Информационная безопасность АСУ
на основе авиационных стандартов

Александр БУРЦЕВ,
директор департамента АСУ,
НТЦ «Станкоинформзащита»

При разработке авиационных автоматизированных систем управления (АСУ) в Европе и США на первое место ставятся надежность и безотказность работы. Повышение информационной безопасности таких систем является следствием возрастания общей безопасности и надежности. Немалую роль в этом играют рекомендации и требования к процессам разработки АСУ. В настоящей статье рассказывается о нескольких стандартах/рекомендациях к АСУ и процессу их разработки, применяемых в Европе и США. В целом требования, предъявляемые к процессам разработки АСУ в авиационной отрасли, нацелены на снижение угроз жизни и здоровью человека, поэтому целесообразно рассмотреть их в контексте требований, предъявляемых к объектам критически важных инфраструктур.

Стандарт DO-178B/C

Применяемый в авиационной промышленности стандарт DO-178B/C Software Considerations in Airborne Systems and Equipment Certification – скорее набор рекомендаций (требований) к процессу разработки и документированию программного обеспечения. Стандарт DO-178B был разработан и утвержден RTCA 1 декабря 1992 г. В январе 2012 г. был утвержден обновленный документ DO-178C, являющийся развитием DO-178B.

В DO-178B/C представлены рекомендации к построению основных этапов жизненного цикла программного продукта – планированию, разработке, верификации, обеспечению качества (рис. 1).

Для дифференциации требований к ПО и процессу разработки стандарт вводит пять уровней критичности отказов ПО в зависимости от последствий отказа:

- уровень A: отказ ПО может привести к невозможности безопасного завершения полета;
- уровень B: отказ ПО может привести к существенному снижению эксплуатационных характеристик самолета и к жертвам среди пассажиров;
- уровень C: отказ ПО может привести к существенному снижению эксплуатационных характеристик самолета и травмам либо значительному уменьшению комфорта для пассажиров;
- уровень D: отказ ПО может привести к незначительному снижению эксплуатационных характеристик самолета или создать неудобства для пассажиров;
- уровень E: отказ ПО не приводит к ухудшению эксплуатационных характеристик самолета.

На этапе планирования стандарт DO-178B/C рекомендует определить:

- основные процедуры процесса разработки, обеспечивающие выполнение требований к разрабатываемой системе;
- особенности жизненного цикла программного обеспечения;
- инструментарий разработки ПО;

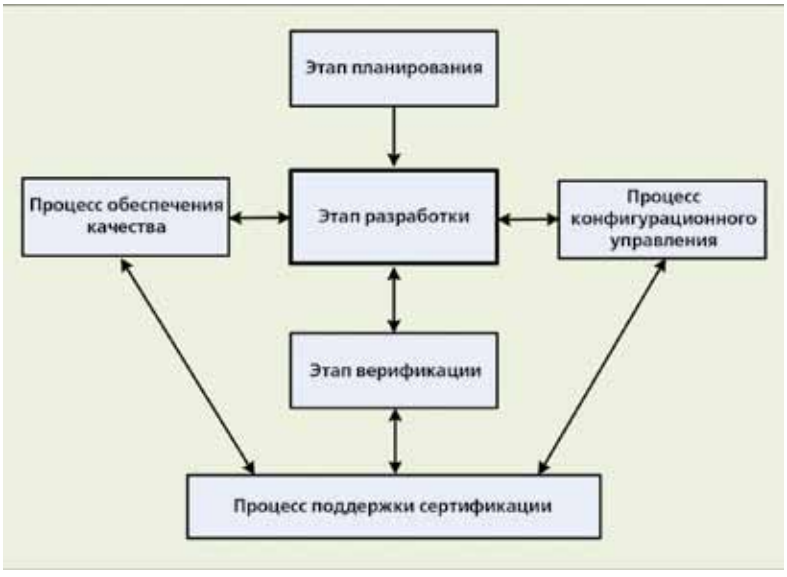

Рис. 1. Процесс создания программных продуктов согласно стандарту DO-178B/C

– необходимые стандарты разработки ПО;
– состав документации. К составу документации стандарт предъявляет требования по составу и содержанию в зависимости от уровня критичности ПО.

В процессе планирования должны быть разработаны процедуры сертификации, разработки ПО, верификации, управления конфигурациями и обеспечения качества.

Процесс разработки в стандарте DO-178B/C представляется в виде последовательного процесса:

- преобразования глобальных системных требований к ПО в требования к ПО высокого уровня;
- преобразования требований к ПО высокого уровня в требования низкого уровня;
- построения архитектуры ПО на базе требований высокого и низкого уровней;
- разработки кода ПО в соответствии с архитектурой;
- разработки проверочных (тестовых) планов на основании требований и полученного кода ПО.

Для каждого процесса стандарт предписывает ведение документации с обязательной возможностью проследить пути от требований более высокого уровня к требованиям более низкого уровня, и наоборот. Например, из документации должно быть понятно, какое системное требование привело к появлению каждого требования низкого уровня, как оно отразилось на архитектуре ПО и в каких строчках кода реализовано, а также какими тестами проверяется.

Под процессом верификации стандарт DO-178B/C понимает более широкий набор действий, нежели простая проверка по разработанным тестовым сценариям. Помимо проверки непосредственно кода ПО верификация включает проверку:

– соответствия требований к ПО глобальным системным требованиям к системе;
– соответствия требований низкого уровня и их реализации в архитектуре ПО требованиям более высокого уровня;
– реализации ПО в соответствии с разработанной архитектурой;

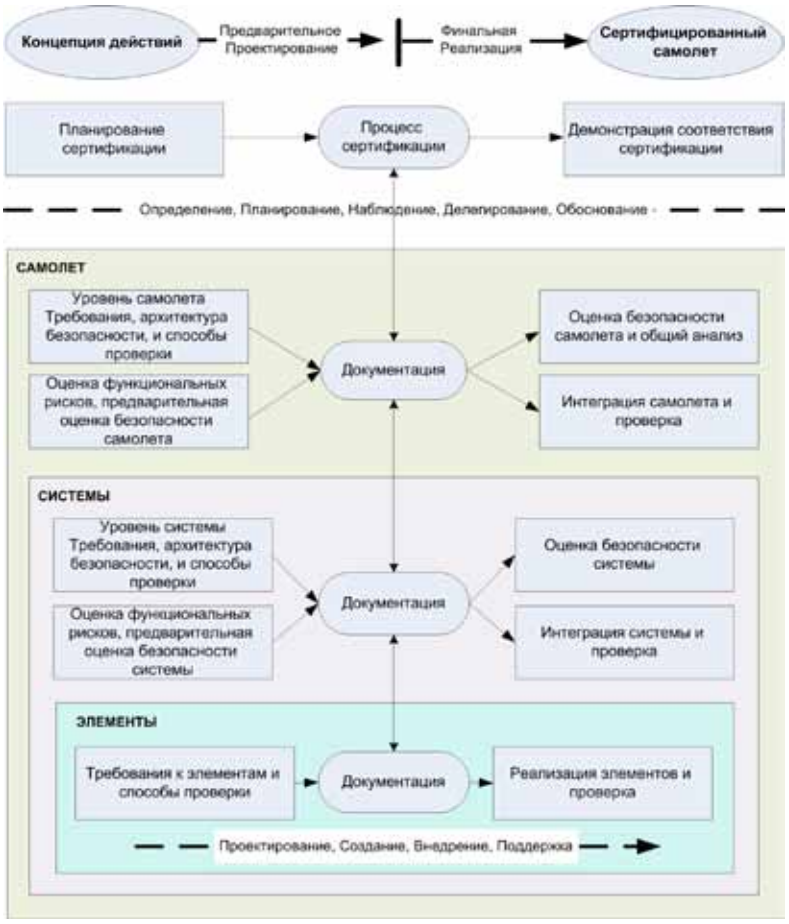

Рис. 2. Основные действия, направленные на обеспечение безопасности самолета в процессе его разработки и сертификации

– соответствия требований к ПО и его реализации.

Для проверки соответствия требований разного уровня стандарт предлагает различные методы анализа, в том числе и формальную инспекцию документов. Для верификации программного кода предлагаются различные варианты тестирования исполняемого кода.

Дополнительно в зависимости от уровня критичности ПО стандарт предусматривает:

1) проверку реализации 100% требований к программному коду;
2) проверку условия 1 и того, что все команды программного кода хотя бы один раз были исполнены в процессе тестирования;
3) проверку условия 2 и того, что все ветви программного кода были выполнены в процессе тестирования;
4) проверку условия 3 и того, что все условия ветвления программного кода были независимо проверены в процессе тестирования.

Проверка условий 2, 3 и 4 подтверждает отсутствие функций и участков кода, не используемых для обеспечения исходных требований, а также необходимость имеющихся условных ветвлений программы (т. е. невозможность удалить или оптимизировать части условий ветвления программного кода).

Требования стандарта к процессу конфигурационного управления относятся в первую очередь к формальному обеспечению разработчиков всеми необходимыми материалами и к обеспечению непрерывности процесса разработки. Процесс конфигурационного управления заключается в непрерывном обеспечении целостности всех элементов разрабатываемой системы – требований, архитектуры ПО, кода ПО и документации, а также взаимосвязей между ними.

В рамках процесса обеспечения качества стандарт предъявляет требования к составу и полноте документации и порядку ее ведения параллельно разработке ПО.

Стандарт DO-326

Стандарт DO-326 Airworthiness Security Process Specification рассматривает основные угрозы информационной безопасности инфраструктуры самолета, такие как:

– заражение бортовых систем вредоносным кодом;
– использование злоумышленником беспроводных каналов связи самолета для доступа к его информационным системам;
– DDoS-атаки на беспроводные каналы связи самолета;
– DDoS-атаки на системы, критичные для безопасности полета;
– злоупотребления персональными устройствами, взаимодействующими с системами самолета;
– получение доступа к интерфейсам и системам самолета из внешних каналов связи.

Все требования, угрозы и реализации системы ИБ рассматриваются в рамках трехуровневой иерархической модели:

1) самолет в целом;
2) системы и подсистемы самолета;
3) отдельные элементы систем или подсистем самолета (рис. 2).

Постепенная детализация угроз ИБ, начиная от самолета в целом и заканчивая подсистемами и элементами подсистем, является ключевым моментом стандарта DO-326.

Одной из составляющих построения надежной системы обеспечения безопасности информации является процесс управления рисками ИБ. В стандарте этот процесс представлен следующими составляющими:

1) определение периметра безопасности – точек взаимодействия рассматриваемой системы с любыми внешними системами;
2) определение угроз безопасности информации – источников угрозы, способов атаки и возможных воздействий на системы самолета;
3) разработка архитектуры системы безопасности исходя из детального описания оборудования и с учетом его сильных и слабых сторон;
4) соотнесение рисков ИБ с реальными последствиями успешного осуществления атаки с учетом его вероятности;
5) усиление элемента или изменение его дизайна или внедрение дополнительных механизмов защиты, если уровень риска неприемлемый;
6) трансляция требований и подходов к обеспечению безопасности информации с более высоких уровней на более низкие вплоть до требований к обеспечению безопасности информации на конечных элементах системы;
7) проверка информационной безопасности системы в целом – подтверждение того, что риски реализации всех угроз ИБ, реализованных через все возможные сценарии, имеют приемлемый уровень.

Стандарт ATA Spec 42

Стандарт ATA Spec 42 Aviation Industry Standards for Digital Information Security предъявляет требования к взаимной идентификации и управлению доступом между отдельными узлами и агрегатами самолета. В основе стандарта лежат широко распространенные в информационных системах общего назначения подходы и методы, такие как:

– инфраструктура открытых ключей (PKI);
– цифровые сертификаты и подписи;
– контрольные и хеш-суммы.

Одно из требований к современным авиационным системам – наличие управления идентификацией на основе PKI, технологии с «цепочкой доверия» к центру сертификации (CA). Центры сертификации используются для успешного применения цифровых подписей к онлайн-документации.

Фундаментальные принципы безопасности цифровых систем, используемые в гражданской авиации:

- информация, отправленная/запрашиваемая воздушным судном или системой, должна быть предоставлена правильному воздушному судну или системе в нужное время, а любые манипуляции или повреждения информации должны обнаруживаться;
- проверка подлинности должна проводиться в согласованном порядке;
- проверка подлинности должна применяться к людям, организациям и устройствам;
- во время передачи информация должна быть защищена последовательным образом;
- должны гарантироваться невозможность отказа системы и управление в согласованном порядке;
- системы должны легко проверяться. Проверки должны выполняться с использованием стандартных инструментов и быть автоматизированы где возможно;
- системы должны работать непрерывно. Если для продолжения работы необходимо смягчение мер безопасности, воздействия угроз должны компенсироваться соответствующими действиями.

Устройства проверки PKI авиационных систем должны иметь регистрационный код (например, C-GABC, N-12345) и 24-битный адрес ИКАО (ICAO – International Civil Aviation Organization, Международная организация гражданской авиации). К ключам предъявляются дополнительные требования:

– если закрытый ключ больше не будет использоваться, он должен быть стерт;
– закрытые ключи должны храниться на уровнях, соразмерных требованиям сертификационной политики;
– закрытые ключи должны загружаться на оборудование воздушного судна доказуемо безопасным способом.

Цифровые системы проверки подписи должны содержать меры по борьбе с атаками, эти меры должны быть таковы, чтобы стоимость успешной атаки оказывалась выше, чем ее возможные выгоды.

Приложение проверки подписей должно соответствовать заявленным целям безопасности для обеспечения гарантий для всей системы. Процесс проверки необходимо определить как очевидный способ проверки цифровой подписи в соответствии с правилами и направленный на достижение целей, соответствующих политике подписи. Чтобы обеспечить достоверность заданной сигнатуры или проверки подписи после определенного момента времени, должна проводиться датировка. Для кроссплатформенного представления подписи и подписанных ею данных необходимо использовать протокол PKCS#7 или XML DigSig.

Механизм идентификации самолета наземными станциями представлен на рис. 3.

От авиационной отрасли к критически важным объектам

Некоторые стандарты не оперируют понятиями информационной безопасности, однако их общая направленность на обеспечение безопасности эксплуатации авиационной техники приводит к серьезному прогрессу и в области защиты информации. Стоит отметить, что ни один из представленных стандартов в явном виде не опирается на специфику авиационной отрасли, поэтому возможно применение данных стандартов для любых сложных систем, несущих повышенные риски для жизни и здоровья людей в случае выхода из строя или нарушения работы.

В частности, хотелось бы рассмотреть применение вышеназванных стандартов для критически важных объектов (КВО) Российской Федерации.

КВО может быть представлен в виде иерархической модели, подобной той, что применяется в стандарте DO-326:

- КВО в целом;
- основные системы и подсистемы КВО, такие как АСУ, СЗИ, средства связи и др.;
- конечные элементы, составляющие различные подсистемы КВО, например ПЭВМ, коммутаторы, средства межсетевого экранирования, контроллеры, SCADA-системы.

При разработке КВО возникает множество общесистемных требований, которые (аналогично стандарту DO-178B/C) должны транслироваться в требования различных уровней для подсистем КВО и конечных элементов.

На этапе проектирования необходимо составить модель угроз и сценариев осуществления воздействий как для КВО в целом, так и для всех конечных элементов. Разработка механизмов обеспечения безопасности информации должна осуществляться начиная от конечных элементов посредством объединения в СЗИ отдельных подсистем КВО и заканчивая целостной СЗИ всего КВО.

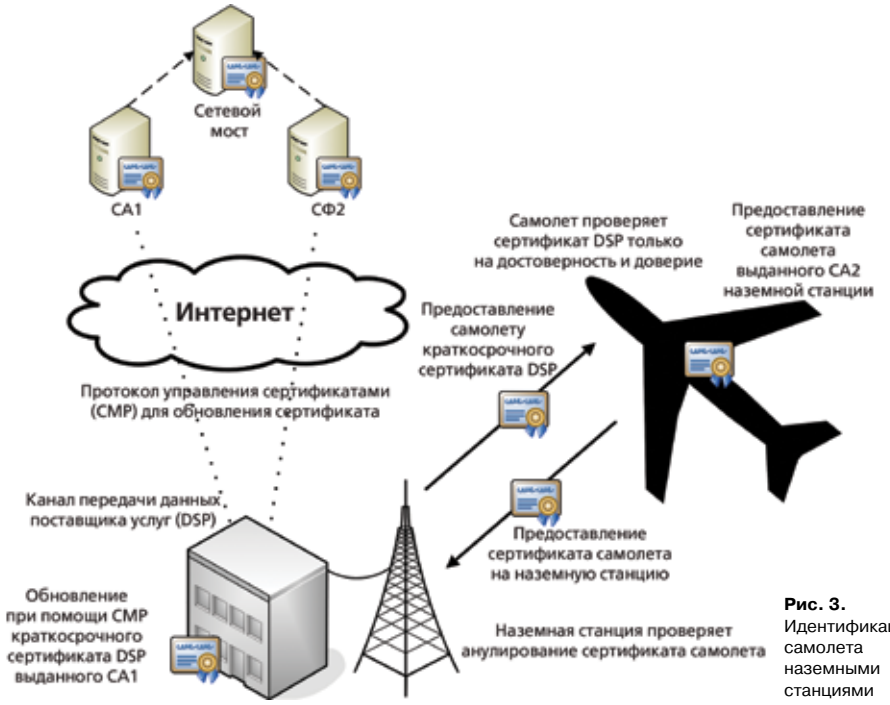

Рис. 3. Идентификация самолета наземными станциями

Ключевым элементом реализации КВО, устойчивого к внешним вредоносным воздействиям, является прослеживаемость пути развития всей системы – от исходных системных требований и требований по обеспечению безопасности информации через архитектурные решения до конечной реализации КВО в виде совокупности взаимно интегрированных систем и элементов.

Применение стандарта DO-326 позволит прогнозировать вероятные риски атак на КВО, а стандарта DO-178 – убедительно заявлять о применимости этих прогнозов для данного КВО. Объем документации, создаваемой в рамках работы по стандарту DO-178, даст возможность в случае обнаружения ошибок или недостатков реализации конечных элементов быстро выявлять проблемы в реализации общесистемных требований и оценивать возникающие в связи с этим риски.

Исходя из собственного опыта исследований безопасности АСУ, отметим, что одним из векторов атак на существующие программные и программно-аппаратные решения является несанкционированный удаленный доступ. Основная причина успешности этого класса атак – недостатки в механизмах идентификации объектов сетевого взаимодействия. Применение методов, изложенных в стандарте ATA Spec 42, позволит повысить уровень доверия к объектам информационного обмена в сетевой инфраструктуре КВО.

Заключение

Европейская и американская авиационные отрасли за последние несколько десятилетий накопили большой практический опыт разработки, строительства и эксплуатации современных воздушных судов с высоким уровнем информатизации. В состав современного воздушного судна входит множество информационных систем и АСУ, но, несмотря на это, безопасность воздушных полетов находится на достаточно высоком уровне. Отчасти в этом есть заслуга и авиационных стандартов, направленных на обеспечение безопасности полетов.

При построении систем с высоким уровнем риска для жизни и здоровья человека не лишним будет учесть опыт, накопленный в авиационной отрасли в различных стандартах, рекомендациях и методиках. ■