УДК 004.414.2
DOI: 10.26467/2079-0619-2017-20-6-99-110

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МОБИЛЬНЫХ МОДУЛЬНЫХ ИЗМЕРИТЕЛЬНЫХ КОМПЛЕКСАХ

А.Н. ТХИШЕВ[1], П.С. ГОРШКОВ[2], А.П. ГОЛОВКИН[3]
[1]ООО «РУБИНТЕХ», г. Москва, Россия
[2]ООО «Экспериментальная мастерская НаукаСофт», г. Москва, Россия
[3]Испытательный центр (Морской) ГЛИЦ МО РФ имени В.П.Чкалова, г. Феодосия, Россия

Особенностью испытаний образцов авиационной техники является проведение как летной оценки, так и наземной эксплуатационной оценки в составе аэродромных средств подготовки и обеспечения полетов, специальных средств снаряжения. Специфика проведения летно-морских испытаний подразумевает выполнение измерений в морской акватории, что исключает возможность использования стационарных, геодезически привязанных измерительных средств. В связи с этим особую роль приобретают измерительные комплексы корабельного базирования, в частности – мобильные модульные измерительные комплексы.

Информация, обрабатываемая в мобильных модульных измерительных комплексах, является критическим ресурсом, имеющим высокий уровень конфиденциальности. При выполнении ими своих функций следует осуществлять надлежащее управление информацией для обеспечения ее защиты от опасностей нежелательного распространения, изменения или потери, т. е. обеспечить определенный уровень информационной безопасности.

Решение проблем информационной безопасности в такого рода комплексах сопряжено с трудностями, обусловленными спецификой их применения. Модель нарушителя, модель угроз, требования безопасности, сформированные для стационарно расположенных объектов информатизации, не применимы для мобильных комплексов. В статье обоснован вывод, что перспективные мобильные модульные измерительные комплексы, предназначенные для мониторинга и управления летными экспериментами, должны создаваться с учетом необходимых мер и средств защиты информации. В статье приводится схема формирования требований безопасности, начиная с анализа среды функционирования и заканчивая практической реализацией. Разработана вероятностная модель информационной безопасности применительно для мобильных модульных измерительных комплексов. Рассматривается перечень актуальных угроз безопасности с учетом среды и особенностей функционирования мобильного измерительного комплекса. Приводится вероятностная модель оценки защищенности информации. Рассматриваются вопросы трансформации уязвимостей проектируемой информационной системы в цели безопасности с последующим формированием перечня необходимых функциональных требований и требований доверия.

Ключевые слова: мобильный модульный измерительный комплекс, летный эксперимент, проектирование информационных систем, информационная безопасность, угрозы безопасности, требования безопасности, требования доверия.

ВВЕДЕНИЕ

Этап испытаний является одним из основных этапов жизненного цикла (ЖЦ) авиационных изделий и представляет собой комплекс работ, проводимых в процессе создания, производства и эксплуатации летательного аппарата и его составных частей с целью проверки их работоспособности, выявления и устранения недостатков, проверки соответствия фактических характеристик расчетным данным и установленным требованиям и подтверждения заданного уровня надежности.

Особенностью испытаний образцов авиационной техники (ОАТ) является проведение как летной оценки, так и наземной эксплуатационной оценки в составе аэродромных средств подготовки и обеспечения полетов, специальных средств снаряжения и вооружения. При этом основной оценкой качества авиационной техники является летный эксперимент (ЛЭ).

Этап испытаний ОАТ реализуется организационно-техническими системами (ОТС) – испытательными центрами (ИЦ). Это, прежде всего, Летно-исследовательский институт имени М.М. Громова и Государственный летно-испытательный центр Министерства обороны имени В.П. Чкалова, которые включают в свой состав различные полигоны, измерительные комплек-

сы и системы, летательные аппараты, корабли, комплексы обеспечения безопасности и управления полетами, пункты и лаборатории обработки информации и многие другие элементы [0].

Подавляющее большинство современных и перспективных авиационных комплексов в соответствии с тактико-техническим заданием (ТТЗ) подразумевают использование в различных географических и климатических условиях: на равнине, в горах, на море. Все это определяет необходимость, характер и требования к экспериментально-испытательной базе (ЭИБ) испытаний авиационной техники.

В качестве примера рассмотрим состав ЭИБ, используемой при проведении летно-морских испытаний. Исходя из анализа отечественного и зарубежного опыта, полигон испытаний ОАТ в морских условиях представляет собой сложную ОТС, включающую в себя:

- обширную номенклатуру бортовой контрольно-измерительной аппаратуры для летных испытаний ОАТ;
- воздушные, надводные и наземные мишени с разными вариантами дооснащения аппаратурой;
- стационарные и передвижные средства траекторных измерений (ТИ) и следящие системы;
- средства обеспечения телеметрии в режиме реального времени;
- имитаторы средств нападения противника;
- средства измерения эффективной поверхности рассеяния;
- мобильные системы ТИ для обеспечения измерений над морской акваторией;
- систему подводных ТИ;
- систему измерений, размещаемых на борту авианесущих кораблей (АНК) на период проведения летных испытаний.

Создание подобного морского ИЦ сопряжено с большими временными и материальными затратами. Кроме того, сама специфика испытаний подразумевает выполнение измерений в морской акватории, что исключает возможность использования стационарных, геодезически привязанных измерительных средств. В связи с этим особую роль приобретают измерительные комплексы корабельного базирования, в частности – мобильные модульные измерительные комплексы.

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В МОБИЛЬНЫХ МОДУЛЬНЫХ ИЗМЕРИТЕЛЬНЫХ КОМПЛЕКСАХ

Информация, обрабатываемая в ИЦ, в том числе и в мобильных измерительных комплексах, является критическим ресурсом, имеющим высокий уровень конфиденциальности. При выполнении мобильными измерительными комплексами своих функций следует осуществлять надлежащее управление информацией для обеспечения ее защиты от опасностей нежелательного распространения, изменения или потери, т. е. обеспечить определенный уровень информационной безопасности.

Информационная безопасность достигается путем реализации соответствующего комплекса мер и средств обеспечения безопасности, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств [0]. Указанные меры и средства обеспечения безопасности необходимо создавать, реализовывать, подвергать мониторингу, модернизировать, если необходимо, для обеспечения требуемого уровня безопасности. Таким образом, понятие безопасности применимо ко всем этапам жизненного цикла мобильного измерительного комплекса, начиная с этапа постановки задачи на проектирование.

При проектировании многих информационных систем проблемы безопасности не учитываются или сводятся к выбору определенных технических средств. Уровень безопасности,

который может быть достигнут техническими средствами, имеет ряд ограничений и не всегда отвечает условиям использования разрабатываемой информационной системы. Так, определение перечня технических средств только на основании уровня конфиденциальности обрабатываемой информации не отражает особенностей использования мобильных комплексов. К таким особенностям могут относиться:

- использование мобильных комплексов вне защищенных помещений;
- широкий, в некоторых случаях неопределенный, круг лиц, который потенциально может получить доступ к мобильному комплексу;
- повышенные риски утери (кражи) при использовании, транспортировке и хранении;
- отсутствие оперативной реакции должностных лиц, отвечающих за информационную безопасность, на попытки несанкционированного доступа, модификации уничтожения;
- использование различных по типу и составу датчиков и каналов коммутации с мобильным измерительным комплексом.
- большие объемы первичных результатов измерений, которые затрудняют использование криптографических средств защиты информации.

Использование мобильного комплекса вне защищенных помещений подразумевает особый режим обработки информации, связанный с риском утечки конфиденциальной информации по техническим каналам.

Определение круга лиц, который потенциально может получить доступ к вычислительному комплексу, лежит в основе построения модели нарушителя. В случае мобильного измерительного комплекса этот круг лиц может быть довольно обширен. Так, при использовании мобильного комплекса на борту АНК, перечень лиц, которые потенциально могут получить доступ к мобильному комплексу, измеряется сотнями человек.

В отличие от стационарных комплексов, использование которых предполагается в составе охраняемых объектов, мобильные комплексы подразумевают транспортировку к местам проведения испытаний. Наличие рисков утери (кражи) мобильного комплекса при транспортировке и эксплуатации накладывает требования как административного, так и технического характера. Например, шифрования всей информации, содержащейся в мобильном измерительном комплексе, или хранения защищаемой информации на отчуждаемом носителе в преобразованном виде.

Использование вычислительных комплексов в составе защищенных информационных систем подразумевает наличие службы информационной безопасности, в задачи которой входит оперативная реакция на инциденты информационной безопасности. Применение мобильных измерительных комплексов подразумевает обработку конфиденциальных данных вне защищенной информационной системы. В связи с этим к системе предъявляются повышенные требования по протоколированию событий информационной безопасности. Например, наличие механизмов теневого копирования выдаваемых на печать документов или сохранения копии всей информации, записываемой на внешние носители.

Использование мобильных комплексов подразумевает их оперативное развертывание, при этом номенклатура измерительных датчиков и их размещение может изменяться в зависимости от характера испытаний ОАТ. Наличие кабельных, а в некоторых случаях и беспроводных систем, накладывает определенные ограничения на процесс передачи данных между мобильным комплексом и измерительными датчиками, связанные с режимом преобразования информации, защитой канала связи и т. д. Интеграция мобильного измерительного комплекса в единое информационное пространство (ЕИП) подразумевает применение механизмов межсетевого экранирования, обнаружения вторжений и анализа уязвимостей.

Наличие в составе мобильного измерительного комплекса оптических датчиков высокого разрешения повлечет за собой накопление большого объема данных, для защиты которых затруднительно применение криптографических средств, что необходимо учитывать при фор-

мировании требований к хранению, копированию, преобразованию и затиранию конфиденциальной информации.

Рассмотрим модель основных подсистем технической инфраструктуры (современной и перспективной) систем измерений и оценки значений физических величин, параметров и характеристик ОАТ, используемых в ходе и в результате ЛЭ [0]. Ее можно представить в виде трех функциональных блоков (рис. 1):

1) формирование цифровых значений $Y(t)$ аналоговых и цифровых сигналов от различных типов бортовых и наземных технических средств измерения (приборов) – уровень (интерфейс) аналогово-цифровых преобразований (ИАЦП) или *первичной* обработки измерений;

2) формирование значений оценок измеряемых физических величин и параметров $\mathrm{X}(t)$ объекта испытания (эксперимента) на основе полученных значений измерений – уровень (интерфейс) формирования обновляемых данных (ИОД) или *вторичной* обработки измерений (получение значений оценок, например: скорости, курса, тангажа, крена, координат, силы ветра и т. п.);

3) накопление и обработка данных с целью мониторинга процессов летного эксперимента и управления его ходом, а также формирование оценочных значений требуемых (-ой) характеристик (-и) на основе одного или множества экспериментов – уровень аналитической (*третичной*) обработки данных.

Рис. 1. Модель системы сбора и обработки данных ЛЭ
Fig. 1. The model system of storage and processing a flight experiment data

Представленные функциональные блоки объединяются с помощью системы связи и обмена данными (ССОД) в единую систему, формирующую информационное пространство ИЦ в виде данных измерений и оценок, выполненных в ходе различных ЛЭ.

В зависимости от вида, структуры и содержания информационных потоков через ИАЦП и ИОД технологическая реализация ССОД может объединять в одном конструктивном элементе функции подсистем 1-го и 2-го уровней, либо 2-го и 3-го уровней, либо сохранять их конструктивную автономность, обеспечивая при этом автоматический или автоматизированный режим обмена данными (рис. 2).

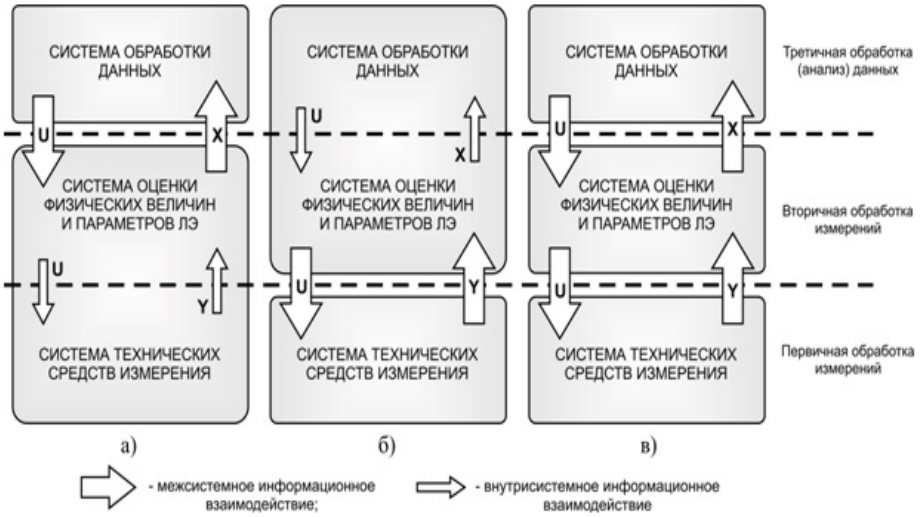

Рис. 2. Возможные схемы технологической реализации АСУ ЛЭ
Fig. 2. Possible schemes of technological realization for automatic control systems in a flight experiment

Приведенные модель и схемы показывают все типы информационного взаимодействия при проведении летного эксперимента, но не отражают особенностей использования технических комплексов, влияющих на управление информацией для обеспечения ее защиты от опасностей нежелательного распространения, изменения или потери.

Таким образом, перспективные мобильные модульные измерительные комплексы, предназначенные для мониторинга и управления летными экспериментами и соответствующие сформулированным выше требованиям (обладающие рассмотренными свойствами), должны создаваться с учетом необходимых мер и средств защиты информации.

Возможный способ последовательного формирования требований безопасности при разработке мобильного измерительного комплекса представлен на рис. 3.

Среда безопасности определяет условия предполагаемого применения мобильного комплекса. Среда безопасности включает также угрозы безопасности, присутствие которых в этой среде установлено или предполагается с учетом условий использования мобильного комплекса. При анализе среды безопасности необходимо принять во внимание:

- физическую среду в той ее части, которая определяет все аспекты эксплуатации мобильного комплекса, касающиеся его безопасности, включая мероприятия, относящиеся к физической защите и персоналу;
- активы, которые требуют защиты элементами мобильного комплекса и к которым применяются требования или политики безопасности;
- предназначение и предполагаемую сферу применения мобильного комплекса.

Рис. 3. Формирование требований безопасности
Fig. 3. Software requirements

Анализ особенностей функционирования, угроз и рисков позволяет сформулировать предположения, которым удовлетворяла бы среда функционирования мобильного комплекса для того, чтобы считаться безопасной, и перечень угроз безопасности. В ГОСТ Р ИСО/МЭК 15408 угрозы раскрываются через понятия источника угрозы, предполагаемого метода нападения, любых уязвимостей, которые являются предпосылкой для нападения, и идентификации активов, являющихся целью нападения. При оценке рисков безопасности квалифицируют каждую угрозу безопасности с оценкой возможности ее перерастания в фактическое нападение, вероятности успешного проведения такого нападения и последствий любого возможного ущерба. С точки зрения способов реализации угроз угрозы можно разделить на три группы: угрозы специальных воздействий, угрозы несанкционированного доступа (НСД) и угрозы утечки информации по техническим каналам [0]. Перечень актуальных для мобильного модульного измерительного комплекса угроз зависит от его конфигурации и условий применения. Примерный перечень актуальных угроз представлен в табл. 1.

Таблица 1
Table 1

Угрозы безопасности мобильного модульного измерительного комплекса
Security threats of a mobile modular measuring system

Название угрозы	**Возможные последствия**
Угрозы специальных воздействий	
Угрозы утери (хищения) мобильного комплекса	Нарушение конфиденциальности, целостности, доступности информации
Угрозы утери (хищения) носителей информации	Нарушение конфиденциальности, целостности, доступности информации
Угрозы механического, химического, термического, электромагнитного воздействия	Нарушение целостности и доступности информации
Угрозы несанкционированного доступа	
Угрозы, направленные на перехват паролей или идентификаторов	Нарушение конфиденциальности, целостности, доступности информации
Угрозы, направленные на модификацию базовой системы ввода/вывода (BIOS)	Нарушение конфиденциальности, целостности, доступности информации. Обход механизмов доверенной загрузки
Угрозы, направленные на перехват управления загрузкой	Нарушение конфиденциальности, целостности, доступности информации
Угрозы, направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы	Нарушение конфиденциальности, целостности, доступности информации
Угрозы внедрения вредоносных программ	Нарушение конфиденциальности, целостности, доступности информации. Скрытое управление системой
Угрозы «Анализа сетевого трафика»	Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
Угрозы внедрения ложного объекта сети	Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений

Продолжение таблицы 1

Угрозы типа «Отказ в обслуживании»	Снижение пропускной способности каналов связи, производительности сетевых устройств. Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения
Угрозы удаленного запуска приложений	Нарушение конфиденциальности, целостности, доступности информации
Угрозы утечки информации по техническим каналам	
Угрозы утечки акустической (речевой) информации	Нарушение конфиденциальности информации
Угрозы утечки видовой (визуальной) информации	Нарушение конфиденциальности информации
Угрозы утечки информации по каналу ПЭМИН	Нарушение конфиденциальности информации

Исходной посылкой при разработке моделей информационной безопасности является предположение: с одной стороны, при нарушении защищенности информации наносится некоторый ущерб, с другой – обеспечение защиты информации сопряжено с расходованием средств [5]. Таким образом, задача построения системы защиты является оптимизационной задачей: при заданных ресурсах достигнуть максимального результата или обеспечить достижение заданного результата при минимальном расходовании ресурсов.

В рассматриваемом случае, общую модель безопасности можно представить в виде рис. 4. В соответствии с данной моделью обработка информации осуществляется в условиях воздействия на информацию угроз (дестабилизирующих факторов). Для противодействия угрозам информации могут использоваться специальные средства защиты, оказывающие нейтрализующее воздействие на дестабилизирующие факторы. При этом характер и уровень воздействия одних факторов не зависит от характера и уровня воздействия других. Однако могут быть и взаимозависимые факторы, характер и уровень воздействия которых существенно зависит от влияния других. Точно так же и средства защиты могут быть как независимыми с точки зрения эффективности защиты, так и взаимозависимыми. Таким образом, при разработке моделей процессов защиты информации надо учитывать не только воздействие дестабилизирующих факторов и средств защиты, но также и взаимное воздействие факторов и средств друг на друга [0].

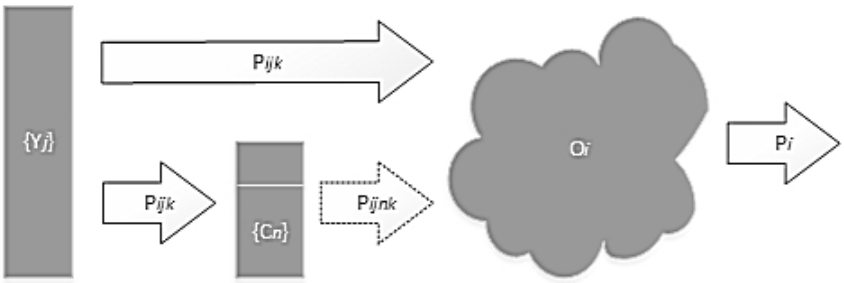

Рис. 4. Общая модель процесса защиты информации
Fig. 4. The general model of information security process

$\{Y_j\}$ – *j-я* угроза воздействия на объект защиты.
O_i – *i-й* объект защиты.
$\{C_n\}$ – *n-е* средство защиты информации.
$\{P_{ijk}\}$ – вероятность негативного воздействия *j-й* угрозы на *i-й* объект в *k-м* его состоянии.
$\{P_{ijnk}\}$ – вероятность негативного воздействия *j-й* угрозы на *i-й* объект в *k-м* его состоянии с учетом применения *n-го* средства защиты.
$\{P_i\}$ – вероятность надежной защиты *i-го* объекта.

С учетом приведенных обозначений, можно вывести следующие зависимости:

$$P_{\text{i}} = \prod_{\forall k}(1 - P_{ik}) \cdot \alpha_k$$

Здесь *k* есть доля *k-го* состояния (режима работы) в анализируемый период времени. Для мобильного измерительного комплекса такими состояниями могут быть: хранение, транспортировка, использование в процессе ЛЭ и т. д. Наиболее объективным будет представление его в виде доли интервала времени пребывания системы в *k-м* состоянии. Таким образом, значение α_k можно представить в виде отношения доли временного интервала пребывания системы в *k-м* состоянии к общей продолжительности оцениваемого интервала времени:

$$\alpha_k = \frac{\Delta t_k}{\Delta T}.$$

При построении модели системы защиты будем используют так называемые модели с полным перекрытием. В данных моделях в качестве исходной берется посылка, что любой угрозе должно соответствовать хотя бы одно средство защиты информации. Однако в общем случае в системе могут отсутствовать системы защиты от некоторых дестабилизирующих факторов. Тогда

$$P_i = P_{ik}^{`} + P_{ik}^{``},$$

где $P_{ik}^{`}$– вероятность защищенности информации на *i-м* объекте в *k-м* его состоянии от совокупного воздействия всех тех угроз, для противодействия которым в системе защиты информации не предусмотрены средства зашиты:

$$P_{ik}^{`} = \prod_{\forall j`}(1 - P_{ijk});$$

$j`$ – принимает значение тех номеров угроз, для противодействия которым в системе не предусмотрены средства защиты. В свою очередь:

$$P_{ik}^{``} = \prod_{\forall \eta``}\prod_{\forall j``}(1 - \text{P}_{ijk\eta});$$

$j``$ – принимает значение тех номеров угроз, для противодействия которым в системе предусмотрены средства защиты, а $\eta``$ – значения номеров тех средств защиты информации, которые оказывают воздействие на угрозу с номером $j``$.

Вероятность защиты информации в группе объектов определяется зависимостью

$$P = \prod_{\forall i} P_i.$$

Исходя из рассмотренного подхода, предполагаемый ущерб U может составить

$$\text{U} = (1 - \text{P}) \cdot \text{G},$$

где G – оценочный коэффициент, который может быть выражен в денежном эквиваленте. Возможный ущерб может быть оценен как для системы в целом, так и для отдельной угрозы. Ре-

шение проблемы оценки возможного ущерба при нарушении защищенности информации сопряжено с некоторыми трудностями. В частности, корректно оценить ущерб в денежном выражении возможно только для коммерческой, промышленной или другой подобной тайны, хотя и в этом случае вероятны весьма большие трудности. Оценить ущерб при нарушении государственной тайны или при несанкционированном доступе к персональным данным еще сложнее. Аналогичная ситуация и с вероятностью возникновения угрозы. Для некоторых типов угроз существуют статистические данные об их проявлении и последствиях, но для большого количества угроз, таких как угрозы утечки по акустическому каналу или угрозы выявления пароля и подобных, трудно оценить вероятность проявления угрозы. Однако это не означает, что данная модель не может быть использована для построения системы защиты информации. Значения вероятности возникновения отдельных угроз и возможного ущерба могут быть получены экспертным путем с учетом методов автоформализации знаний. При этом важное значение приобретает оценка достоверности данных, опираясь на которые эксперт-аналитик принимает то или иное решение [0].

Результаты анализа используются для установления целей безопасности, которые направлены на противостояние установленным угрозам. Цели безопасности должны быть согласованы с установленными целями применения или предназначением мобильного комплекса как программно-аппаратного измерительного комплекса, а также со всеми известными сведениями о физической среде функционирования.

Смысл определения целей безопасности заключается в том, чтобы соотнести их со всеми поставленными ранее вопросами безопасности и декларировать, какие аспекты безопасности связаны непосредственно с мобильным комплексом, а какие – с его средой функционирования.

Цели безопасности для среды функционирования мобильного измерительного комплекса достигаются как в рамках использования программно-аппаратных средств защиты, так и нетехническими или административными способами.

Требования безопасности являются результатом преобразования целей безопасности в совокупность требований безопасности для самого мобильного комплекса и отдельно для среды функционирования. В ИСО/МЭК 15408 представлены две различные категории требований безопасности – функциональные требования и требования доверия [0].

Функциональные требования предъявляются к тем функциям аппаратно-программного комплекса, которые предназначены для поддержания его безопасности и определяют желательный безопасный режим функционирования. Функциональные требования определены в ИСО/МЭК 15408-2. Примерами функциональных требований являются требования к идентификации-аутентификации, разграничению доступа, аудиту безопасности и т. д.

В отличие от функциональных требований, требования доверия предъявляются не к определенным функциям разрабатываемого комплекса, а к действиям разработчика. Таким образом, требования доверия определяют степень доверия к реализации заданных функциональных требований. Степень доверия может меняться и, как правило, выражается через возрастание уровня строгости, задаваемого компонентами доверия. ИСО/МЭК 15408-3 определяет требования доверия и шкалу оценочных уровней доверия (ОУД), формируемых с использованием этих компонентов. Примерами требований доверия являются требования к организации процесса разработки, поиску потенциальных уязвимостей и анализу их влияния на безопасность.

Доверие к тому, что цели безопасности достигаются посредством выбранных функций безопасности, зависит от уверенности:

- в корректности реализации функций безопасности, то есть оценки того, правильно ли они реализованы;
- в эффективности функций безопасности, то есть оценки того, действительно ли они отвечают изложенным целям безопасности.

Спецификация определяет отображение требований безопасности для разрабатываемого мобильного комплекса. В ней обеспечивается высокоуровневое определение функций безопас-

ности, заявляемых для удовлетворения функциональных требований и мер доверия, предпринимаемых для удовлетворения требований доверия.

ЗАКЛЮЧЕНИЕ

Рассмотренный в статье подход описывает общий порядок проектирования перспективных мобильных модульных измерительных комплексов в контексте обеспечения информационной безопасности. Последовательный переход от анализа среды функционирования к формированию списка актуальных угроз позволяет сформулировать цели обеспечения безопасности и сформировать достаточный и непротиворечивый перечень необходимых функциональных требований и требований доверия. Формирование перечня необходимых требований с учетом особенностей функционирования мобильного измерительного комплекса является нетривиальной задачей, для решения которой целесообразно использовать системы поддержки принятия решений.

Реализацией мобильного комплекса является его воплощение, основанное на функциональных требованиях безопасности и спецификации комплекса, содержащейся в задании по безопасности (ЗБ). Разрабатываемый комплекс будет отвечать целям безопасности, если он правильно и эффективно реализует все требования безопасности, содержащиеся в ЗБ.

СПИСОК ЛИТЕРАТУРЫ

1. Всероссийская научно-техническая конференция «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского»: сборник докладов. М.: Издательский дом Академии имени Н.Е. Жуковского, 2015. 552 с.

2. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М.: Стандартинформ, 2014. 3 с.

3. Ветошкин В.М., Горшков П.С., Жолобов А.Б. Методологические проблемы и пути создания автоматизированной системы управления испытаниями авиационной техники // Научный Вестник МГТУ ГА. 2017. Том 20, № 01. С. 159–166.

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008. 14 с.

5. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МИФИ, 1997. С. 95, 161.

6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком, 2004. 105 с.

7. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М.: Стандартинформ, 2014.

8. Горшков П.С. Ресурсно-ограничительный метод исследования сложных информационных систем / П.С. Горшков, Б.И. Бачкало // Труды симпозиума «Надежность и качество». М., 2008. С. 274–277.

9. Ветошкин В.М. Основы теории концептуального проектирования баз данных для автоматизированных систем / В.М. Ветошкин. М.: ВВИА им. проф. Н.Е. Жуковского, 1992. 267 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Тхишев Александр Николаевич, ведущий сотрудник ООО «РУБИНТЕХ», tan@rubinteh.ru.

Горшков Павел Сергеевич, кандидат технических наук, доцент, исполнительный директор ООО «Экспериментальная мастерская НаукаСофт», pgorshkov@xlab-ns.ru.

Головкин Алексей Петрович, начальник управления ИЦ (Морского) Государственного летно-испытательного центра Министерства обороны имени В.П. Чкалова, headman69@rambler.ru.

INFORMATION SECURITY IN MOBILE MODULAR MEASURING SYSTEMS

Alexander N. Tkhishev[1], Pavel S. Gorshkov[2], Alexey P. Golovkin[3]
[1]LLC "RUBINTECH", Moscow, Russia
[2]LLC "Experimental Laboratory NaukaSoft", Moscow, Russia
[3]Chkalov State Flight Test Center (Maritime) GLIC, the Russian Federation, Feodosia, Russia

ABSTRACT

A special aspect of aircraft test is carrying out both flight evaluation and ground operation evaluation in a structure of flying aids and special tools equipment. The specific of flight and sea tests involve metering in offshore zone, which excludes the possibility of fixed geodetically related measuring tools. In this regard, the specific role is acquired by ship-based measurement systems, in particular the mobile modular measuring systems.

Information processed in the mobile modular measurement systems is a critical resource having a high level of confidentiality. When carrying out their functions, it should be implemented a proper information control of the mobile modular measurement systems to ensure their protection from the risk of data leakage, modification or loss, i.e. to ensure a certain level of information security.

Due to the specific of their application it is difficult to solve the problems of information security in such complexes. The intruder model, the threat model, the security requirements generated for fixed informatization objects are not applicable to mobile systems.

It was concluded that the advanced mobile modular measuring systems designed for flight experiments monitoring and control should be created due to necessary information protection measures and means. The article contains a diagram of security requirements formation, starting with the data envelopment analysis and ending with the practical implementation. The information security probabilistic model applied to mobile modular measurement systems is developed. The list of current security threats based on the environment and specific of the mobile measurement system functioning is examined. The probabilistic model of the information security evaluation is given. The problems of vulnerabilities transformation of designed information system into the security targets with the subsequent formation of the functional and trust requirements list are examined.

Key words: mobile modular measuring system, flight experiment, information systems design, information security, security threats, security requirements, trust requirements.

REFERENCES

1. *Vserossijskaja nauchno-tehnicheskaja konferencija «Nauchnye chtenija po aviacii, posvjashhjonnye pamjati N.E. Zhukovskogo». Sbornik dokladov 2015* [All-Russian scientific and technical conference "Scientific readings on aviation dedicated to the memory of N.E. Zhukovsky". A collection of reports 2015]. M., Zhukovsky Air Force Academy Publishing house, 2015. 552 p. (in Russian)

2. GOST P ISO/IEC 27002:2012 "Information technology – Security techniques – The code of practice for information security management". M., Standartinform, 2014, 3 p.

3. Vetoshkin V.M., **Gorshkov P.S.**, **Zholobov A.B.** *Metodologicheskie problemy i puti sozdanija avtomatizirovannoj sistemy upravlenija ispytanijami aviacionnoj tehniki* [Methodological problems and ways of creation of the aircraft equipment test automated control system]. Scientific Bulletin of MSTUCA, 2017, Vol. 20, no. 01, pp. 159–166. (in Russian)

4. *Bazovaja model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh* [The basic model of personal data security threats while processing in personal data information systems]. FSTEK Russia, 2008. 14 p. (in Russian)

5. Gerasimenko V.A., **Malyuk A.A.** *Osnovy zashhity informacii* [The basics of information security]. M., MEPhI, 1997, pp. 95, 161. (in Russian)

6. Malyuk A.A. *Informacionnaja bezopasnost': konceptual'nye i metodologicheskie osnovy zashhity informacii* [Information security: conceptual and methodological foundations of information security]. M., Hot line – Telecom, 2004, 105 p. (in Russian)

7. GOST P ISO/IEC 15408-1-2012. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and a general model. M., Standartinform, 2014.

8. Gorshkov P.S. *Resursno-ogranichitel'nyj metod issledovanija slozhnyh informacionnyh sistem* [Resource-restrictive method for the study of complex information systems]. Gorshkov P.S., Bachkalo B.I. M., Proceedings of the Symposium on Reliability and Quality, 2008, pp. 274–277. (in Russian)

9. Vetoshkin V.M. *Osnovy teorii konceptual'nogo proektirovanija baz dannyh dlja avtomatizirovannyh sistem* [Theory fundamentals of database conceptual design for the automated systems]. V.M. Vetoshkin. M., Zhukovsky Air Force Engineering Academy, 1992, 267 p. (in Russian)

INFORMATION ABOUT THE AUTHORS

Alexander N. Tkhishev, LLC "RUBINTECH", Leading Expert, tan@rubinteh.ru.

Pavel S. Gorshkov, Candidate of Technical Sciences, Associate Professor, Executive Director, LLC "Experimental laboratory NaukaSoft", pgorshkov@xlab-ns.ru.

Alexey P. Golovkin, Head of Department, Chkalov State Flight Test Center (Maritime) (GLIC), the Russian Federation, headman69@rambler.ru.

Поступила в редакцию	17.10.2017	Received	17.10.2017
Принята в печать	23.11.2017	Accepted for publication	23.11.2017