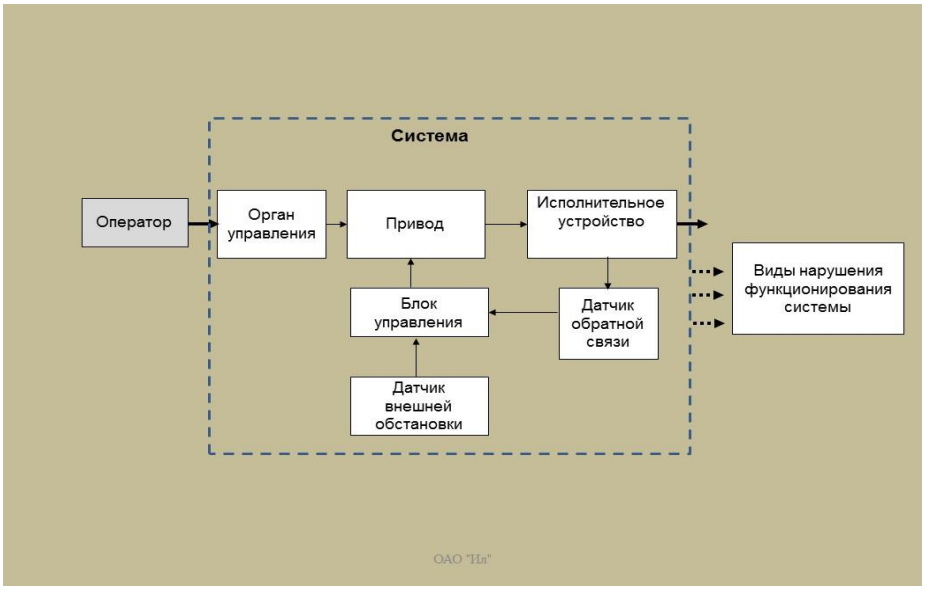

Рис.5. Пример схемы человеко-машинной системы

Система работает следующим образом. На орган управления (ОУ) поступает управляющая команда оператора. Орган управления транслирует команду на привод, а тот передает управляющий сигнал на исполнительное устройство (ИУ). Блок управления (БУ) корректирует управляющий сигнал привода на основании данных датчика внешней обстановки (ДВО) и датчика обратной связи (ДОС).

Результаты анализа безопасности системы без учета оператора, выполненного, как описано в [2], представлены в таблице 1. Результаты анализа представляют собой полный перечень возможных видов нарушения функционирования или функциональных отказов (ФО) системы, причины в форме логического уравнения с видами отказов элементов системы (в таблице 1 для краткости только перечислены сами элементы), вероятность ФО и оценка критичности ФО с позиции влияния на безопасность системы в целом. Вероятность рассчитывается на основании логических уравнений и данным по интенсивности соответствующих видов отказов элементов. В графе Причины ФО для разных ФО для разных ФО могут быть указаны одинаковые элементы, при этом имеются в виду разные виды отказов этих элементов. В качестве оценки критичности использована шкала критичности из [6] со следующими обозначениями. УУП –усложнение условий полета (незначительные последствия), СС – сложная ситуация (заметные последствия).

Таблица 1 Результаты анализа безопасности системы

№	Вид нарушения функционирования системы (ФО)	Причины ФО (виды отказов каких элементов)	Вероятность, 1/час	Степень опасности ФО (критичность)
1	Невозможность срабатывания ИУ	ОУ, Привод, ИУ	$5*10^{-5}$	УУП
2	Срабатывание ИУ в произвольный момент времени	ОУ, Привод, ИУ	$5*10^{-6}$	УУП
3	Переход ИУ в крайнее положение	ОУ, Привод, ИУ, ДОС	10^{-6}	СС
4	Работа ИУ с недопустимой погрешностью относительно управляющего сигнала	ОУ, Привод, ИУ, БУ, ДВО, ДОС	10^{-5}	УУП
5	Автоколебания ИУ	ОУ, Привод, ИУ, БУ, ДВО, ДОС	10^{-6}	СС
6	Работа ИУ без коррекции по внешней обстановке	БУ, ДВО	$2*10^{-6}$	СС

Добавим в анализ безопасности системы учет ошибок оператора. Параметры модели оператора, в соответствии с рис.4 и [2], приведены в таблице 2.

Таблица 2 Модель нарушения функционирования оператора

№	Вид нарушения функционирования оператора	Вид нарушения функционирования системы (ФО))	Оценка вероятность ошибки оператора, 1/час	Критичность ошибки оператора
1	Невыдача управляющей команды на ОУ	Невозможность срабатывания ИУ	10^{-5} - 10^{-3}	Незначительная
2	Выдача управляющей команды на ОУ не вовремя	Срабатывание ИУ в произвольный момент времени	10^{-5} - 10^{-3}	Незначительная
3	Выдача постоянной команды на ОУ	Переход ИУ в крайнее положение	10^{-5} - 10^{-3}	Заметная

Сравнение таблиц 1 и 2 показывает, ошибки оператора в качестве причин необходимо включить в логические уравнения ФО №1,2,3. Из них ФО №3 имеет заметную критичность (СС). Для этого ФО целесообразно предусмотреть схемную защиту от ошибки, например ограничение времени непрерывной выдачи управляющего сигнала.

Заключение

В работе изложен подход и соответствующий метод учета ошибочных действий оператора при выполнении анализа безопасности и оценки риска при функционировании АТС на основе модели безопасности. В качестве модели ошибочных действий оператора предложена модель нарушенного функционирования (МНФ), аналогичная по структуре МНФ элемента системы []. Приведен пример интеграции МНФ оператора в МНФ системы. Данный подход может быть реализован при анализе безопасности и оценке риска в сложных транспортных системах и других многокомпонентных и разнородных систем. При этом принципы формирования МНФ оператора на различных уровнях иерархии систем сохраняют свою применимость. Используя модель МНФ оператора можно повысить объективность и эффективность корректирующих мероприятий, как показано в [7].

Авторы выражают глубокую признательность выдающемуся авиаконструктору и ученому, Генеральному конструктору самолетов «Ил», академику РАН Генриху Васильевичу Новожилову за фундаментальный вклад в теорию и практику обеспечения безопасности полета самолетов в авиационной транспортной системе.

Литература

1. ICAO Doc9859 An/474 Руководство по управлению безопасностью полетов (РУБП).
2. *Новожилов Г.В., Неймарк М.С., Цесарский Л.Г.* Безопасность полета самолета: Концепция и технология. – М.: Изд-во МАИ, 2007. – 194с.
3. *Nancy G. Leveson, John P. Thomas*. STPA HANDBOOK, March 2018. Massachusetts Institute of Technology. Электронное издание. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
4. *Narinder Taneja*. Human factors in aircraft accidents: a holistic approach to intervention strategies, University of Illinois, Aviation Human Factors Division Savoy, Illinois To appear in the Proceedings of the 46th Annual Meeting of the Human Factors and Ergonomics Society. Santa Monica, Human Factors and Ergonomics Society, 2002.
5. Справочник по надежности под ред. Б.Е. Бердичевского, в 3-х т., т.3, – М.: Изд-во Мир, 1970. – 376с.
6. Авиационные правила. Часть 25. Нормы летной годности самолетов транспортной категории. Межгосударственный авиационный комитет. 1994.
7. *Новожилов Г.В., Резчиков А.Ф., Кушников В.А., Неймарк М.С., Иващенко В.А., Цесарский Л.Г., Богомолов А.С., Филимонюк Л.Ю.* Решение проблемы коррекции ошибок персонала авиационных транспортных систем // Общероссийский научно-технический журнал "Полет", 2017. №2. – С. 3-8.