УДК 629.7.017.1 DOI: 10.18698/0236-3933-2016-6-85-96

МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БОРТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ СРЕДСТВ САМОЛЕТА

Е.В. Глинская Glinskaya-iu8@rambler.ru
Н.В. Чичварин genrih.gertz@gmail.com

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Изложены результаты исследований и анализа вычислительных средств в комплексах связи и навигации самолета, проведенных в целях построения формализованной модели угроз. На основании анализа обзоров доступной литературы показано, что проблема безопасности полетов нарастает. По мнению специалистов, в условиях повышения уровня автоматизации перспективных авиационных двигателей, бортового оборудования, систем и агрегатов летальных аппаратов, возрастания сложности бортовых информационных систем существенное значение приобретает проблема защиты автоматизированных систем авиационной техники от угроз информационной безопасности. Рассмотрены возможности учета специфических лавинных атак, которые могут возникать в вычислительных системах, построенных на модульных платформах

Ключевые слова

Авионика, автоматизированные системы, безопасность, вычислительные системы, информация, модуль, платформа

Поступила в редакцию 05.05.2016

Введение. Публикация посвящена результатам исследований и анализу средств информационной безопасности (ИБ) комплексов связи и навигации самолета, проведенных в целях построения формализованной модели угроз комплекса бортового оборудования (КБО). Основное внимание уделено ИБ бортовых вычислительных средств. Анализ обзоров доступной литературы показывает, что проблема безопасности полетов нарастает [1, 2]. В условиях возрастания уровней сложности и автоматизации перспективных бортовых инофрмационных систем, агрегатов и систем летательных аппаратов (ЛА), по мнению ведущих специалистов в области ИБ, немаловажное значение приобретает проблема защиты автоматизированных систем авиационной техники от угроз ИБ. Источниками подобных угроз являются:

- беспроводные информационно-телекоммуникационные устройства пассажиров, находящиеся на борту ЛА во время полета;
- информационные атаки внешних злоумышленников по беспроводным каналам передачи данных, обеспечивающим доступ к бортовой вычислительной сети;
- помехи, случайно либо умышленно поставленные с помощью средств радиоэлектронной борьбы (РЭБ).

Основными факторами, обусловливающими актуализацию угроз ИБ в отношении бортовых автоматизированных систем, являются:

- увеличение функциональной нагрузки и возрастание сложности бортовой вычислительной сети, лежащей в основе всего КБО;
- резкое возрастание сложности контрольно-измерительной (сенсорной) инфраструктуры перспективных двигательных установок и общесамолетных систем, включающей распределенные сети интеллектуальных датчиков и базирующейся в том числе на использовании беспроводных технологий;
- агрегирование бортового и наземного оборудования информационного обеспечения в рамках концепции авиационной безопасности CNS/ATM [3, 4];
- децентрализация архитектуры построения систем автоматизированного управления двигательными установками и общесамолетными системами, обеспечивающая сокращение количества радиальных линий связи за счет перехода к мультиплексным каналам [5];
- значительная доля импортного радиоэлектронного оборудования со встроенным программным обеспечением;
- не декларированные возможности встроенного программного обеспечения бортового радиоэлектронного оборудования.

Стали известными действия злоумышленников по вредоносному воздействию на ЛА. Так, на конференции *Hack In The Box* в Амстердаме, консультант по безопасности из *n.runs AG* Хьюго Тесо сообщил о полностью достоверном сценарии угона самолета с помощью простого Android-приложения. Воспользовавшись преимуществом двух новых авиационных систем для обнаружения уязвимости, сбора сообщений и эксплуатации, создав фреймворк (SIMON) и приложение для Android (PlaneSploit), которые доставляют атакующее сообщение системе управления полетом самолета (Flight Management Systems), он продемонстрировал возможность получить полный контроль над самолетом. Участившиеся локальные и региональные конфликты, в которых применяются современное высокоточное оружие и средства РЭБ, угрожают почти напрямую полетам гражданских ЛА. Таким образом, вопросы проектирования средств обеспечения ИБ ЛА и ИБ средств связи, управления и навигации ЛА можно считать актуальными.

Цель исследований и решаемые задачи. В процессе подготовки статьи проведен аналитический обзор доступных источников, позволивший установить, что для разработки средств обеспечения ИБ ЛА необходима строгая и хорошо формализованная модель угроз. Известные подходы к ее построению основаны на вербальных оценках и обобщении мнений экспертов. При этом невозможно ограничить область адекватности теоретически возможными атаками, т. е. обеспечить необходимую полноту модели. Кроме того, такие модели не учитывают лавинообразно нарастающие сбои и отказы КБО (эффект домино). Таким образом, целью настоящей работы является описание разработанной методики формирования модели угроз ИБ КБО при лавинном нарастании атак. Для достижения поставленной цели решались следующие задачи:

- анализ состава КБО ЛА с учетом перспектив его развития;
- анализ атак на ИБ КБО, возможность которых ограничена физической реализуемостью;
- выявление условий возникновения спровоцированных лавинных сбоев и отказов.

Основные результаты аналитического обзора и проведенных исследований. В проектах известных сегодня отечественных образцов бортовых цифровых вычислительных систем (БЦВС) [5–8] в качестве внутрисистемного интерфейса используются интерфейсы ARINC664 (Gigabit Ethernet 1000Base-SX, AFDX), CompactPCI (PICMG 2.0, D3.0), PCI Express, RapidIO, VME64x и др. В рассмотренных публикациях отмечается, что построение БЦВС на основе параллельных внутрисистемных интерфейсов типа CompactPCI, PCI Express, RapidIO (LP-LVDS), VME64x с большим количеством проводников во внутрисистемном интерфейсе сегодня не может обеспечивать высокую отказоустойчивость БЦВС при работе интерфейса в гигагерцовом диапазоне частот и, следовательно, отказобезопасность работы БЦВС в целом. Но даже отсутствие отказов не исключает возникновение сбоев. Следует отметить, перспективная архитектура БЦВС базируется сегодня на сетевых технологиях с применением высокоскоростных последовательных внутрисистемных интерфейсов, допускающих коммутацию электрических межмодульных соединений и, следовательно, возможность построения динамически реконфигурируемых вычислительных структур. А это может породить вероятное возникновение лавинообразных либо волновых сбоев в процессе их функционирования. Примером перспективной БЦВС, построенной на основе унифицированных конструктивно-функциональных модулей, является комплекс, разработанный в АО «ОКБ «Электроавтоматика» им. П.А. Ефимова» [6]. В качестве функциональных модулей (ФМ) в нем выступают:

– вычислительные модули, производящие расчеты для управления полетом ЛА;

– модули ввода-вывода, обеспечивающие функции обмена данными по всем каналам;

– графические модули, обрабатывающие изображение для его вывода на средства бортовой индикации;

– модули постоянной памяти (МПП), предназначенные для хранения системного программного обеспечения.

В основу архитектуры вычислительной системы положены сетевые топологии коммутации модулей «двойная звезда» и «полносвязная сеть» (рис. 1).

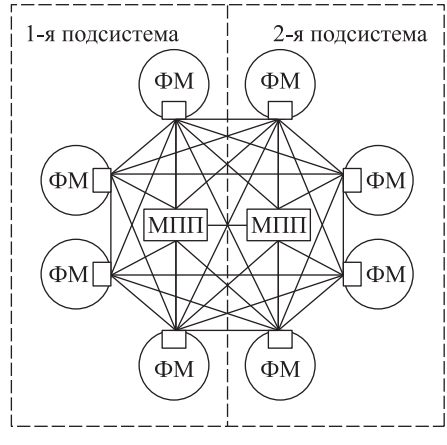

Рис. 1. Структурная схема сетевой топологии БЦВС

Схема, представленная на рис. 1, обеспечивает повышение надежности благода-

ря возможности полного резервирования каналов связи при подключении по топологии «двойная звезда», обеспечивает резервирование каналов и максимальные значения пропускной способности благодаря использованию топологии «полносвязная сеть». Отмечается, что такая архитектура создает предпосылки для реализации нескольких вариантов решения вычислительных задач:

– каждая задача выполняется на собственном вычислительном устройстве;

– все задачи реализуются на одном вычислительном устройстве;

– часть задач выполняется на индивидуальных вычислительных устройствах, остальные задачи — на одном вычислительном устройстве.

Разработчики показывают, как за счет организации логических протоколов взаимодействия между модулями разные правила назначения функциональных задач на имеющиеся вычислительные ресурсы влияют на возможность повышать надежность или увеличивать количество решаемых задач. Приведем пример модульной структуры (рис. 2).

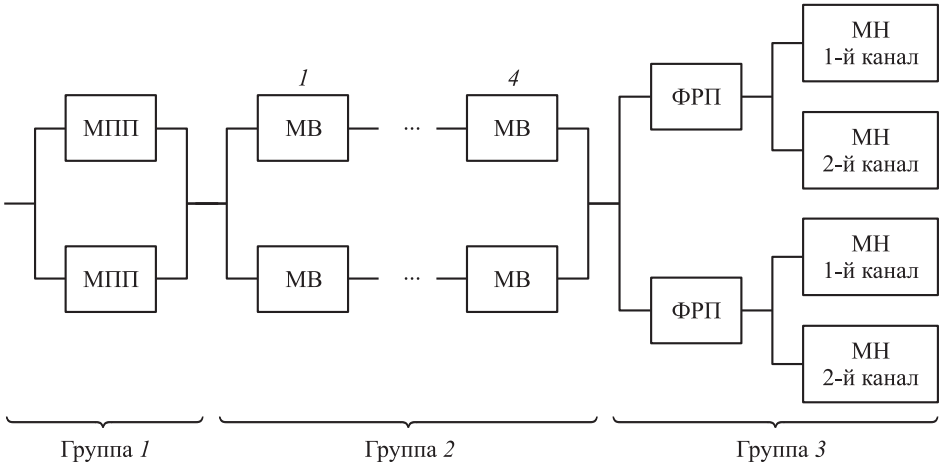

Рис. 2. Схема вычислительной системы с резервированием в виде дублирования последовательных групп из четырех модулей МВ (вычислительных)

Показатели надежности по группам

Последовательные группы	Вероятность безотказной работы $P(\tau)$	Интенсивность отказов $Q(\tau)$
1	0,999976	$2{,}48 \cdot 10^{-5}$
2	0,999855	$1{,}45 \cdot 10^{-4}$
3	0,9999999997	$2{,}58 \cdot 10^{-9}$
Система	–	$1{,}94 \cdot 10^{-4}$

Структура разбита на три группы: группу *1*, состоящую из двух модулей МПП, группу *2*, состоящую из восьми модулей МВ и группу *3*, состоящую из четырех модулей МН и двух фильтров радиопомех (ФРП). Представлен вариант, когда для решения необходимого объема задач в полете достаточно четырех вычислительных модулей, поэтому оставшиеся четыре вычислительных модуля можно использовать как резервную цепочку для горячего резервирования. Показатели вероятности безотказной работы $P(\tau)$ и интенсивности отказа $Q(\tau)$ для каждой группы представлены в таблице.

Таким образом, показатель наработки на отказ при допущении о независимости каждого отказа для времени полета $t = 25$ ч будет равен

$$T = \frac{t}{Q_{\text{сист}}} = 129100 \text{ ч.}$$

Приведенный оптимистичный пример не учитывает последствий воздействия побочного электромагнитного излучения на КБО в случаях возникновения сбоев, так как методика, используемая разработчиками, не учитывает зависимых сбоев и отказов.

Модели лавинных угроз ИБ КБО. Как отмечалось, существенным фактором ИБ КБО является возникновение аппаратно-программных сбоев, каждый из которых не в полной мере определяет безопасное функционирование вычислительной системы в целом, но последствия атаки на один из модулей могут стать атаками на другие модули. Отметим, что это явление может стать характерным для постоянно усложняющегося КБО. Для построения таких моделей применим аппарат сетей Петри.

Модель на основе сети Петри. Существует несколько формальных определений сети Петри, отличающихся способами задания элементов и связей в сети. Поэтому далее отражаются основные положения [10], принятые в настоящей работе. Одно из важнейших свойств сети Петри, которая должна моделировать реальное устройство, — это безопасность. Сеть Петри безопасна, если безопасны все позиции сети. Принимается, что сеть Петри $C = (P, T, I, O)$, где P — непустое множество элементов сети, называемых местами; T — непустое множество элементов сети, называемых переходам; I — функция инцидентности, задающая связи между элементами множеств P и T; O — функция выходов. Принимается, что позиция p_i, принадлежащая P, с начальной маркировкой m является безопасной, если $m'(p_i) \le 1$ для любой m', принадлежащей $R(C, m)$. Сеть Петри безопасна, если безопасна каждая ее позиция. Если интерпретировать сети как условия и события, то маркировка каждой позиции должна быть безопасной. В безопасной сети любой переход, удаляющий фишку из p_i, должен помещать фишку в $p_{i'}$, а всякий переход, удаляющий фишку из $p_{i'}$, должен помещать фишку в p_i. Начальная маркировка также должна быть модифицирована для обеспечения того, чтобы только одна фишка была либо в p_i, либо в $p_{i'}$. Такая принудительная безопасность возможна лишь для позиций, которые в начальной маркировке являются безопасными, и входная, и выходная кратность которых равна нулю или единице для всех переходов. Позиция, имеющая для некоторого перехода выходную кратность два, будет получать при его запуске две фишки и, следовательно, не может быть безопасной. На рис. 3 простая сеть Петри (*а*) преобразована в безопасную (*б*).

Установлено, что сети Петри можно использовать для моделирования как систем распределения ресурсов (в частности, вычислительных), так и ресурсов надежности. Для их сохранности фишки, представляющие ресурсы, не должны

создаваться или уничтожаться, общее число фишек в сети должно оставаться постоянным. Для моделирования разветвленных систем возможно применение методов расширения, которые позволяют экстраполировать результаты построения модели частной задачи, например, при построении модели для большего числа пользователей. Для решения таких задач полезно применение структурированных сетей. В структурированных сетях некоторые из переходов являются сложными. При их срабатывании запускается сеть другого уровня иерархии (рис. 4).

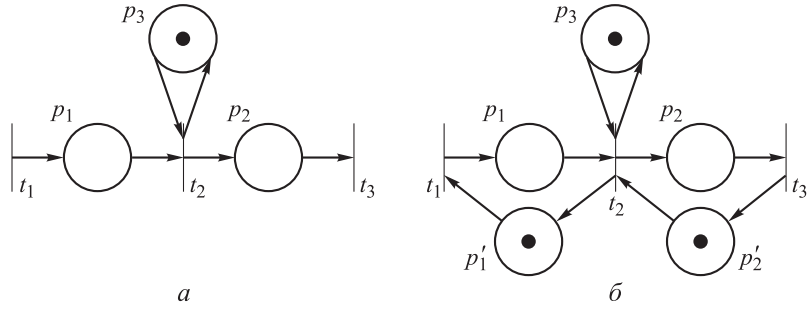

Рис. 3. Сеть Петри, не являющаяся безопасной (*а*), и безопасная сеть Петри (*б*), эквивалентная сети (*а*)

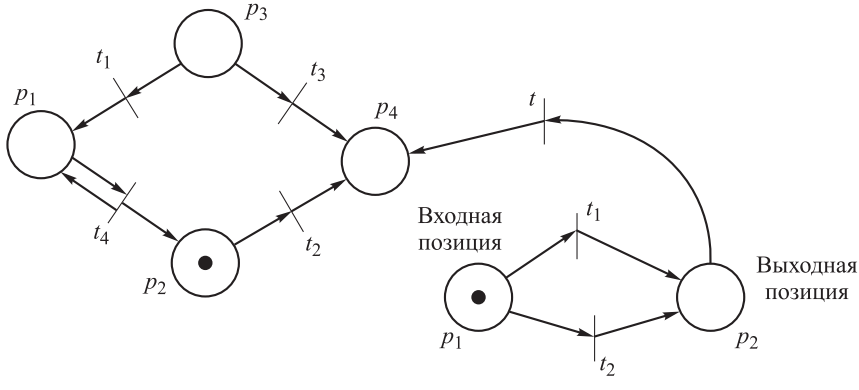

Рис. 4. Структурированная сеть Петри

Срабатывание t_2 приводит к запуску сети другого уровня. Выполнение сложного перехода заключается в помещении во входную позицию по сети фишки. После выполнения сети фишка появляется в ее выходной позиции, затем формируются фишки в выходных позициях сложного перехода. Преобразование сети к виду, имеющему один вход и один выход, всегда возможно. Поскольку такие сети используются для моделирования модульных вычислительных систем, они полезны для решения задач, поставленных в работе.

Методы, основанные на нейросетях. Такая группа методов основана на концепции: на вход персептрона (сети из взаимосвязнных нейронов) поступают данные (сигналы) о значениях контролируемых параметров КБО ЛА. На выходах продуцируются:

- данные о возможных управляющих воздействиях (1-й вариант);
- данные о соответствии систем КБО ЛА требованиям безопасности (2-й вариант).

Пример совокупности N взаимосвязанных нейронов представлен на рис. 5.

Выход i-го нейрона обозначен как $n_i(t)$, потенциал — $h_i(t)$, $i = 1, 2, ..., N$. Введем векторы-строки:

$$n(t) = \big(n_1(t),\ n_2(t), ..., n_N(t)\big),$$
$$h(t) = \big(h_1(t),\ h_2(t), ..., h_N(t)\big).$$

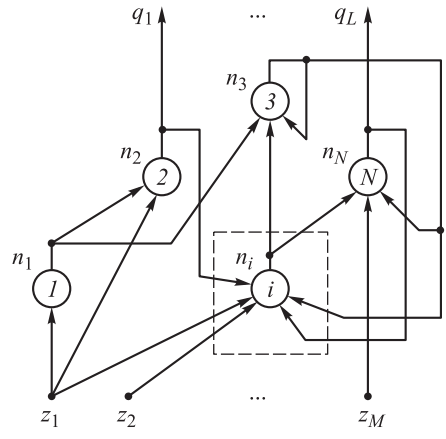

Рис. 5. Схема нейронной сети, содержащей N нейронов и имеющей M входов и L выходов

Нейронная сеть, состоящая из N указанных нейронов, подвергается воздействию вышеописанных внешних сигналов. Это воздействие представлено вектором-строкой $z(t) = \big(z_1(t),\ z_2(t),\ ...,\ z_M(t)\big)$ размерности M. Кроме внешнего воздействия $z(t)$, i-й нейрон может получать возбуждение со стороны других нейронов, что моделирует взаимосвязанность систем ЛА. Необходимо учесть и вероятные факторы полета и управления ЛА. Это можно реализовать за счет обратных связей. С учетом обратной связи с собственного выхода совокупность всех возможных входов i-го нейрона образует вектор $y(t) = \big(z(t),\ n(t)\big)$ размерности $M + N = Q$. Потенциал h_i i-го нейрона может быть представлен в форме:

$$h_i(t) = \sum_{j=1}^{N} w_{ij} n_j(t) + \sum_{j=1}^{M} v_{ij} z_j(t) - b_i,\ i = 1,\ 2,\ ...,\ N, \qquad (1)$$

где w_{ij}, $j = 1, 2, \ldots, N$, и v_{ij}, $j = 1, 2, \ldots, M$, — синоптические коэффициенты передачи соответствующих сигналов на i-й нейрон; $(-b_i)$ — смещение i-го нейрона. Введение матриц $W = \{w_{ij},\ i, j = 1, 2, \ldots, N\}$, $V = \{v_{ij},\ i = 1, 2, \ldots, N,\ j = 1, 2, \ldots, M\}$ и вектора $b = (b_1, b_2, \ldots, b_N)$ позволяет записать выражение (1) в краткой векторно-матричной форме:

$$h(t) = n(t)W^{\mathrm{T}} + z(t)V^{\mathrm{T}} - b.$$

Векторная активационная характеристика нейронов:

$$\theta[h] = \big(\theta_1[h_1], \theta_2[h_2], ..., \theta_N[h_N]\big). \qquad (2)$$

Нижний индекс в обозначении активационной характеристики $q_i[h_i]$ i-го нейрона введен в связи с тем, что нейроны могут иметь разные активационные характеристики. Обозначение (2) позволяет записать совокупность скалярных преобразований

$$n_i(t+1) = \theta_i\left[h_i(t)\right],\ \ i = 1, 2, ..., N, \tag{3}$$

в векторной форме

$$n(t+1) = \theta\left[h(t)\right]. \tag{4}$$

На рис. 6 представлена схема преобразования данных i-м нейроном в соответствии с описанной математической моделью.

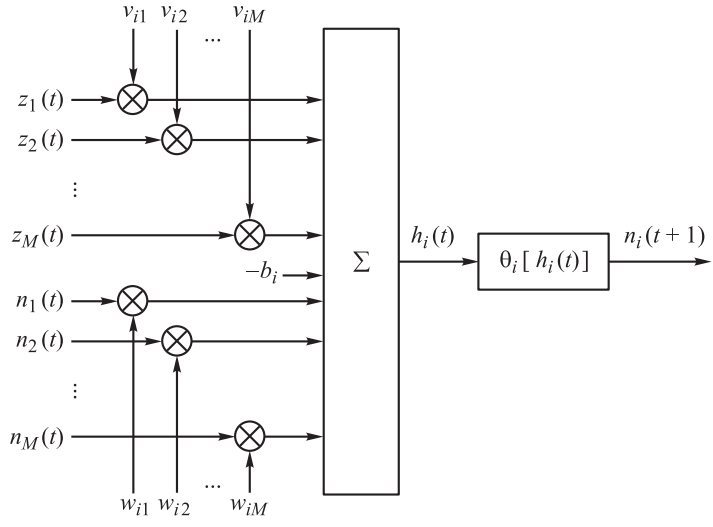

Рис. 6. Схема преобразования данных i-м нейроном в нейронной сети

Выходы нейронной сети $q_1(t)$, $q_2(t)$,..., $q_L(t)$ образуют вектор-строку $q(t)$ размерности L и представляют собой некоторое подмножество выходов нейронов $n_1(t)$, $n_2(t)$, ..., $n_N(t)$. Математически это представляется формулой

$$q(t) = n(t)R, \tag{5}$$

где R — матрица размера $N \times L$. В качестве примера можно рассмотреть следующее матричное преобразование:

$$\left(q_1, q_2, q_3\right) = \left(n_1, n_2, n_3, n_4, n_5\right)\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

которое реализует формирование выходов $q_1 = n_2$, $q_2 = n_4$, $q_3 = n_5$ в нейронной сети, содержащей пять нейронов.

Совокупность выражений (2), (4) и (5) представляет собой математическую модель нейронной сети, которая эволюционирует во времени $t = 0, 1, 2, \ldots$, отталкиваясь от начального состояния

$$n(0) = n_0, \tag{6}$$

где n_0 — вектор-строка размерности N.

Сеть реализуется совокупностью стохастических нейронов. Выход нейрона $n(t+1)$ однозначно определяется значением потенциала $h(t)$. Если потенциал нейрона в момент времени t равен $h(t)$, то на следующем такте дискретного времени вероятность события $[n(t+1)=1]$ равна $p_+(h)$, а события $[n(t+1)=-1]\, p-(h)$. Согласно формуле полной вероятности,

$$p_+(h) + p_-(h) = 1. \tag{7}$$

Существенно, что значения вероятностей $p_+(h)$ и $p_-(h)$ зависят от потенциала нейрона. Рассмотрим в качестве функции $p_+(h)$ логистическую функцию

$$p_+(h) = \frac{1}{1+e^{-\alpha h}}, \ \alpha > 0. \tag{8}$$

Тогда на основании формулы (8) вычисляется выражение для $p_-(h)$:

$$p_-(h) = \frac{1}{1+e^{\alpha h}}. \tag{9}$$

На рис. 7 дана графическая иллюстрация к формулам. Если потенциал нейрона $h(t)=0$, то с равными вероятностями реализуются значения $[n(t+1)=1]$ и $[n(t+1)=-1]$. Смещение потенциала нейрона в область положительных значений приводит к увеличению вероятности принять положительное значение $[n(t+1)=1]$. Отрицательный потенциал нейрона ведет к увеличению вероятности $[n(t+1)=-1]$. На рис. 7 в качестве примера рассмотрено положительное значение потенциала $h(t)=h'$.

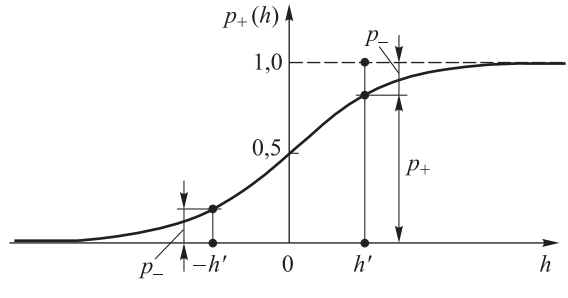

Рис. 7. Зависимость вероятности значения $n(t+1)=1$ от потенциала $h(t)$

Математическое ожидание случайного значения выхода $n(t+1)$ нейрона, если его потенциал равен $h(t)$, имеет вид:

$$M[n] = (+1)P[n = +1] + (-1)P[n = -1] =$$
$$= p_+(h) - p_-(h)\frac{1}{1+e^{-\alpha h}} - \frac{1}{1+e^{\alpha h}} = \frac{1-e^{-\alpha h}}{1+e^{-\alpha h}}. \quad (10)$$

Элементарное преобразование выражения (10) приводит к следующей формуле:

$$M[n] = \frac{e^{\frac{\alpha}{2}h} - e^{-\frac{\alpha}{2}h}}{e^{\frac{\alpha}{2}h} + e^{-\frac{\alpha}{2}h}} = \text{th}\left(\frac{\alpha}{2}h\right). \quad (11)$$

Детерминированный нейрон — это нейрон, у которого потенциал совпадает с потенциалом стохастического нейрона, а активационная характеристика определяется формулой

$$\theta[h] = \text{th}\left(\frac{\alpha}{2}h\right). \quad (12)$$

Выход детерминированного нейрона

$$\overline{n} = \text{th}\left(\frac{\alpha}{2}h\right). \quad (13)$$

Заключение. Сопоставление рассмотренных методов позволяет признать наиболее перспективным для поставленных авторами задач направление, связанное с развитием разработки когнитивных персептронов, свободных от:

- отсутствия моделей «человеческого фактора» в пилотировании, сопровождения, наведения и навигации ЛА;
- необходимости введения экспертных оценок, что нельзя применить при экспресс-контроле ЛА.

Модель лавинных угроз можно использовать в автотренажерах и авиасимуляторах для решения задачи прогноза возможности безопасного вылета ЛА.

ЛИТЕРАТУРА

1. *Aviasafety.ru:* веб-сайт. URL: http://aviasafety.ru/crash-stat (дата обращения 25.12.2013).

2. *Куклев Е.А., Волынский-Басманов Ю.М.* Обеспечение авиационной безопасности объектов гражданской авиации на основе методов управления рисками возникновения актов незаконного вмешательства. Наука и транспорт // Гражданская авиация. 2013. № 3. С. 16–21.

3. *Документы* ИКАО. Библиотека // Airspot.ru: Авиационный портал. URL: http://airspot.ru/library/dokumenty-ikao (дата обращения 20.04.2016).

4. Воздушный кодекс РФ от 19.03.1997. № 60-ФЗ // Консультант Плюс: веб-сайт. URL: http://consultant.ru/popular/air/ (дата обращения 25.04.2016).

5. *Ефанов В.Н.* Открытые архитектуры в концепции авионики пятого поколения // Мир авионики. 2004. № 5. С. 20–28.

6. *Книга Е.В.* Принципы организации вычислительных систем перспективных летательных аппаратов. URL: http://elektropribor.spb.ru/cnf/kmu2013/text/63.docx (дата обращения 15.04.2016).

7. *Евгенов А.В.* Направления развития интегрированных комплексов бортового оборудования самолетов гражданской авиации // Авиакосмическое приборостроение. 2003. № 3. С. 48–53.

8. *Писаренкова Н.С., Гарбуз Г.Г.* Некоторые вопросы моделирования АСУ ПВО с применением аппарата сетей Петри // Сб. Научные труды академии. Вып. 2. Смоленск: ВА ПВО СВ РФ, 1995.

9. *Волосатова Т.М., Чичварин И.Н.* Структурное моделирование угроз информационной безопасности систем автоматизированного проектирования // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2013. № 3. С. 58–75.

10. *Розенблатт Ф.* Принципы нейродинамики: Перцептроны и теория механизмов мозга. М.: Мир, 1965. 480 с.

Глинская Елена Вячеславовна — старший преподаватель кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5).

Чичварин Николай Викторович — канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5).

Просьба ссылаться на эту статью следующим образом:

Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2016. № 6. С. 85–96. DOI: 10.18698/0236-3933-2016-6-85-96

MODELING OF INFORMATION SECURITY THREATS OF ONBOARD AIRCRAFT COMPUTING FACILITIES

E.V. Glinskaya Glinskaya-iu8@rambler.ru
N.V. Chichvarin genrih.gertz@gmail.com

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The purpose of the work was to examine and analyze computational facilities in aircraft communication and navigation complexes. In our research we aimed at constructing a formal threat model. As a result of reviewing the available literature, we conclude that the flight safety problem is growing. According to experts, due to the increase in automation level of advanced aircraft engines, airborne equipment, aircraft systems and components, as well as the growth in complexity of on-board information systems, it becomes essential to protect automated aviation technology systems from information security threats. We consider specific «avalanche» attacks which are likely to occur in modular platform computer systems

Keywords

Avionics, automated systems, security, computer systems, information, modular platform

REFERENCES

[1] Aviasafety.ru: website. Available at: http://aviasafety.ru/crash-stat (accessed 25.12.2013).

[2] Kuklev E.A., Volyn Yu.M. Ensuring security of civil aviation facilities on the basis of risk management techniques occurrence of unlawful interference. Science and Transportation. *Grazhdanskaya aviatsiya* [Civil Aviation], 2013, no. 3 (7), pp. 16–21 (in Russ.).

[3] Dokumenty IKAO. Biblioteka [IKAO documents. Library]. Airspot.ru: Aviation portal. Available at: http://airspot.ru/library/dokumenty-ikao (accessed 20.04.2016).

[4] Vozdushnyy kodeks RF ot 19.03.1997. No. 60-FZ [Air Code of the Russian Federation dated 19.03.1997. No. 60-FZ]. Konsul'tant Plyus: website. Available at: http://consultant.ru/popular/air/ (accessed 25.04.2016).

[5] Efanov V.N. Open architecture in the concept of the fifth-generation avionics. *Mir avioniki*, 2004, no. 5, pp. 20–28 (in Russ.).

[6] Kniga E.V. Printsipy organizatsii vychislitel'nykh sistem perspektivnykh letatel'nykh apparatov [Organization principles of computing perspective aircrafts systems]. Available at: http://elektropribor.spb.ru/cnf/kmu2013/text/63.docx (accessed 15.04.2016).

[7] Evgenov A.V. Development directions of integrated avionics packages for civil aviation aircraft. *Aviakosmicheskoe priborostroenie* [Aerospace Instrument-Making], 2003, no. 3, pp. 48–53 (in Russ.).

[8] Pisarenkova N.S., Garbuz G.G. Some questions of modeling automation of air defense with the apparatus of Petri nets Sb. *Nauchnye trudy akademii. Vyp. 2* [Academy transactions. Iss. 2]. Smolensk, VA PVO SV RF Publ., 1995.

[9] Volosatova T.M., Chichvarin I.N. Structural modeling of threats to information security of computer-aided design systems. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie* [Herald of the Bauman Moscow State Technical University. Ser. Instrument Engineering], 2013, no. 3, pp. 58–75 (in Russ.).

[10] Rozenblatt F. Principles of Neurodynamic: Perceptrons and the Theory of Brain Mechanisms. Washington, Spartan Books, 1962. 616 p. (Russ. ed.: Printsipy neyrodinamiki: Pertseptrony i teoriya mekhanizmov mozga. Moscow, Mir Publ., 1965. 480 p.).

Glinskaya E.V. — senior lecturer of Information Security Department, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation).

Chichvarin N.V. — Cand. Sci. (Eng.), Assoc. Professor of Information Security Department, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation).

Please cite this article in English as:

Glinskaya E.V., Chichvarin N.V. Modeling of Information Security Threats of Onboard Aircraft Computing Facilities. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2016, no. 6, pp. 85–96.
DOI: 10.18698/0236-3933-2016-6-85-96