УДК 004.056

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ЖИЗНЕННОГО ЦИКЛА ВОЗДУШНЫХ СУДОВ

© 2013 И.В. Жалдак, М.А. Ефремова

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, технологий и нормативно-правовой базы.

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

Обеспечение безопасности интегрированной системы поддержки жизненного цикла воздушного судна организационно-правовыми средствами представляет собой сложный процесс, который сочетает в себе различные составляющие. По своей направленности эти средства и меры можно условно разделить на правовые и организационные. Именно правовые меры являются базисом, определяющим порядок и объем применения организационных мер. Ключевым моментом в этом направлении является принятие локальных нормативных актов, отражающих как политику предприятия по обеспечению информационной безопасности в целом, так и детализирующих отдельные ее направления. Политика информационной безопасности определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуются сотрудники предприятия в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения информационной безопасности. Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий на предприятии, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений. Политика информационной безопасности предприятия является основополагающим нормативным актом в этом направлении. К нормативным актам, регулирующим отдельные направления обеспечения информационной безопасности можно отнести следующие:

- План обеспечения информационной безопасности.
- Модель угроз безопасности функционирования автоматизированных систем.
- Положение «О порядке оформления, передачи и хранения документов в электронном виде».
- Комплексный план защиты информационных ресурсов от несанкционированного доступа.
- Правила обеспечения информационной безопасности при работе пользователей в корпоративной сети предприятия.
- Правила по работе сетью Интернет.

Безусловно, данный перечень является примерным и может постоянно дорабатываться и пополняться. По мере совершенствования используемых на предприятии организационных, технологических и процедурных аспектов обеспечения информационной безопасности, должны обновляться и нормативные акты предприятия в этой сфере. Использование устаревших нормативных актов по вопросам обеспечения информационной безопасности предприятия может привести к резкому снижению эффективности применения иных мер, в том числе организационных.

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 подсисте-

Жалдак Иван Васильевич, начальник Центра телекоммуникаций и технологий Интернет. E-mail: zi@ulsu.ru
Ефремова Марина Александровна, доцент кафедры уголовного права и криминологии. E-mail: seamaid63@gmail.com

мами 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).

Безопасность информации— состояние защищённости информации, при котором обеспечены её конфиденциальность, доступность и целостность[2].

Для логической связи компонент КИС предприятия 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;

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 (рисунок 1):

а) отключенный корневой сервер (Root CA);

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

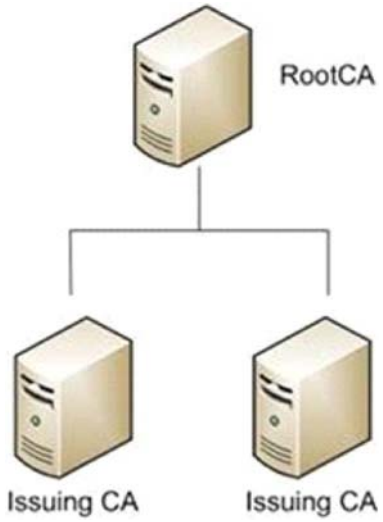

Рис. 1. Двухуровневая иерархия PKI

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 информа-

ции 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.

Работа выполнена при частичном финансировании Министерства образования и науки Российской федерации в рамках государственного контракта № 12.527.11.0010

СПИСОК ЛИТЕРАТУРЫ

1. *Ершов В.А., Кузнецов Н.А.* Мультисервисные телекоммуникационные сети. М.: МГТУ им. Н. Э. Баумана, 2003. 432 с.
2. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).
3. *Ватаманюк А.* Создание, обслуживание и администрирование сетей на 100%. СПб.: Питер, 2010. 288 с.
4. *Берлин А.Н.* Телекоммуникационные сети и устройства. М.: Интернет-университет информационных технологий, Бином. Лаборатор, 2008. 320 с.
5. *Полянская О.Ю., Горбатов В.С.* Инфраструктуры открытых ключей. Учебное пособие. М.: Бином, 2007 г.
6. Информационная безопасность систем организационного управления. Теоретические основы. В 2-х томах. Том 1. СПб, Наука, 2006. 496 с.
7. Информационная безопасность систем организационного управления. Теоретические основы. В 2-х томах. Том 2. СПб, Наука, 2006. 440 с.
8. *Мэйволд Э.* Безопасность сетей. Самоучитель. М.:, Эком, 2005. 528 с.
9. Методы и средства защиты информации. Том 2. Информационная безопасность / *С.В. Ленков, Д.А. Перегудов, В.А. Хорошко.* М.: Арий, 2008. 344 с.

PROVIDING OF INFORMATION SECURITY OF INTEGRATED LIFE CYCLE SUPPORT SYSTEMS OF AIRCRAFT

© 2013 I.V. Zhaldak, M.A. Efremova

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 requirement, technologies and law basis.
Keywords: information security, distributed systems, design documentation, aviation industry.

Ivan. Zhaldak, Director of Regional Teaching and Research Center of Information Security Problems. E-mail: zi@ulsu.ru
Marina Efremova, Candidate of Jurisprudence, Associate Professor at the Criminal Law and Criminology Department. E-mail: Seamaid63@gmail.com