УДК 004.056

МОДЕЛЬ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ПОДДЕРЖКИ ЖИЗНЕННОГО ЦИКЛА ВОЗДУШНОГО СУДНА

© 2013 И.В. Жалдак, И.А.Кузахметов, А.Е. Трифанов

Ульяновский государственный университет

Поступила в редакцию 10.06.2013

Рассмотрены основные вопросы обеспечения безопасности интегрированной системы поддержки жизненного цикла воздушного судна с учетом специфики производства, современных требований и технологий.

Ключевые слова: безопасность информации, распределенные системы, конструкторская документация, авиационная промышленность.

В настоящее время в качестве инструментальных средств на каждом этапе жизненного цикла воздушного судна используются соответствующие специализированные информационные системы: системы конструкторского проектирования (CAD),системы управления данными об изделии (PDM), системы автоматизированного проектирования технологических процессов (CAPP), системы управления ресурсами (ERP), системы взаимодействия с клиентами (CRM), системы послепродажного обслуживания и др. [1] В авиационной промышленности наличие единой интегрированной информационной системы играет определяющую роль в снижении ресурсных затрат (временных, трудозатрат, финансовых, материальных), повышении качества и как следствие конкурентоспособности продукции. Безопасность такой системы является одной из главной составляющей работы в этом направлении. Цель этой статьи определить минимальный набор программно-аппаратных элементов для комплексного подхода к обеспечению безопасности интегрированной системы поддержки жизненного цикла воздушного судна с учетом специфики предприятий авиационной промышленности, которые описаны ниже.

Исходя из структуры систем поддержки жизненного цикла изделий [1] и специфики предприятий авиационной промышленности можно выделить следующие ее особенности:

1. Компоненты корпоративной информационной системы (далее – КИС) расположены не только на разных компьютерах, но и территориально удалены друг от друга, в связи с большой площадью предприятия, подключение КБ, находящиеся в других городах.

2. Для управления различными подсистемами КИС предприятия используются разные операционные системы (Microsoft Windows, Linux/Unix-системы, Mac и др.).

3. Разнообразие программного(CAD, PDM, CAPP, ERP, CRM-системы и другие) и технического обеспечения (сервера, СХД, коммутаторы, программируемые станки и т.д.).

4. Огромное количество документов и их видов (так, только техническая документация самолета состоит более чем 1 млн. документов).

5. Большие объемы хранимых данных.

6. Высокая степень конфиденциальности информации (персональные данные, коммерческая тайна, государственная тайна).

7. Большое количество пользователей с различными правами доступа, ролями и функциями.

8. Требование к неизменности документов (электронное дело изделия – паспорт ВС).

Для построения модели безопасности необходимо дать определение термину безопасности информации. Безопасность информации — состояние защищённости информации, при котором обеспечены её конфиденциальность, доступность и целостность [2].

Чтобы обеспечить конфиденциальность информации, учитывая особенности сферы применения, описанные выше, необходимо использовать распределенную архитектуру [3]. Для упрощения управления такой системой существуют специальные структуры - домены, которые построены на базе иерархической модели. В корне такой структуры находится специальная система – контроллер домена, выполняющая следующие основные функции:

а) учет всех узлов, входящих в домен;

б) учет пользователей и групп домена;

в) хранение и реализация групповых политик учетных записей;

Иван Васильевич Жалдак, начальник Центра телекоммуникаций и технологий Интернет. E-mail: zi@ulsu.ru

Илгуз Кузахметов, начальник отдела локальных сетей. E-mail: ilgiz@ulsu.ru

Андрей Трифанов, кандидат технических наук, заместитель директора технопарка «УлГУ – высокие технологии»

г) авторизация служб и приложений внутри домена;

д) авторизация пользователей и узлов домена.

Большинство современных операционных систем имеют возможность включения в домен, по крайней мере, позволяют реализовать аутентификацию с удаленного сервера (контроллера домена) [4]. Использование такого подхода позволит обеспечить конфиденциальность и целостность данных.

Разнообразие политик доменных служб распространяется и на пользовательское программное обеспечение. Существует возможность предоставлять пользователям права на работу с конкретными приложениями вне зависимости от конкретного рабочего места пользователя. Что повышает надежность работы, позволяет планировать и оптимизировать затраты на лицензии для ПО.

Проблемы обеспечения должного уровня конфиденциальности информации, управления правами доступа пользователей и контроля неизменности данных позволяют решать групповые политики безопасности, криптографические подсистемы и межсетевое экранирование. Наличие контроллера домена значительно упрощает реализацию и управление данными механизмами. Наличие криптографической подсистемы внутри домена позволяет решить следующие задачи:

а) использование функций шифрования каналов связи (конфиденциальность данных, передаваемых по сети);

б) использование функций шифрования данных (конфиденциальность информации, хранящейся на файловой системе);

в) использование функций электронной подписи (обеспечение и проверка целостности информации);

г) создание, хранение, распространение и проверка ключевой информации пользователей;

д) реализация функций многофакторной аутентификации пользователей.

Инфраструктура открытых ключей (PKI) — инфраструктура, предназначенная для управления открытыми ключами и сертификатами с целью поддержки услуг аутентификации, шифрования, целостности и неотрицания авторства. Открытый ключ, связанный с определенным пользователем, должен быть удостоверен сертификатом, подлинность которого должна проверяться доверенным учреждением — Центром Сертификации (Certification Authority) [5].

Другой термин, принятый для именования такого объекта — Удостоверяющий Центр (УЦ). По сути, такое именование более корректно, однако менее распространено в технической литературе.

Функции удостоверяющего центра:

а) Подтверждение аутентичности объекта, запрашивающего сертификат. Механизмы проверки зависят от типа CA.

б) Выдача сертификатов. Информация в сертификате определяется его шаблоном.

в) Управление отзывом сертификатов. Список отзыва сертификатов (CRL) гарантирует невозможность использования «неправильных» сертификатов.

В результате проектирования инфраструктуры PKI необходимо определить:

- кол-во уровней иерархии и структуру УЦ;
- типы используемых цифровых сертификатов;
- виды УЦ, работающих на каждом из уровней иерархии;
- необходимость интеграции со службой каталога;
- методы защиты УЦ;
- потребности в различных политиках сертификатов.

Существуют несколько моделей иерархии PKI: одноуровневая, двухуровневая, трехуровневая и четырехуровневая. В описываемой модели рекомендуется использовать двухуровневую модель, как оптимально подходящую по всем критериям:

а) масштабируемости;

б) простоты реализации;

в) надежности;

г) стоимости.

Криптографическая подсистема в домене (инфраструктура открытых ключей - PKI) при двухуровневой иерархии состоит из следующих элементов (рис. 1):

а) отключенный корневой сервер (Root CA);

б) один или несколько издающих сертификаты серверов (Issuing CA);

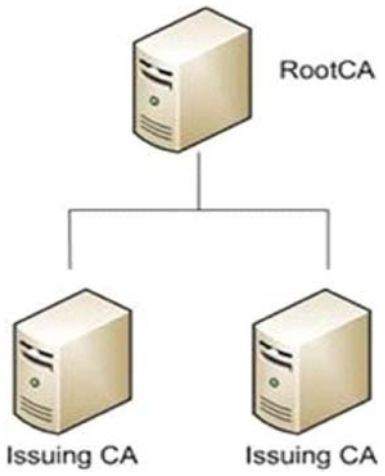

Рис. 1. Двухуровневая иерархия PKI

При этом на издающие УЦ ложится функционал по управлению политиками сертификатов. Для обеспечения безопасности инфраструктуры

корневой центр является “отдельностоящим” (stand-alone) и автономным (offline), то есть не входит в состав домена не подключается к сети предприятия, и, практически, постоянно находится в отключенном состоянии. Тем самым, мы избегаем атак на корневой сервер. Что касается издающих центров, то они получают сертификат, подписанный корневым сервером, которому доверяют все участники взаимодействия, то есть обладатели сертификатов, полученных с любого УЦ предприятия.

Для реализации и соответствия требований нормативно-правовых актов Российской Федерации, корневой центр сертификации должен представлять сертифицированный программный или программно-аппаратный комплекс выпускающий сертификаты в соответствии с текущим алгоритмом ГОСТ на электронную подпись. Издающий центр (центры) должны быть интегрированы в домен и распространять сертификаты в формате x509, для наилучшей совместимости с узлами домена.

В целях повышения уровня доступности и отказоустойчивости сервиса предусматривается развертывания более чем одного издающего сервера [6].

Таким образом, сертификаты открытых ключей пользователей и корневой сертификат доступны всем пользователям домена. Закрытые ключи пользователей необходимо хранить на специальных ключевых носителях (USB-токенах или смарт-картах). Удобство использования подобных устройств обусловлено тем, что:

а) сертифицированные ключевые носители обладают высокой степенью надежности;

б) вводится не ключевая фраза, а пароль к устройству;

в) возможно использование ключевого носителя в разных подсистемах;

г) возможно хранение нескольких ключей на одном устройстве.

Так же ключевые носители необходимо использовать для реализации двухфакторной аутентификации пользователей на узлах домена [7].

Использование систем межсетевого экранирования (далее - МЭ), а так же политик их работы внутри домена, повышает общий уровень информационной безопасности модели, мешает злоумышленникам получать информацию о структуре сети, сетевых узлах, сетевых службах на узлах и т.д. Кроме того, МЭ предотвращает или существенно затрудняет реализации таких видов сетевых атак, как: “ переполнение буфера” и “отказ в обслуживании”, что повышает уровень доступности информации и информационных ресурсов.

Доступность информации с помощью виртуализации и постоянным контролем и управлением информационной инфраструктурой. Как уже было отмечено выше, наша система распределена не только на несколько компьютеров, но также распределена территориально. В единую управляемую систему возможно развернуть на различном оборудовании, в состав таких систем могут входить [8]:

- отдельные сервера;
- серверные кластеры;
- бездисковые рабочие станции (терминальные клиенты);
- сетевое коммутационное оборудование;
- оборудование для разграничения доступа к сети;
- аппаратные системы хранения данных (с сетевым и бессетевым доступом);
- системы резервного копирования данных;
- аппаратные носители ключевой информации;
- и многое другое.

Следовательно, необходимо, что бы все операции были максимально автоматизированы. Для достижения высокой доступности информации мы должны воспользоваться технологиями виртуализации и постоянным контролем и управлением информационной инфраструктурой с едиными центрами.

Виртуализация повышает эффективность использования и доступность ИТ-ресурсов и приложений. Увеличение доступности оборудования и приложений для повышения уровня непрерывности бизнеса: надежное резервное копирование и перенос виртуальных сред целиком без прерывания работы. Исключение плановых простоев и быстрое восстановление после непредвиденных сбоев.

Эксплуатационная гибкость: оперативное реагирование на изменения рынка благодаря динамическому управлению ресурсами, ускоренной инициализации серверов и улучшенному развертыванию настольных компьютеров и приложений.

Улучшение управляемости и безопасности настольных компьютеров: развертывание, администрирование и мониторинг безопасных сред настольных компьютеров, к которым пользователи могут обращаться локально или удаленно через сетевое подключение или без него, используя практически любой стандартный настольный компьютер, ноутбук или планшетный ПК [9]. Системы виртуализации так же могут работать внутри домена.

Использование виртуальной платформы, средств кластеризации серверов и сетевых систем хранения данных (далее – СХД) позволяют работу с высокой степенью надежности, безопасности и производительности различных систем управления базами данных (далее – СУБД) и больших объемов информации. СУБД размещаются на виртуальных системах, а сами данные

хранятся на специализированных СХД. Однотипные СХД можно так же объединять в группы (кластеры), увеличивая производительность, безопасность, надежность и максимальный объем хранимых данных. Таким образом, учитывая платформу виртуализации и распределенное внешнее хранение данных (включая сами файлы-образы виртуальных машин), мы имеем схему, устойчивую к различным сбоям, с высокой производительностью и низким временем восстановления после аварийных ситуаций [10].

Сетевое оборудование, серверы, специализированные технические и программные решения и службы являются компонентами ИТ-инфраструктуры и нуждаются не только в качественной настройке и сопровождении, но и в постоянном управлении, модернизации и адаптации всей ИТ-инфраструктуры к потребностям бизнеса и меняющимся внешним условиям[11].

Определим способы управления и мониторинга информационной инфраструктурой:

- получение актуальной информации о составе аппаратного и программного обеспечения, его настройках;

- управление жизненным циклом программного обеспечения: развертывание приложений, установка обновлений, инвентаризация, анализ использования ПО;

- автоматизация и контроль процесса развертывания операционных систем на серверах и рабочих станциях, включая миграцию на новые версии ОС;

- централизованное управление виртуальной серверной инфраструктурой на всех стадиях жизненного цикла физических и виртуальных серверов. Когда у вас пара физических серверов, на которых крутится десяток другой виртуальных машин, вполне можно обойтись штатной консолью гипервизора. Если же мы имеем дело с ЦОД, с десятками серверов и сотнями или даже тысячами виртуальных машин, управлять такой виртуальной средой без специализированных инструментов практически невозможно. Позволяет осуществлять миграцию виртуальных машин, что дает возможность без остановки работы сервера (например, при техническом обслуживания физического сервера или при большой текущей загрузка CPU на одном из узлов кластера, в то время как другие узлы относительно свободны);

- необходимо решение для резервирования и восстановления сред, обеспечивающий наилучшую защиту и использующий наиболее распространенные сценарии восстановления с дисков, ленточных носителей и из облака, осуществляя это масштабируемым, управляемым и экономически выгодным способом. Обеспечивает централизованное управление, централизованный контроль, централизованное устранение неисправностей, совместное размещение носителей данных, поддерживает совместимость с существующими средами, интеграция с существующими системами отслеживания ошибок, рабочими процессами и структурами групп, корпоративная масштабируемость, отказоустойчивость и надежность;

- анализ готовности существующей инфраструктуры к развертыванию новых операционных систем и приложений;

- проактивный мониторинг ключевых объектов ИТ-инфраструктуры. Под ключевыми объектами подразумеваются Windows-, Linux-серверы, но также ими могут активное сетевое оборудование или, например, конкретные .NET-приложения. Позволяет принять превентивные меры до того как проблемы скажутся на доступности сервисов;

Подводя итоги, можно сказать, что модель (рис. 2) безопасности интегрированной системы поддержки жизненного цикла воздушного судна

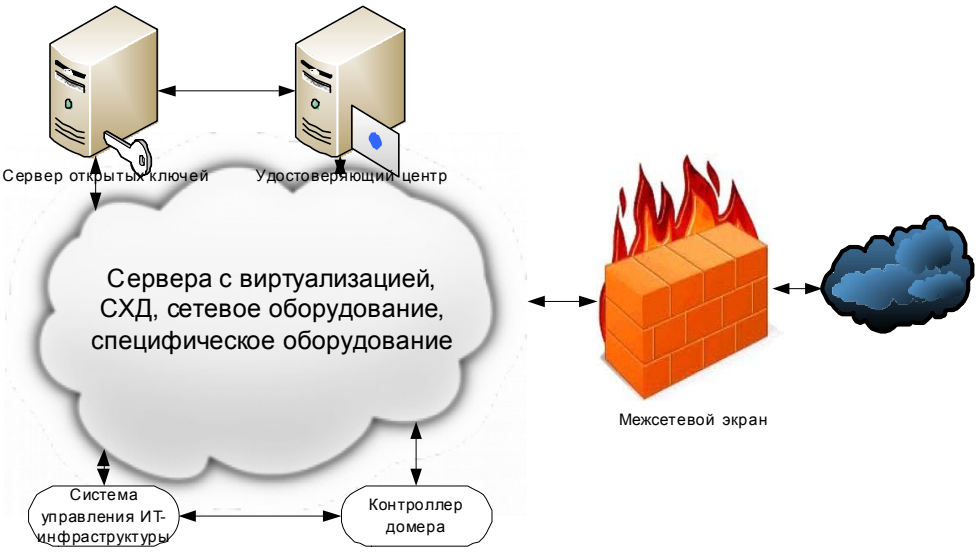

Рис. 2. Модель безопасности интегрированной системы

должна состоять из следующих элементов.

1. Система контроля доступа. Контроллер домена (может быть реализован на базе Microsoft Active Directory, OpenLDAP и др).

2. Криптографические подсистемы с инфраструктурой открытых ключей и удостоверяющим центром (для корневых центров - сертифицированные программные, аппаратно-программные решения, в соответствии с руководящими документами федеральных органов исполнительной власти РФ, для издающих центров – удовлетворяющие этим требованиям штатные средства операционных систем, например Microsoft PKI).

3. Межсетевое экранирование (сертифицированные программные, аппаратно-программные решения, в соответствии с руководящими документами федеральных органов исполнительной власти РФ или удовлетворяющие этим требованиям штатные средства операционных систем, сетевого оборудования)

4. Виртуализация (Microsoft Hyper-V, VMware ESX, Xen и др).

5. Система управления информационной инфраструктурой (Microsoft System Center 2012, HP OpenView и др.).

Подбор этих элементов должен основываться на том программно-аппаратном комплексе, существующем на предприятии. Если преобладают продукты фирмы Microsoft, то и продукты для реализации этих элементов тоже должен быть Microsoft. Без любого из этих элементов невозможно достигнуть необходимого уровня безопасности интегрированной системы.

Таким образом, данная модель позволяет реализовать современные подходы к безопасности информации с учетом особенностей информационной сферы предприятий авиационной промышленности.

Система, построенная на данной модели, имеет такие преимущества как, масштабируемость, возможность модернизации и тиражирования данного решения. Каждый ее элемент имеет несколько практических реализаций. Комбинируя реализации можно получить наиболее оптимальной вариант для конкретного предприятия, что является дальнейшим продолжением работы в этом направлении.

Работа выполнена при частичном финансировании Министерства образования и науки Российской федерации в рамках государственного контракта ! 07.514.11.4131

СПИСОК ЛИТЕРАТУРЫ

1. Развитие полиплатформенной интегрированной автоматизированной системы информационной поддержки жизненного цикла воздушных судов на основе электронного определения изделия / *Ю.В. Полянсков, С.Г. Дементьев, Д.Ю. Шабалкин, А.М. Топорков, В.В. Назаров* // Известия Самарского научного центра РАН. 2012, Т. 14. № 4 (2). С. 333-338.
2. *Ершов В.А. Кузнецов Н.А.* Мультисервисные телекоммуникационные сети М.: МГТУ им. Н. Э. Баумана, 2003 г. 432 с.
3. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).
4. *Ватаманюк А.* Создание, обслуживание и администрирование сетей на 100% . СПб.: Питер, 2010. 288 с.
5. *Берлин А.Н.* Телекоммуникационные сети и устройства. М.: Интернет-университет информационных технологий, Бином. Лаборатор, 2008. 320 с.
6. Инфраструктуры открытых ключей. Учебное пособие / *О.Ю. Полянская, В.С. Горбатов.* М.: Бином, 2007.
7. Информационная безопасность систем организационного управления. Теоретические основы. В 2-х томах. Том 1. СПб.: Наука, 2006. 496 с.
8. Информационная безопасность систем организационного управления. Теоретические основы. В 2-х томах. Том 2. СПб.: Наука, 2006. 440 с.
9. *Мэйволд Э.* Безопасность сетей. Самоучитель. М.: Эком, 2005. 528 с.
10. Методы и средства защиты информации. Том 2. Информационная безопасность / *С.В. Ленков, Д.А. Перегудов, В.А. Хорошко.* М.: Арий, 2008. 344 с.
11. *Елманова Н., Пахомов С.* Виртуальные машины 2007 // КомпьютерПресс. 2007. №9. С.29-42.
12. Система обеспечения информационной безопасности Взаимоувязанной сети связи РФ. Термины и определения (ОСТ 45.127-99).

SECURITY MODEL OF INTEGRATED LIFE CYCLE SUPPORT SYSTEMS OF AIRCRAFT

© 2013 I.V. Zhaldak, I.A. Kuzakhmetov

Ulyanovsk State University

Presents the main issues of providing security of integrated life cycle support systems of aircraft, in view of specificity of production, modern requirements and technologies.

Key words: information security, distributed systems, design documentation, aviation industry.

Ivan Zhaldak, Head of Telecommunication and Internet Technologies Centre. E-mail: zi@ulsu.ru
Ilgiz Kuzakhmetov, Head of Local Area Networks Department. E-mail: ilgiz@ulsu.ru
Andrey Trifanov, Candidate of Technics,Vice-Director of Technopark «UlSU – High Technology».