УДК 629.735

DOI: 10.26467/2079-0619-2020-23-4-84-95

ОЦЕНКА РИСКОВ ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ БОРТОВЫХ СИСТЕМ ВОЗДУШНОГО СУДНА

Х.Э. ФУРАР¹, Б.Д. ОГУНВОУЛ², В.Д. БУДАЕВ³, Ф. ЛАШИ¹

¹Университет Хаджи Лахдар, г. Батна, Алжирская Народная Демократическая Республика

²Национальное агентство космических исследований и разработок, г. Абуджа, Нигерия

³Департамент технического обслуживания ПАО «Аэрофлот», г. Москва, Россия

Рассмотрена методика оценки риска бортовой информационной системы воздушного судна (ВС), позволяющая обеспечивать надёжность и безопасность такой комплексной системы в эксплуатации. Эта методика призвана применять объединённые математические инструменты для оценки рисков, которым подвергаются комплексные изделия авиационной техники (АТ). Существующие методики оценки рисков недостаточно гибки для решения комплексной задачи обеспечения всесторонней безопасности бортовой информационной системы (БИС) воздушных судов из-за сложности в унификации критериев оценки степени опасности по всем концепциям безопасности, т.е. сейчас не учитываются тяжесть рисков, механизм развития одного нежелательного события (события риска) в более сложные формы в процессе технической эксплуатации изделия АТ. Однако предложенная в статье методика призвана стать катализатором формирования новых критериев единой базы оценки безопасности такой технической сложной (комплексной) системы, как БИС, так как содержит в себе трёхкомпонентные параметры риска, т.е. риск по угрозам от актов незаконного вмешательства (АНВ), уязвимости (функциональные опасности, способствующие АНВ и их развития в системе) и ущербу (совокупность критериев, оценивающих последствия АНВ). В результате эти критерии и параметры трёхкомпонентной безопасности позволят находить новый подход в определении комплексного риска, которому подвергаются важные системы ВС, такие, как бортовые информационные системы ВС. В статье предлагается методика определения риска, учитывающая трёхкомпонентную концепцию. Совместно эти компоненты позволяют оценивать степень опасности технических систем с учётом их совершенства. Приведённые авторами сведения в данной работе являются научной гипотезой и призваны обратить внимание научного сообщества на проблему отсутствия методик оценки многокомпонентных рисков в такой системе, как БИС. В статье приведены базовые критерии оценки комплексного трёхкомпонентного риска, которые недостаточны для полноценного формирования новых критериев оценки безопасности комплексной системы/изделия АТ и требуется уточнение их параметров. Таким образом, настоящая работа не позволяет в полной мере решить комплексную задачу обеспечения всесторонней безопасности БИС ВС, а лишь предлагает методику унификации трёх компонентов безопасности для определения комплексного риска.

Ключевые слова: риск, безопасность, бортовая информационная система, процесс технической эксплуатации.

ВВЕДЕНИЕ

Параллельно с развитием и совершенствованием авиационных систем и автоматизацией бортовых комплексов и оборудования развиваются возможности появления неблагоприятных факторов в виде внешнего вмешательства в эксплуатационный процесс, а также человеческого фактора, проявляющегося из-за сложности взаимодействия человека с современными комплексами типа блоков информационной системы воздушного судна (БИС) [1, 2, 3]. Риски, которым подвергаются блоки информационной системы ВС, одной из важнейших бортовых систем, необходимо рассматривать с трёх позиций обеспечения безопасности, а именно обеспечение безопасности полетов, авиационной безопасности и информационной безопасности, что в свою очередь вызывает осложнение и дополнение к критериям для оценки безопасности такой системы. Вероятность совершения актов незаконного вмешательства актуальна не только в отношении ВС, но и в отношении объектов обслуживания пассажиров и грузов, т.е. объектов транспортной инфраструктуры. По оценке официального представителя правительства США во время испытаний, проведённых 19 сентября 2016 года на Boeing 757,

команда IT-специалистов национальной безопасности США во главе с Робертом Хикки смогла «захватить» пассажирский самолет в аэропорту Атлантик-Сити в Нью-Джерси, взломав системы лайнера [4]. Во время этого испытания управление самолетом, находящимся на ВПП, захватил кибершпион. Специалисту удалось полностью взять под свой контроль управление бортовой системой самолета.

МЕТОДИКА ОЦЕНКИ РИСКА БОРТОВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВС

В связи с растущей угрозой, связанной с информационной безопасностью, и развитием технологий, применяемых с целью совершения актов незаконного преступного вмешательства в сфере информационных технологий [5, 6], возрастает также необходимость в нахождении новых решений для снижения уровня опасности таких АНВ для ликвидации последствий и ущерба для бортовых информационных систем ВС [3, 7, 8, 9]. Эта проблема является актуальной и сложной, так как содержит в себе три подкатегории:

- 1) авиационная безопасность;
- 2) безопасность полетов;
- 3) информационная безопасность.

С точки зрения комбинации информационной и авиационной безопасности эта проблема носит экспоненциальный характер, выраженный вероятностью совершения акта незаконного вмешательства с последствиями, сравнимыми с терактом [10, 11, 12].

Экспоненциальный характер развития сочетания этих двух концепций продиктован возрастанием величины (тяжести) одной концепции при скорости роста пропорционально значению тяжести второй концепции и наоборот.

Рис. 1. Эксплуатационный риск технической системы
Fig. 1. Technical system operation risk

С точки зрения безопасности полетов, эта проблема носит модельный характер, выраженный вероятностью возникновения нежелательных особых ситуаций, способных повысить уровень риска при оценке возможности обеспечения благоприятного завершения полета.

Следовательно, можно объединить показатели оценки первой и третьей концепций безопасности, т.к. они обладают общим базовым свойством, которое выражается вероятностью совершения нежелательных событий в важных системах ВС. В случае первой концепции приобретенный риск при обеспечении безопасности полета ВС в эксплуатации можно описать по рис. 1, поясняющему характер развития этого риска.

Эта зависимость характерна тем, что при эксплуатации исправного ВС его производительность снижается, при том, что он годен для выполнения полета. Риск в данном случае оценивается по формуле (1):

$$R_{iБП} = y_i * \lambda_t (1 - P_x(t)), \quad (1)$$

где y – функция, описывающая летную годность (ЛГ);

λ – интенсивность отказов изделия ВС за период t ;

$P_x(t)$ – вероятность безопасного выполнения задачи.

Точки соприкосновения двух кривых показывают время (наработка), до которого $P_x(t)$ будет обеспечивать приемлемый уровень риска изделия АТ в эксплуатации с учетом мер по противодействию угрозам с применением контрольного механизма процесса поддержания летной годности (ППЛГ) в эксплуатации. Рисунок показывает, как определяется уровень приемлемого риска изделия АТ в зависимости от качества/обеспеченности мероприятиями ППЛГ и технического состояния [8].

В первой зоне приемлемый уровень риска обеспечивается мероприятиями по ППЛГ и контролю технического состояния. Во второй зоне приемлемый уровень риска не обеспечивается мероприятиями ППЛГ в полной мере, т.к. эффект от восстановительного процесса сопровождается небольшими коррективными изменениями из-за старения изделия АТ. N – предел периода, при котором риск приемлем и $P_x(t)$ оптимальна. L – интервал приемлемого риска, $R_{опт}$ – оптимальный риск.

Под степенью функциональной опасности изделия АТ следует понимать коэффициент, относящийся к уровню ресурсного цикла изделия определенного возраста x . Это понятие относится к уравнению функции опасности, которое определяет вероятность того, что изделие будет работоспособно до определенного момента времени, основываясь на его выживаемости до более раннего времени t . Другими словами, это вероятность того, что, если восстанавливаемое изделие доживет до некоторого момента времени в эксплуатации, то оно также доживет и до следующего при условии постоянного поддержания уровня надежности процессом технического обслуживания и ремонта (ТОиР). Упрощенный вид уравнения можно представить следующим образом:

$$h(t) = \frac{f(x)}{\bar{\mu}(x)}, \quad \text{для всех } x < u_x, \quad (2)$$

где $f(x)$ – функция плотности распределения вероятности того, что значение (отказ или повреждение) выпадет в заданной выборке или интервале. Например, в определенный эксплуатационный цикл (времени), а $\bar{\mu}(x)$ – это функция выживаемости или вероятность того, что изделие продолжит функционировать после определенного времени t .

То есть, если случайная величина X представляет собой жизненный цикл или ресурс изделия в целом или отдельного агрегата изделия, то данная функция определяет вероятность мгновенного отказа в момент времени x . Учитывая непрерывную случайную величину X с функцией распределения F и функцией плотности распределения f , ее функция степени опасности определяется по формуле (2).

Эта функция связана со случайной величиной $X_x = [X - x | X > x]$ и известна как остаточный срок эксплуатации в момент времени x .

Функция выживания X_x :

$$\bar{\mu}(t) = P[X - x > t | X > x] = \frac{\bar{\mu}(x+t)}{\bar{\mu}(x)}, \quad \text{для всех } x \geq 0, \quad (3)$$

следовательно,

$$h(t) = \lim_{\Delta \rightarrow 0^+} A = \pi r^2 \frac{1}{\Delta} \frac{\bar{\mu}(x+\Delta) - \bar{\mu}(x)}{\bar{\mu}(x)} = \lim_{\Delta \rightarrow 0^+} \frac{1}{\Delta} P[X_x \leq \Delta], \quad \text{для всех } x \geq 0.$$

Из этого равенства очевидно, что эта функция является интенсивностью отказа блока/узла рассматриваемого изделия. Свойство увеличивающейся (уменьшающейся) функции степени опасности называется растущей интенсивностью отказа (РИО) (снижающей

интенсивностью отказа (СИО)), и это хорошо известное и широко изученное свойство [13]. Аналогично, случайная величина X является РИО (СИО) тогда и только тогда, когда (3) уменьшается (возрастает) в x при всех $t \geq 0$. Множество случайных величин, обладающих данным свойством, понимается и классифицируется как характеристики стареющего изделия в теории надежности. В частности, данная теорема получена Барлоу и Прошаном [13, 14].

Существует еще одна функция, которая тесно связана с функцией степени опасности: функция среднего остаточного ресурса. Учитывая случайную величину X с конечным средним значением, ее средняя функция остаточного ресурса определяется как:

$$m(x) = E[X_x], \quad \text{для всех } x < u_x. \quad (4)$$

Функция среднего остаточного ресурса измеряет дополнительный ожидаемый срок службы изделия или отдельного элемента изделия, функционирующего до момента времени x . Функция среднего остаточного ресурса также имеет обоснование в теории риска. При организации ТОиР и заключении договоров поставки запчастей и услуг с фиксированным удержанием x , с целью ограничения/контроля убытков по приближению стареющего изделия к нижней доверительной границе остаточного ресурса (т.е. до перехода в предельное состояние) можно применить уравнение (4) $m(x)$ для измерения ожидаемых затрат для страховой компании.

Из (2) и (3) следует, что

$$m(x) = \frac{\int_x^{+\infty} \bar{\mu}(x) dx}{\bar{\mu}(x)}, \quad \text{для всех } x < u_x. \quad (5)$$

Следовательно, для определения риска, обусловленного эксплуатацией стареющего изделия АТ с учетом вероятности безопасного завершения полета и возможной неоперативной затратой, подставляем (5) в (1) и получаем:

$$R_{\text{БП}} = \frac{\int_x^{+\infty} \bar{\mu}(x) dx}{\bar{\mu}(x)} * \lambda_t (1 - P_x(t)), \quad \text{для всех } x < u_x. \quad (6)$$

Так как существующие методики оценки риска во многом игнорируют составляющие вероятности нежелательного вмешательства в процесс технической эксплуатации бортовой информационной системы ВС [15, 16, 17], акцент необходимо делать на поиск фундаментального решения трехкомпонентной безопасности, что и превращает методику оценки риска в комплексную задачу [18, 19, 20, 21].

Стоит отметить, что при формировании критериев конструктивных важных элементов изделия для оценки рисков при обеспечении безопасности полетов [18, 19, 20, 21] необходимо провести структуризацию по степени опасности выполняемых отдельными элементами системы функций. Одной из методик решения этой задачи может послужить метод анализа видов и последствий отказов (FMEA) в сочетании с методом анализа безопасности системы (SSA).

Стратегическая роль бортовой информационной системы ВС в обеспечении БП очевидна, однако она является одной из самых уязвимых с точки зрения вероятности совершения акта незаконного вмешательства. Система входит в перечень важных систем безопасности в документах ARP4754A, ARP4761, RTCA, DO-178C/DO-178B и DO-254 [22, 23].

Для оценки риска R по совокупности авиационной и информационной безопасности этой системы предлагается уравнение (7):

$$R = P_{\text{уг}} * P_{\text{уя}} * P_{\text{уш}}, \quad (7)$$

где $P_{уг}$ – уровень угрозы АНВ с учетом уровня технического эксплуатационного совершенства изделия АТ;

$P_{уя}$ – степень уязвимости изделия АТ для АНВ;

$P_{уш}$ – степень ущерба вероятной угрозы.

$P_{уш}$ – это соотношение эффективной функциональной производительности изделия после наступления нежелательного события (f_0^e) к эффективной функциональной производительности изделия до наступления нежелательного события (f_t^e):

$$P_{уш} = \frac{\lim_{f_0 \rightarrow 0^-} f_0^e}{\lim_{t \rightarrow \infty} f_t^e},$$

f_0^e вычисляется в области функции, где невозможно осуществлять заданную функцию с учетом восстановительных аварийных мероприятий, а f_t^e вычисляется в точке экстремума функции относительно исследуемого периода времени.

Уровень угрозы вычисляется по степени уязвимости u_z , исходя из критичности и вероятности реализации угрозы через уязвимость. Уровень угрозы показывает, насколько критично воздействие той или иной угрозы на функции изделия бортовой информационной системы с учетом вероятности реализации такой угрозы:

$$u_z = \frac{k_r}{100} * \frac{P_v}{100}, \quad (8)$$

где k_r – критичность реализации угрозы, задается качественно, т.е. в баллах экспертами;

P_v – вероятность возникновения угрозы через эту уязвимость. Значение уровня угрозы по уязвимости колеблется от 0 до 1.

Под уровнем угрозы по i -й уязвимости понимается величина, характеризующая тяжести последствий той или иной угрозы для показателя эффективной производительности рассматриваемой системы/изделия, т.е. насколько конкретная угроза по степени уязвимости повлияет на систему/изделие. Вероятность возникновения угрозы зависит от реализуемости, степени уязвимости рассматриваемой системы, от наличия бэкдоров (backdoors) в алгоритмах, криптосистемах шифрования и прочих [14, 17].

Связь уровня угрозы АНВ с учетом уровня технического эксплуатационного совершенства изделия АТ со степенью ущерба вероятной угрозы $P_{уг} = P_{уш} \cdot u_z$ вычисляется через степень уязвимости u_z .

В случаях возникновения нескольких угроз одновременно, суммарный уровень угрозы для всех уязвимостей ϕ_h :

$$\phi_h = 1 - \sum_{i=1}^n (1 - \beta_i), \quad (9)$$

где β – уровень угрозы по уязвимости для случаев развивающейся угрозы, т.е. одна угроза ведет к новой, более коварной угрозе.

Значение уровня угрозы по уязвимости в данном случае задается в диапазоне от 0 до 1.

Общий уровень нескольких угроз уязвимости ϕ_{hk} БИС (с учетом всех угроз, воздействующих на БИС) рассчитывается по следующей формуле:

$$\phi_{hk} = 1 - \sum_{i=1}^n (1 - \frac{\beta_i}{n}), \quad (10)$$

где β – суммарный уровень угрозы для всех уязвимостей. Величина уровня угрозы варьируется от 0 до 1.

Следовательно, $P_{уя}$ технического изделия, находящегося в эксплуатации, можно рассчитывать следующим образом: (11)

$$P_{уя} = \phi_{hk} * f(t),$$

где $f(t)$ – критичность ресурса. Качественный показатель, задаваемый экспертом или количественно, рассчитывается как разница в вероятности отказа при определенном расходе ресурса в момент t ;

ϕ_{hk} – общий уровень угрозы ресурса за все время эксплуатации изделия.

$P_{уя}$ БИС ВС рассчитывается по следующим уравнениям:

для количественной оценки уровня риска из уравнения (4, 5, 6) для (7) получаем (ε):

$$\varepsilon = 1 - \sum_{i=1}^n R_i, \quad (12)$$

где R – ресурсный риск;

для качественной оценки уровня рисков, протекающих параллельно (ε):

$$\varepsilon = \left(1 - \prod_{i=1}^n \left(1 - \frac{R_i}{100}\right)\right) * 100. \quad (13)$$

Следовательно, уравнение (13) преобразуется в (14) :

$$\varepsilon = \left(1 - \prod_{i=1}^n \left(1 - \frac{\sum_{i=1}^n \left(\left(1 - \frac{\beta_i}{n}\right) - \left(\left(1 - \frac{\beta_i}{n}\right) * f(t) \right) + \left(\left(1 - \frac{\beta_i}{n}\right)^2 * f(t) \right) \right) * P_{уш}}{100}\right)\right) * 100 \quad (14)$$

Для оценки ожидаемых ущербов от одинарной или комбинированной концепции безопасности $Y_{но}$ применяем уравнение (15):

$$Y_{но} = P_{уш} * k_s * E, \quad (15)$$

где k_s – условное математическое ожидание ущерба с учетом того, что событие угрозы уже произошло; E – параметр, измеряющий степени воздействия угроз(ы) в момент реализации события угрозы.

Следовательно, степень ущерба вероятной угрозы $P_{уш}$ покажет, до какой степени контрольные меры противодействий угроз системы с учетом технической оснащенности изделия допускает появление события угрозы в результате, которого последствия угрозы могут привести к частичной или полной потери функциональности изделия/системы АТ. Модели оценки степени вероятной угрозы используют комбинацию поведенческих данных (тенденции прошлых событий и истории), финансовой информации (опережающие индикаторы на основе финансовых коэффициентов) и субъективной информации (профиль персонала, информационное обеспечение службы авиационной, информационной безопасности и безопасности полетов). Условное математическое ожидание ущерба с учетом того, что событие угрозы уже произошло k_s .

Оценка k_s варьируется в зависимости от базового события угрозы, обусловленного требованиями к трем концепциям безопасности. k_s также можно выразить как $1 - v_s$, где v_s

означает скорость восстановления от совершенного события угрозы. Параметр, измеряющий степени воздействия угроз(ы) в момент реализации события угрозы оценивается как:

$$E = \alpha * \left(\frac{C - \emptyset}{\emptyset} \right),$$

где α – коэффициент подобия k_s ; C – стоимость защищаемого объекта до совершения угрозы; $\emptyset$ – вероятная стоимость защищаемого объекта после совершения угрозы. Уровень ожидаемого ущерба можно выразить по уравнению (16):

$$Y_{\text{но}} = P_{\text{уш}} * (1 - v_s) * \left(\alpha * \left(\frac{C - \emptyset}{\emptyset} \right) \right). \quad (16)$$

Если предположить, что уровень ожидаемого ущерба определенной угрозы задается на этапе проектирования защищаемого объекта как $Y_{\text{но}} = 1 - E$, получим:

$$1 - E = P_{\text{уш}} * (1 - v_s) * E. \quad (17)$$

Таким образом получаем выражение степени ущерба вероятной угрозы для подстановки обратно в уравнение (14):

$$P_{\text{уш}} = \frac{1 - E}{(1 - v_s) * E}. \quad (18)$$

Следовательно, уравнение (14) принимает вид:

$$\varepsilon = \left(1 - \prod_{i=1}^n \left(1 - \frac{\sum_{i=1}^n \left(\left(1 - \frac{\beta_i}{n} \right) - \left(\left(1 - \frac{\beta_i}{n} \right) * f(t) \right) + \left(\left(1 - \frac{\beta_i}{n} \right)^2 * f(t) \right) \right) * \frac{1 - E}{(1 - v_s) * E}}{100} \right) \right) * 100 \quad (19)$$

Качественная оценка трехкомпонентных рисков позволит иметь общую картинку состояния обеспеченной безопасности относительно нескольким угрозам и их последствиям.

ЗАКЛЮЧЕНИЕ

Выявлена проблема обеспечения безопасности сложных комплексных бортовых систем ВС, которая должна решаться с учетом комплексной функции обеспечения авиационной безопасности, информационной безопасности и безопасности полетов. В связи с этим оценка риска безопасности только одним из математических инструментов нецелесообразна, т.к. будет ограничена отдельными показателями одной из рассматриваемых концепций безопасности. Отдельная оценка риска в данном случае не позволит учитывать тяжесть всех опасностей для определения доверительной границы приемлемого риска. Также нельзя будет оценивать эффективность контрольного уровня риска в процессе технической эксплуатации АТ с учетом стоимостных, функциональных параметров, что может в эксплуатации привести к неуправляемым расходам по ТО и Р [24]. Например, будет сложно определить насколько оправдано отправить ВС на техническое обслуживание и ремонт после внешнего воздействия нарушителя при совершении АНВ.

Изложенные выше сведения являются лишь базовыми критериями, требующими уточнения, и не позволяют в полной мере решить комплексную задачу обеспечения всесторонней безопасности бортовых информационных систем (БИС) ВС из-за сложности в

унификации критериев оценки степени опасности по всем концепциям безопасности. Однако предложенная в статье методика может стать катализатором формирования новых критериев единой базы оценки безопасности такой технической системы, как БИС, так как содержит в себе трехкомпонентные параметры риска, т. е. риск по угрозам, уязвимости и ущербу (последствиям). В заключение можно сделать вывод о том, что для повышения эффективности оцениваемого риска бортовых информационных систем ВС целесообразно объединение критериев и математических инструментов риска по трем компонентам безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. **Федосов Е.А.** Перспективный облик и технологии разработки комплексов бортового оборудования воздушных судов / Е.А. Федосов, Г.А. Чуянов, В.В. Косьянчук, Н.И. Сельвесюк // Полет. Общероссийский научно-технический журнал. 2013. № 8. С. 41–52.
2. **Белов Е.Б.** Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. М.: Горячая линия–Телеком, 2006. 544 с.
3. **Демин В.В., Суворов Е.В.** Интегрированная система информационной безопасности // Сети и системы связи. 1996. № 9. С. 127–133.
4. **Biesecker C.** Boeing 757 testing shows airplanes vulnerable to hacking [Электронный ресурс] // Aviation explorer. URL: <https://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/> (дата обращения 11.05.2020).
5. **Alhabeeb M.** Information security threats classification pyramid / M. Alhabeeb, A. Almuhaideb, P.D. Le, B. Srinivasan // Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications Workshops, 2010. Pp. 208–213.
6. **Strohmeier M.** On perception and reality in wireless air traffic communication security / M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, I. Martinovic // IEEE Transactions on Intelligent Transportation Systems. 2017. Vol. 18, no. 6. Pp. 1338–1357.
7. **Jacob J.M.** High assurance security and safety for digital avionics // The 23rd Digital Avionics Systems Conference (IEEE Cat. No.04CH37576), USA: Salt Lake City, UT, 2004. Pp. 8. DOI: 10.1109/DASC.2004.1390776
8. **Sun J.Z.** Integration of scheduled structural health monitoring with airline maintenance program based on risk analysis / J.Z. Sun, D. Chen, C.Y. Li, H.S. Yan // Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. 2018. Vol. 232, iss. 1. Pp. 92–104. DOI: <https://doi.org/10.1177/1748006X17742777>
9. **Liao N., Li F., Song Y.** Research on real-time network security risk assessment and forecast // International Conference on Intelligent Computation Technology and Automation (ICICTA), China: Changsha. 2010. Vol. 3. Pp. 84–87.
10. **Jungwirth P.** Cyber defense through hardware security / P. Jungwirth, P. Chan, T. Barnett, A.H. Badawy // Disruptive Technologies in Information Sciences. International Society for Optics and Photonics, 2018. Vol. 10652. Pp. 106520P. DOI: <https://doi.org/10.1117/12.2302805>
11. **Ortalo R., Deswarte Y., Kaaniche M.** Experimenting with quantitative evaluation tools for monitoring operational security // IEEE Transactions on Software Engineering. 1999. Vol. 25, no. 5. Pp. 633–650. DOI: 10.1109/32.815323
12. **Ben Mahmoud M.S., Larrieu N., Pirovano A.** A risk propagation based quantitative assessment methodology for network security-aeronautical network case study // 2011 Conference on Network and Information Systems Security. La Rochelle, 2011. Pp. 1–9. DOI: 10.1109/SAR-SSI.2011.5931372

13. **Barlow R.E., Proschan F.** Importance of system components and fault tree events // Stochastic Processes and their Applications. 1975. Vol. 3, iss. 2. Pp. 153–173. DOI: [https://doi.org/10.1016/0304-4149\(75\)90013-7](https://doi.org/10.1016/0304-4149(75)90013-7)
14. **Barlow R.E., Proschan F.** Statistical theory of reliability and life testing. probability models. Silver Springs, MD, 1981. 290 p.
15. **Goncharenko A.** Development of a theoretical approach to the conditional optimization of aircraft maintenance preference uncertainty // Aviation. 2018. Vol. 22, no. 2. Pp. 40–44. DOI: <https://doi.org/10.3846/aviation.2018.5929>
16. **Obadimu S.O., Karanikas N., Kourousis K.I.** Development of the minimum equipment list: Current practice and the need for standardization [Электронный ресурс] // Aerospace. 2020. Vol. 7, iss. 1. 7. URL: <https://www.mdpi.com/2226-4310/7/1/7> (дата обращения 3.05.2020). DOI: <https://doi.org/10.3390/aerospace7010007>
17. **Chuyanov G.A.** Advanced avionics equipment on the basis of second generation integrated modular avionics / G.A. Chuyanov, V.V. Kosyanchuk, N.I. Selvesyuk, E.Yu. Zybin // 29th Congress of the International Council of the Aeronautical Sciences, ICAS 2014. 6 p.
18. **Зубков Б.В.** Методологические основы анализа и оценки безопасности полетов и летной годности воздушных судов (теория и практика). М.: МГТУГА, 1997. 68 с.
19. **Зубков Б.В., Аникин Н.В.** Авиационное техническое обеспечение безопасности полетов. М.: Воздушный транспорт, 1993. 280 с.
20. **Зубков Б.В., Шаров В.Д.** Теория и практика определения рисков в авиапредприятиях при разработке системы управления безопасностью полета. М.: МГТУГА, 2010. 196 с.
21. **Зыбин Е.Ю., Косьянчук В.В., Сельвесюк Н.И.** Электрификация и интеллектуализация - основные тенденции развития энергокомплекса воздушных судов // Авиационные системы. 2016. № 5. С. 45–51.
22. **Deng Q.C., Santos B.F., Curran R.** A practical dynamic programming based methodology for aircraft maintenance check scheduling optimization // European Journal of Operational Research. 2020. Vol. 281, iss. 2. Pp. 256–273. DOI: <https://doi.org/10.1016/j.ejor.2019.08.025>
23. **Batuwangala E., Silva J., Wild G.** The regulatory framework for safety management systems in airworthiness organisations [Электронный ресурс] // Aerospace. 2018. Vol. 5, iss. 4. 117. URL: <https://www.mdpi.com/2226-4310/5/4/117> (дата обращения 7.06.2020). DOI: <https://doi.org/10.3390/aerospace5040117>
24. **Stadnicka D.** Skills management in the optimization of aircraft maintenance processes / D. Stadnicka, D. Arkhipov, O. Battaia, M.C. Chandima Ratnayake // 20th IFAC World Congress. 2017. Vol. 50, iss. 1. Pp. 6912–6917. DOI: <https://doi.org/10.1016/j.ifacol.2017.08.1216>

СВЕДЕНИЯ ОБ АВТОРАХ

Фурап Хуссам Эддин, Университет Хаджи Лахдар, г. Батна, Алжирская Народная Демократическая Республика, housameddine05500@gmail.com.

Огунвоул Блессинг Деле, Национальное агентство космических исследований и разработок, г. Абуджа, Нигерия, dams4iboko@mail.ru.

Будаев Владислав Дмитриевич, ПАО «Аэрофлот», vlad_budaev@mail.ru.

Лаши Фахреддин, Университет Хаджи Лахдар, г. Батна, Алжирская Народная Демократическая Республика, fakhroadkins@gmail.com.

RISK ASSESSMENT IN ENSURING AIRCRAFT ON-BOARD SYSTEMS SAFETY

Houssam E. Fourar¹, Blessing D. Ogunvoul², Vladislav D. Budaev³,
Fakhreddine Lachi¹

¹Hadj Lakhdar University, Batna, People's Democratic Republic of Algeria

²National Space Research and Development Agency, Abuja, Nigeria

³PJSC "Aeroflot – Russian Airlines", Moscow, Russia

ABSTRACT

A method of risk assessment of an aircraft on-board information system is being considered, which allows ensuring reliability and safety of such a complex system in operation. This technique implies application of combined mathematical tools to estimate the risks that complex systems/items are being exposed to. The existing risk assessment methods are not flexible enough to solve the complex task of enhancing comprehensive safety of an aircraft information system (AIS) due to difficulty in unifying the criteria for estimating the degree of hazard in reference to all safety concepts. Currently, risks severity and mechanism for the development of one undesirable event (risk event) into more complex forms during technical operation of an aircraft items/system are not being considered. However, the method proposed in this article intends to become a catalyst for generation of new criteria on a unified basis for estimating safety of such a technical complex system such as AIS, since it contains three-component risk parameters. I.e. the risk for threats from violators (cases of unlawful interference (UI)), vulnerabilities (functional hazards that contribute to UI and its development in a system) and loss (set of criteria that evaluates consequences of UI). As a result, these criteria and parameters of three-component safety will allow us to find a new approach to determining the complex risk to which important aircraft systems, such as on-board aircraft information systems, are exposed. This article presents a method for determining risk that takes into account the three-component safety concept. Together, these components will make it possible to evaluate technical systems hazard degree, taking into account their sophistication. The information provided in this paper by the authors is a scientific hypothesis designed to draw attention of the scientific community to the problem of lack of methods for evaluating multicomponent risks in such a system as AIS. The article presents the basic criteria for evaluating a complex three-component risk; they are not sufficient for the full formation of new criteria for evaluating the safety of a complex aircraft system/item and requires clarification of their parameters. Thus, this work is not absolute as a complete solution to the complex problem of enhancing comprehensive safety of AIS, but only offers a methodology for unifying the three safety components to evaluate complex risk.

Key words: risk; safety; on-board information system; technical operation process.

REFERENCES

1. Fedosov, E.A., Chuyanov, G.A., Kosyanchuk, V.V. and Selvesyuk, N.I. (2013). *Future image of technology and the development of the aircraft onboard equipment*. Scientific-Technical Journal "Polyot" ("Flight"), no. 8, pp. 41–52. (in Russian)
2. Belov, E.B., Los, V.P., Meshcheryakov, R.V. and Shelupanov, A.A. (2006). *Osnovy informatsionnoy bezopasnosti: uchebnoye posobiye dlya VUZov* [Information security fundamentals: Tutorial]. Moscow: Goryachaya liniya-Telekom, 544 p. (in Russian)
3. Demin, V.V. and Suvorov, E.V. (1996). *Integrirovannaya sistema informatsionnoy bezopasnosti* [Integrated information security system]. Seti i sistemy svyazi, no. 9, pp. 127–133. (in Russian)
4. Biesecker, C. *Boeing 757 testing shows airplanes vulnerable to hacking*. Aviation explorer. Available at: <https://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/> (accessed: 11.05.2020).

5. **Alhabeeb, M., Almuhaideb, A., Le, P.D. and Srinivasan, B.** (2010). *Information security threats classification pyramid*. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications Workshops, pp. 208–213.
6. **Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V. and Martinovic, I.** (2017). *On perception and reality in wireless air traffic communication security*. IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 6, pp. 1338–1357.
7. **Jacob, J.M.** (2004). *High assurance security and safety for digital avionics*. The 23rd Digital Avionics Systems Conference (IEEE Cat. No.04CH37576), Salt Lake City, UT, USA, pp. 8. DOI: 10.1109/DASC.2004.1390776
8. **Sun, J.Z., Chen, D., Li, C.Y. and Yan, H.S.** (2018). *Integration of scheduled structural health monitoring with airline maintenance program based on risk analysis*. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, vol. 232, issue 1, pp. 92–104. DOI: <https://doi.org/10.1177/1748006X17742777>
9. **Liao, N., Li, F. and Song, Y.** (2010). *Research on real-time network security risk assessment and forecast*. International Conference on Intelligent Computation Technology and Automation (ICICTA), Changsha, China, vol. 3, pp. 84–87.
10. **Jungwirth, P., Chan, P., Barnett, T. and Badawy, A.H.** (2018). *Cyber defense through hardware security*. Disruptive Technologies in Information Sciences. International Society for Optics and Photonics, vol. 10652, pp. 106520P. DOI: <https://doi.org/10.1117/12.2302805>
11. **Ortalo, R., Deswarte, Y. and Kaaniche, M.** (1999). *Experimenting with quantitative evaluation tools for monitoring operational security*. IEEE Transactions on Software Engineering, vol. 25, no. 5, pp. 633–650. DOI: 10.1109/32.815323
12. **Ben Mahmoud, M.S., Larrieu, N. and Pirovano, A.** (2011). *A risk propagation based quantitative assessment methodology for network security-aeronautical network case study*. 2011 Conference on Network and Information Systems Security, La Rochelle, pp. 1–9. DOI: 10.1109/SAR-SSI.2011.5931372
13. **Barlow, R.E and Proschan, F.** (1975). *Importance of system components and fault tree events*. Stochastic Processes and their Applications, vol. 3, issue 2, pp. 153–173. DOI: [https://doi.org/10.1016/0304-4149\(75\)90013-7](https://doi.org/10.1016/0304-4149(75)90013-7)
14. **Barlow, R.E and Proschan, F.** (1981). *Statistical theory of reliability and life testing. probability models*. Silver Springs, MD, 290 p.
15. **Goncharenko, A.** (2018). *Development of a theoretical approach to the conditional optimization of aircraft maintenance preference uncertainty*. Aviation, vol. 22, no. 2, pp. 40–44. DOI: <https://doi.org/10.3846/aviation.2018.5929>
16. **Obadimu, S.O., Karanikas, N. and Kourousis, K.I.** (2020). *Development of the minimum equipment list: Current practice and the need for standardisation*. Aerospace, vol. 7, issue 1, 7. Available at: <https://www.mdpi.com/2226-4310/7/1/7> (accessed 3.05.2020). DOI: <https://doi.org/10.3390/aerospace7010007>
17. **Chuyanov, G.A., Kosyanchuk, V.V., Selvesyuk, N.I. and Zybin, E.Yu.** (2014). *Advanced avionics equipment on the basis of second generation integrated modular avionics*. 29th Congress of the International Council of the Aeronautical Sciences, ICAS 2014, 6 p.
18. **Zubkov, B.V.** (1997). *Metodologicheskiye osnovy analiza i otsenki bezopasnosti poletov i letnoy godnosti vozdushnykh sudov (teoriya i praktika)* [Methodological bases of analysis and evaluation of the aircraft flight safety and airworthiness (theory and practice)]. Moscow: MGTU GA, 1997. 68 p. (in Russian)
19. **Zubkov, B.V. and Anikin, N.V.** (1993). *Aviatsionnoye tekhnicheskoye obespecheniye bezopasnosti poletov* [Aviation technical maintenance of flight safety]. Moscow: Vozdushnyy transport, 280 p. (in Russian)

20. Zubkov, B.V. and Sharov, V.D. (2010). *Teoriya i praktika opredeleniya riskov v aviapredpriyatiyakh pri razrabotke sistemy upravleniya bezopasnostyu poleta* [Theory and practice of determining risks in aviation enterprises during the flight safety management system development]. Moscow: MGTU GA, 196 p. (in Russian)

21. Zybin, E.Yu., Kosyanchuk, V.V. and Selvesyuk, N.I. (2016). *Elektrifikatsiya i intellektualizatsiya - osnovnyye tendentsii razvitiya energokompleksa vozдушnykh sudov* [Electrification and intellectualization are the main trends in the development of the aircraft power complex]. *Aviatsionnyye sistemy*, no. 5, pp. 45–51. (in Russian)

22. Deng, Q.C., Santos, B.F. and Curran, R. (2020). *A practical dynamic programming based methodology for aircraft maintenance check scheduling optimization*. *European Journal of Operational Research*, vol. 281, issue 2, pp. 256–273. DOI: <https://doi.org/10.1016/j.ejor.2019.08.025>

23. Batuwangala, E., Silva, J. and Wild, G. (2018). *The regulatory framework for safety management systems in airworthiness organisations*. *Aerospace*, vol. 5, issue 4, 117 p. Available at: <https://www.mdpi.com/2226-4310/5/4/117> (accessed 7.06.2020). DOI: <https://doi.org/10.3390/aerospace5040117>

24. Stadnicka, D., Arkhipov, D., Battaia, O. and Chandima Ratnayake, M.C. (2017). *Skills management in the optimization of aircraft maintenance processes*. 20th IFAC World Congress, vol. 50, issue 1, pp. 6912–6917. DOI: <https://doi.org/10.1016/j.ifacol.2017.08.1216>

INFORMATION ABOUT THE AUTHORS

Houssam E. Fourar, Hadj Lakhdar University, Batna, People's Democratic Republic of Algeria, houssameddine05500@gmail.com

Blessing D. Ogunvoul, National Space Research and Development Agency, Abuja, Nigeria, dams4iboko@mail.ru.

Vladislav D. Budaev, PJSC "Aeroflot – Russian Airlines", budaev_2021@mail.ru

Lachi Fakhreddine, Hadj Lakhdar University, Batna, People's Democratic Republic of Algeria, fakhroadkins@gmail.com.

Поступила в редакцию 29.02.2020
Принята в печать 23.07.2020

Received 29.02.2020
Accepted for publication 23.07.2020