

УДК 621.396.969.34

МЕТОДИКА АНАЛИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БОРТОВЫХ КОМПЬЮТЕРОВ ВОЗДУШНОГО СУДНА НА ОТСУТСТВИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ СИГНАТУРНО-ЭВРИСТИЧЕСКИМ СПОСОБОМ

В.И. ПЕТРОВ¹

¹*Московский государственный технический университет гражданской авиации,
г. Москва, Россия*

В статье исследуются вопросы информационной безопасности бортовых компьютеров на самолетах гражданской авиации (ГА). В информационной безопасности под недекларированными возможностями понимают возможности технических устройств или программного обеспечения, не отраженные в документации. Требования к документации и к содержанию испытаний накладываются при сертификации программного обеспечения. Требования к документации включают контроль состава и содержания документации (спецификация, описание и тексты программ, исходники). Требования к содержанию испытаний включают статический анализ исходных текстов программ (в том числе контроль соответствия исходных текстов их загрузочным модулям); динамический анализ исходных текстов программ (в том числе контроль выполнения маршрутов). В настоящее время не существует комплексных мер по проверке программного обеспечения (ПО) бортовых компьютеров самолетов. Нет нормативно-правовой базы, позволяющей контролировать ПО закупаемых самолетов зарубежного производства, а сам факт получения ПО достаточно трудоемок. Вследствие этого предлагается разработать основные положения авиационного законодательства, позволяющие проводить анализ программ бортовых компьютеров самолетов ГА. В случае отсутствия исходных текстов ПО используются два подхода анализа кода: структурный статический и динамический анализ исходного кода; сигнатурно-эвристический анализ потенциально опасных операций. Статическим анализом определяют поведение программы путем прочтения программного кода (без запуска программы), который представлен на языке ассемблера – листинга дизассемблирования. При динамическом анализе выполняется трассировка программы. В этой статье проведен анализ программного обеспечения бортовых компьютеров самолетов на обнаружение недекларированных возможностей с использованием интерактивного дизассемблера.

Ключевые слова: программное обеспечение, бортовой компьютер самолета, недекларируемые возможности, структурный статический анализ, динамический анализ, сигнатурно-эвристический анализ.

Возросшее количество авиационных происшествий в гражданской авиации требует особого внимания к причинам, которые приводят к катастрофам. При этом возможные причины авиационных катастроф и происшествий, а также их предпосылки можно разделить на три основных класса:

- отказ техники;
- влияние факторов внешней среды;
- человеческий фактор.

В статистике причин авиационных происшествий имеют место и случаи необъяснимой пропажи связи с воздушным судном, исчезновения самолета с экранов радаров и смены курса полета воздушного судна.

На сегодняшний день воздушное судно обладает развитой многоуровневой вычислительной системой, элементы которой решают разнообразные задачи в течение всего времени от взлета до посадки. К основным задачам вычислительной системы относят задачи навигации, автоматизации самолетовождения, управления работой силовыми установками, управления работой бортовых систем и устройств.

В то же время программное обеспечение бортовых компьютеров вычислительных систем самолетов зарубежного производства является неизвестным. Если предположить, что состав документации программного обеспечения зарубежного производства отвечает всем заявленным требованиям, то нельзя быть уверенным в том, что в нем отсутствуют неописанные, так называемые недекларируемые возможности.

В информационной безопасности под недекларированными возможностями понимают функциональные возможности технических устройств или программного обеспечения, не отраженные в документации, при использовании которых возможно нарушение конфиденциальности, целостности и доступности информации [1, 2].

Эта проблема рассмотрена в ряде статей [3–8]. На данный момент не существует комплексных мер по проверке программного обеспечения бортовых компьютеров воздушных судов. Нет нормативно-правовой базы, позволяющей контролировать программное обеспечение закупаемых самолетов зарубежного производства.

В связи с этим возникает задача разработки методики анализа программного обеспечения бортовых компьютеров воздушных судов, позволяющей определить отсутствие недекларируемых возможностей.

В основе методики предлагается использовать сигнатурно-эвристический метод. Суть метода заключается в разработке программы недекларируемых возможностей бортового компьютера воздушного судна, получении сигнатуры и эвристики этого программного обеспечения и поиске аналогичных сигнатур в программном обеспечении бортового компьютера реального воздушного судна.

Алгоритм недекларируемых возможностей бортового компьютера воздушного судна может иметь вид, представленный на рис. 1.

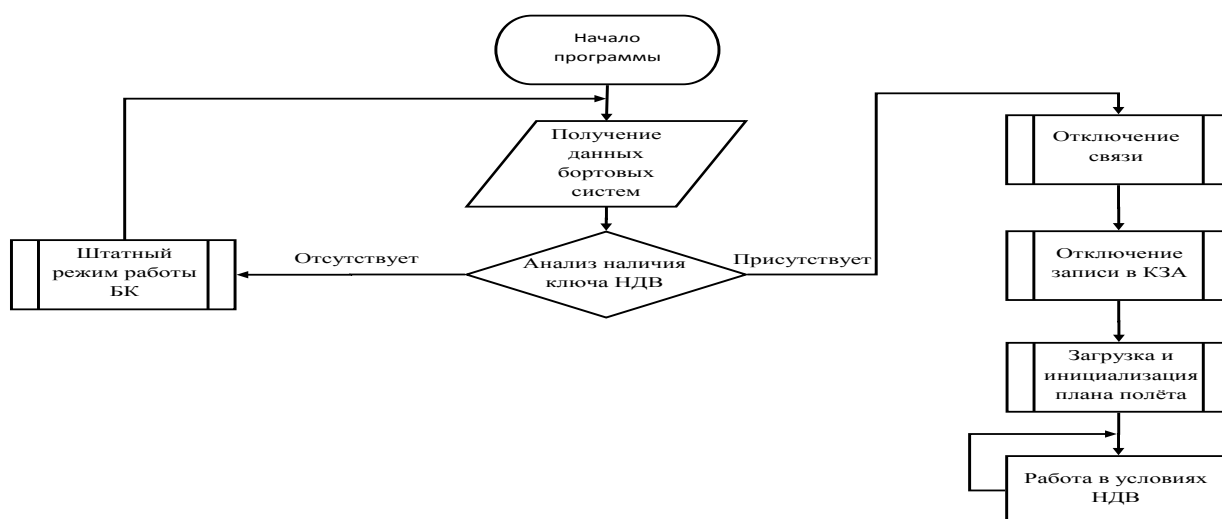


Рис. 1. Алгоритм НДВ бортового компьютера воздушного судна
Fig. 1. Algorithm of the undeclared capabilities on-board computer of air vessel

Основными действиями алгоритма НДВ бортового компьютера воздушного судна после проверки ключа НДВ являются следующие:

- отключение связи с воздушным судном;
- отключение записи параметров полета в контрольно-записывающую аппаратуру («черный ящик»);
- загрузка и инициализация нового плана полета (flight plan).

Различают два вида планов полета:

- план полета flight plan (FPL);
- повторяющийся план полета repetitive flight plan (RPL).

План полета представляет собой параметры намеченного полета воздушного судна, предоставляемые перед вылетом органу управления воздушным движением, либо загружаемые пилотом через базу планов полета.

Повторяющийся план полета применяется для выполняемых на регулярной основе многократно используемых полетов с одинаковыми основными элементами.

План полета заполняется по определенной форме в виде бланка и содержит информацию, основной из которой является:

- обозначение самолета и его тип;
- аэродром вылета и прибытия;
- крейсерская скорость и эшелон;
- маршрут полета;
- запасные аэродромы;
- запас топлива.

План полета выводится непосредственно пилоту на борт воздушного судна и перед полетом проходит проверку. Для исполнения план полета, созданный или загруженный из базы, должен быть активизирован.

В базе данных полетных планов могут быть планы полетов как подготовленные специалистами аэропорта, так и пилотами, использующими бортовые компьютеры на борту воздушного судна. На рис. 2 показана база данных полетных планов в бортовом компьютере воздушного судна.

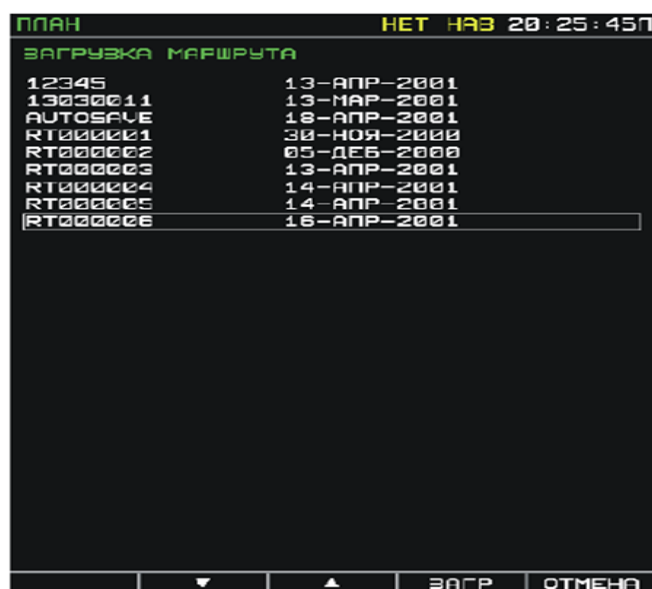


Рис. 2. База данных полетных планов

Fig. 2. The database of flight plans

На рис. 3–5 представлена пошаговая загрузка планов полета: главного и запасного. Также представлена проверка правильности загрузки планов полета и дальнейшая их инициализация. Эта операция выполняется летчиком непосредственно перед полетом.

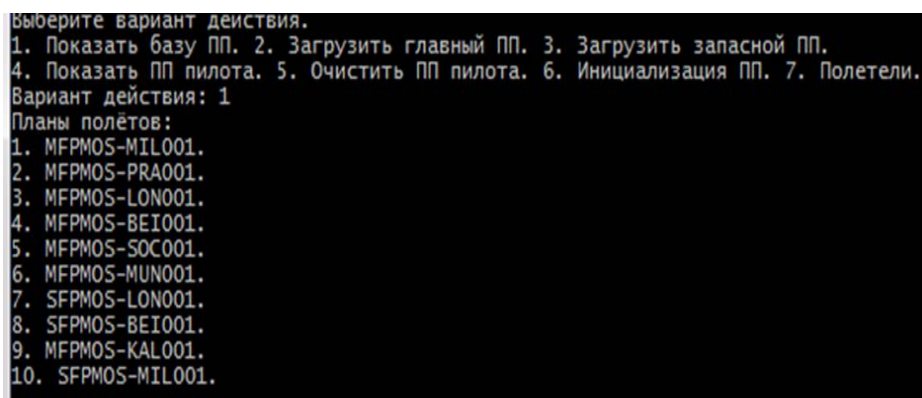


Рис. 3. База планов полета

Fig. 3. The base of the plans of flying

```
Выберите вариант действия.
1. Показать базу ПП. 2. Загрузить главный ПП. 3. Загрузить запасной ПП.
4. Показать ПП пилота. 5. Очистить ПП пилота. 6. Инициализация ПП. 7. Полетели.
Вариант действия: 4
Главный ПП:
SVO(Moscow) - LHR(London)
Date: 20.12.2016
Model: A320/S345G
SVO Airport: C 55B'58' B 37B'24'
LHR Airport: C 51B'28' B 30B'27'
Запасной ПП загружен.
```

Рис. 4. Проверка загрузки планов полета
Fig. 4. Check of loading of the plans of flying

```
Выберите вариант действия.
1. Показать базу ПП. 2. Загрузить главный ПП. 3. Загрузить запасной ПП.
4. Показать ПП пилота. 5. Очистить ПП пилота. 6. Инициализация ПП. 7. Полетели.
Вариант действия: 6
Инициализация ПП пилота прошла успешно.
```

Рис. 5. Инициализация планов полета
Fig. 5. Initialisation of the plans of flying

При использовании недекларируемых возможностей программного обеспечения бортовых компьютеров имеется возможность загрузки нового полетного плана с помощью системы ACARS во время полета воздушного судна. Инициализация полетного плана в этом случае может выполняться без участия летчика программным способом. В этом случае принудительно записывается «1» в бит ячейки памяти, отвечающей за нажатие летчиком кнопки «инициализация» в кабине воздушного судна.

В соответствии с алгоритмом НДВ бортового компьютера воздушного судна разработано программное обеспечение, которое описывает все действия по реализации НДВ на борту воздушного судна. Далее из программного обеспечения НДВ получены сигнатуры [2] по отключению связи с воздушным судном [3], отключению записи параметров полета в контрольно-записывающую аппаратуру, загрузки и инициализации нового плана полета.

Так, сигнатура загрузки и инициализации нового плана полета приведена на рис. 6.

```
bool bInitialization = false;           // инициализация ПП.
string sSettings2;                      // настройки.
string sMasPilotPlan[2];                // массив ПП пилота.
sMasPilotPlan[0] = sMasPlanov[...];
sMasPilotPlan[1] = sMasPlanov[...];
ifstream ifSettingRead("core\\settings.txt");
ifSettingRead>>sSettings2; ifSettingRead.close();

...
bInitialization = true;
while(true) // 2. Выполнение программы.
{
    ifstream ifSettingRead2("core\\settings.txt");
    ifSettingRead2>>sSettings2; ifSettingRead2.close();
    if(sSettings2 == "smenaPP=0")
    {
        ...
    }
    else if(sSettings2 == "smenaPP=1")
    {
        ...
    }
}
```

Рис. 6. Сигнатура НДВ загрузки и инициализации плана полета
Fig. 6. Signature undeclared capabilities load and initiation of Flight plan of flying

Структурно алгоритм поиска недекларируемых возможностей в программном обеспечении бортовых компьютеров воздушных судов представлен на рис. 7.

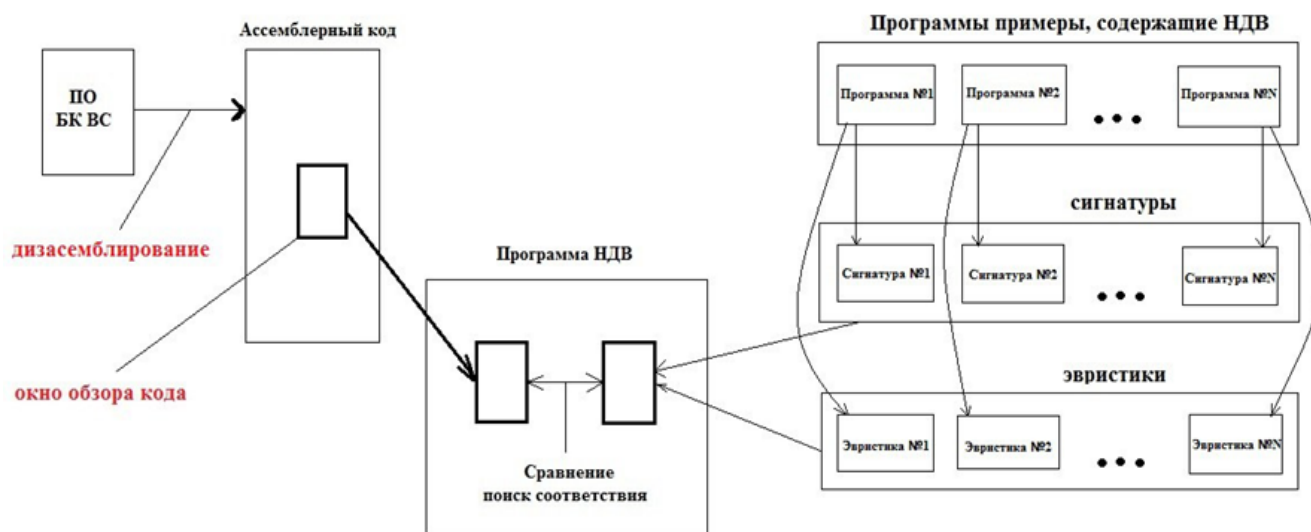


Рис. 7. Алгоритм поиска недекларируемых возможностей в программном обеспечении бортовых компьютеров воздушных судов
Fig. 7. Algorithm of search undeclared capabilities in software of on-board computers of air vessels

Для инвариантности от языка программирования, на котором написано программное обеспечение бортового компьютера, в методике анализа используется дизассемблер Ida Pro, позволяющий получить из «слепок памяти» бортового компьютера ассемблерный код. Ida Pro воспринимает максимальное количество форматов файлов и множество типов процессоров, легко справляясь с байт-кодом виртуальных машин Java и .NET, поддерживает макросы, плагины и скрипты, содержит интегрированный отладчик, работает под MS-DOS, Windows, Linux и обладает способностью распознавать имена стандартных библиотечных функций по их сигнатурам.

В последних версиях IDA Pro выполняется автоматическая распаковка файлов и снятие обфускаторов, используемых многими производителями программного обеспечения для намеренного запутывания кода в качестве дополнительной защиты.

Дизассемблер Ida Pro до определенной степени умеет автоматически выполнять анализ кода, используя перекрестные ссылки, знание параметров вызовов функций стандартных библиотек. В начале исследования дизассемблер выполняет автоматический анализ программы, а затем пользователь с помощью интерактивных средств Ida Pro может создавать сложные структуры данных и добавлять информацию в листинг, генерируемый дизассемблером, пока не станет ясно, что именно и как делает исследуемая программа.

Далее используется сигнатурно-эвристический анализ, проверяющий программное обеспечение бортового компьютера на отсутствие недекларированных возможностей. При совпадении ассемблерного кода с сигнатурой отключения связи с воздушным судном, или с сигнатурой отключения записи параметров полета в контрольно-записывающую аппаратуру, или с сигнатурой загрузки и инициализации нового плана полета, фиксируются факт присутствия в программном обеспечении бортового компьютера недекларированных возможностей и корреляция сравниваемых сигнатур с ассемблерным кодом.

Результаты исследования программного обеспечения бортовых компьютеров воздушного судна с помощью предлагаемой методики анализа программного обеспечения представлены на рис. 8.

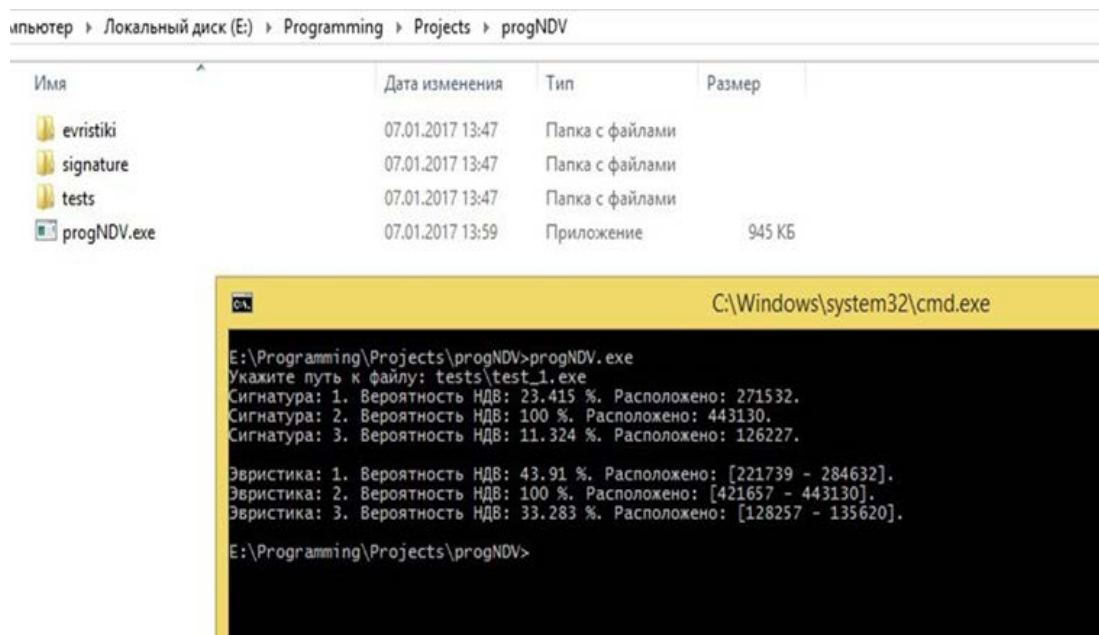


Рис. 8. Результаты исследования программного обеспечения

Fig. 8. Results of research of software

Методика анализа программного обеспечения на отсутствие недеklarированных возможностей позволяет с определенной долей вероятности определить присутствие недеklarированных возможностей в программном обеспечении бортовых компьютеров воздушных судов при реализации действий по отключению связи с воздушным судном, отключению записи параметров полета в контрольно-записывающую аппаратуру и загрузки и инициализации нового плана полета. Указано также возможное их расположение. Дальнейшее исследование найденных подозрительных участков программного обеспечения бортовых компьютеров воздушных судов можно проводить динамическим тестированием при выполнении программы.

СПИСОК ЛИТЕРАТУРЫ

1. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей // Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114. 4 с.
2. Касперски К. Компьютерные вирусы изнутри и снаружи. СПб.: Питер, 2006. 400 с.
3. Петров В.И. Недекларированные возможности программного обеспечения бортовых компьютеров воздушного судна // Гражданская авиация на современном этапе развития науки, техники и общества: сборник тезисов докладов участников Международной научно-технической конференции, посвященной 45-летию Университета. М.: ИД Академии имени Н.Е. Жуковского, 2016. С. 160.
4. Перспективный облик и технологии разработки комплексов бортового оборудования воздушных судов / Е.А. Федосов, Г.А. Чуянов, В.В. Косьянчук, Н.И. Сельвесюк // Общероссийский научно-технический журнал «Полет». 2013. № 8. С. 41–52.
5. Алгоритмическое и программное обеспечение по исследованию бортовых вычислительных устройств / Н.Я. Половинчук, А.А. Дрюков, О.В. Дорошевский, В.В. Калашников // Инновационные процессы в современном мире (Иннофорум-2016): материалы международной научно-практической конференции. М., 2016. С. 380–383.
6. Болелов Э.А. Модели выходных сигналов радионавигационных измерителей бортового комплекса применительно к условиям аномального режима их функционирования // Проблемы безопасности Российского общества. 2015. № 2. С. 44–50.

7. Кузнецов С.В. Анализ структуры современных комплексов и систем авионики воздушных судов гражданской авиации // Научный Вестник МГТУ ГА. 1998. № 3. С. 5–26.

8. Кузнецов С.В. Математические модели процессов и систем технической эксплуатации авионики как марковские и полумарковские процессы // Научный Вестник МГТУ ГА. 2015. № 213. С. 28–33.

СВЕДЕНИЯ ОБ АВТОРЕ

Петров Виктор Иванович, кандидат технических наук, доцент, декан факультета авиационных систем и комплексов, заведующий кафедрой защиты информации Московского государственного технического университета гражданской авиации, rvi-pos@mail.ru.

THE TECHNIQUE OF ANALYSIS OF SOFTWARE OF ON-BOARD COMPUTERS OF AIR VESSEL TO ABSENCE OF UNDECLARED CAPABILITIES BY SIGNATURE-HEURISTIC WAY

Viktor I. Petrov¹

¹*Moscow State Technical University
of Civil Aviation, Moscow, Russia*

ABSTRACT

The article considers the issues of civil aviation aircraft onboard computers data safety. Information security undeclared capabilities stand for technical equipment or software possibilities, which are not mentioned in the documentation. Documentation and tests content requirements are imposed during the software certification. Documentation requirements include documents composition and content of control (specification, description and program code, the source code). Test requirements include: static analysis of program codes (including the compliance of the sources with their loading modules monitoring); dynamic analysis of source code (including implementation of routes monitoring). Currently, there are no complex measures for checking onboard computer software. There are no rules and regulations that can allow controlling foreign production aircraft software, and the actual receiving of software is difficult. Consequently, the author suggests developing the basics of aviation rules and regulations, which allow to analyze the programs of CA aircraft onboard computers. If there are no software source codes the two approaches of code analysis are used: a structural static and dynamic analysis of the source code; signature-heuristic analysis of potentially dangerous operations. Static analysis determines the behavior of the program by reading the program code (without running the program) which is represented in the assembler language – disassembly listing. Program tracing is performed by the dynamic analysis. The analysis of aircraft software ability to detect undeclared capabilities using the interactive disassembler was considered in this article.

Key words: software, aircraft on-board computer, undeclared capabilities, structural static analysis, dynamic analysis, signature-heuristic analysis.

REFERENCES

1. *Zashchita ot nesanktsionirovannogo dostupa k informatsii Chast' 1. Programmnoye obespecheniye sredstv zashchity informatsii. Klassifikatsiya po urovnyu kontrolya otsutstviya nedeklarirovannykh vozmozhnostey* [Protection against unauthorized access to information Part 1. Software protection information. Classification by the level of control of absence undeclared -bath options].

Prikaz predsedatelya Gostekhkommisii Rossii [Order of the Chairman of the State Technical Commission of Russia]. June 4, 1999, № 114. 4 p. (in Russian)

2. **Kasperski K.** *Komp'yuternyye virusy iznutri i snaruzhi* [Computer viruses inside and outside]. SPb., Peter, 2006, 400 p. (in Russian)

3. **Petrov V.I.** *Nedeklarirovannyye vozmozhnosti programmnoy obespecheniya bortovykh komp'yuterv vozdukhnogo sudna* [Undeclared capabilities of software-board computers of the aircraft]. *Grazhdanskaya aviatsiya na sovremennom etape razvitiya nauki, tekhniki i obshchestva. Sbornik tezisev dokladov uchastnikov Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii, posvyashchennoy 45-letiyu Universiteta* [Civil aviation at the present stage of development of science, technology and society. Abstracts of the participants of the International scientific conference devoted to the 45th anniversary of the University]. Moscow, Academy named after N.E. Zhukovsky Publ., 2016, p. 160. (in Russian)

4. **Fedosov Ye.A., Chuyanov G.A., Kos'yanchuk V.V., Sel'vesyuk N.I.** *Perspektivnyy oblik i tekhnologii razrabotki kompleksov bortovogo oborudovaniya vozdukhnykh sudov* [Perspective image of technology and the development of systems of aircraft avionics]. *Obshcherossiyskiy nauchno-tekhnicheskii zhurnal «Polet»*. [Flight. All-Russian scientific and technical journal], 2013, № 8, pp. 41–52. (in Russian)

5. **Polovinchuk N.Y., Dryukov A.A., Doroszewska O.V., Kalashnikov V.V.** *Algoritmicheskoye i programmnoye obespecheniye po isledovaniyu bortovykh vychislitel'nykh ustroystv* [Algorithmic and the software on the researches of the onboard computing devices]. *Innovatsionnyye protsessy v sovremennom mire (Innoforum-2016). Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Innovative processes in the modern world (Innoforum 2016). Proceedings of the international scientific-practical conference]. Moscow, 2016, pp. 380–383. (in Russian)

6. **Bolelov E.A.** *Modeli vykhodnykh signalov radionavigatsionnykh izmeriteley bortovogo kompleksa primenitel'no k usloviyam anomal'nogo rezhima ikh funktsionirovaniya* [Model output signals navigation gauges avionics complex in relation to the conditions of the anomalous mode of their functioning]. *Problemy bezopasnosti Rossiyskogo obshchestva* [Security Problems of the Russian society], 2015, № 2, pp. 44–50. (in Russian)

7. **Kuznetsov S.V.** *Analiz struktury sovremennykh kompleksov i sistem avioniki vozdukhnykh sudov grazhdanskoy aviatsii* [Analysis of the structure of modern avionics systems and complexes of civil aircrafts]. *Nauchnyy Vestnik MGTU GA* [Scientific Bulletin of the MSTUCA], 1998, no. 3, pp. 5–26. (in Russian)

8. **Kuznetsov S.V.** *Matematicheskiye modeli protsessov i sistem tekhnicheskoy ekspluatatsii avioniki kak markovskiy i polumarkovskiy protsessy* [Mathematical models of processes and systems of avionic technical operation as Markov and Semimarkov processes]. *Nauchnyy Vestnik MGTU GA* [Scientific Bulletin of the MSTUCA], 2015, no. 213, pp. 28–33. (in Russian)

INFORMATION ABOUT THE AUTHOR

Petrov Viktor Ivanovich, PhD, Associate Professor, Dean of the Faculty of Aviation Systems and Complexes, Head of Chair of Information Security of the Moscow State University of Civil Aviation, pvi-pos@mail.ru.