УДК 004.056

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОНСТРУКТОРСКОЙ ДОКУМЕНТАЦИИ НА ПРЕДПРИЯТИЯХ АВИАЦИОННОЙ ПРОМЫШЛЕННОСТИ

© 2012 И.В. Жалдак, Н.А. Карманович

Ульяновский государственнфй университет

Поступила в редакцию 10.10.2012

Рассмотрены основные требования к построению системы обеспечения информационной безопасности информационной системы поддержки жизненного цикла конструкторской документации на предприятиях авиационной промышленности.

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

На сегодняшний день информационные системы и технологии тесно связаны с промышленностью. И не удивительно, что в промышленности используются электронные модели изделий. Порядок формирования подобных электронных документов, структура, условия использования, хранения и другие операции описаны в соответствующих государственных стандартах.

Стандарты являются методическим базисом развития информационных технологий, определяющим правила электронного представления данных об изделиях, среде и процессах, а также правила обмена этими данными. В области конструкторской документации (КД) в машиностроении и приборостроении главным системообразующим элементом стандартизации является Единая система конструкторской документации (ЕСКД), основное назначение которой состоит в установлении единых взаимосвязанных правил, требований и норм выполнения, оформления и обращения КД [1].

Большинство стандартов было разработано более 30 лет назад и остаются актуальными по сей день, соответственно проблема легитимности использования электронной КД, ее юридическая значимость и безопасность остается актуальной. Дополнение стандартов ЕСКД соответствующими положениями для решения вышеописанных проблем – серьезная и сложная задача, которая должна решаться на государственном уровне.

Предприятия авиационной промышленности особенно чувствительны к подобным проблемам, ведь практически все они получают КД из конструкторских бюро (КБ) в электронном виде, кроме того, авиационная промышленность (АП) – одна из самых трудоемких, наукоемких и ответственных. Еще один момент: на предприятиях АП КД представляет собой как минимум коммерческую тайну, а в некоторых случаях и государственную.

Жалдак Иван Васильевич, директор Регионального учебно-научного центра по проблемам информационной безопасности УлГУ. E-mail: zi@ulsu.ru

Карманович Николай Алексеевич, научный сотрудник Регионального учебно-научного центра по проблемам информационной безопасности УлГУ. E-mail: kna@ulsu.ru

Для обеспечения безопасности КД и информационной системы поддержки ее жизненного цикла необходимы мероприятия, сочетающие в себе организационную и техническую части. Причем данные мероприятия необходимо проводить регулярно, подстраиваясь под эволюцию информационных технологий и средств вычислительной техники.

На организационном уровне руководством организаций, использующих защищаемые ИС, определяются требования к их функционированию, процедуры и мероприятия, направленные на безопасное использование этих систем, требования к персоналу и т.п.

На техническом уровне разворачиваются средства защиты информации, к которым относятся специализированные программные и программно-аппаратные комплексы, предназначенные для применения в компьютерах и компьютерных сетях, системы видео наблюдения, сигнализации, средства обнаружения подслушивающих устройств, средства устранения побочных каналов утечки информации (например, через излучение монитора) и т.п. [2].

Подробнее остановимся на техническом уровне. Рассмотрим систему поддержки жизненного цикла КД, построенную на следующей базе трехуровневой модели:

1. Ядро ИС (на этом уровне обеспечивается хранение данных, сюда входит СУБД и PDM-подсистема, ответственная за хранение данных);

2. Сервисная шина предприятия и средства интеграции; (на этом уровне организуется “бесшовная” интеграция всевозможных приложений и программных комплексов предприятия и их доступ к общему хранилищу данных);

3. Интегрированные приложения (CAD, CRM, PDM, ERP, офисные и другие системы и приложения).

Для обеспечения безопасности формируется ряд требования к каждому уровню модели и к системе обеспечения информационной безопасности (СОИБ).

В состав СОИБ должны входить следующие подсистемы [2,3,4]:

• подсистема управления политикой информационной безопасности;
• подсистема анализа и управления рисками;
• подсистема идентификации и аутентификации;
• подсистема разграничения доступа;
• подсистема протоколирования и пассивного аудита;
• подсистема активного аудита;
• подсистема контроля целостности данных;
• подсистема контроля защищенности;
• подсистема удостоверяющий центр (криптографическая подсистема);
• подсистема сегментирования ЛВС и межсетевого экранирования;
• подсистема VPN;
• подсистема антивирусной защиты;
• подсистема фильтрации контента;
• подсистема управления безопасностью;
• подсистема предотвращения утечки информации по техническим каналам.

Важную роль в обеспечении информационной безопасности КД играет система аутентификации и криптографическая подсистема [5]. Современные технологии позволяют использовать средства защиты информации (СЗИ) и средства криптографической защиты информации (СКЗИ) совместно. Так, например, использование электронных замков совместно с USB-токеном, для аутентификации на рабочем месте. Этот же токен можно использовать для хранения закрытого ключа шифрования/подписи пользователя. Открытые ключи и их сертификаты хранятся на сервере, поддерживающим PKI-инфраструктуру (инфраструктуру открытых ключей), которая непосредственно связанна с удостоверяющим центром.

Таким образом, при использовании сервера аутентификации (например LDAP и его варианты), электронный замок и токен получаем многофакторною аутентификацию.

Также единый центр аутентификации хранит не только информацию о пользователях АРМ, но и информацию о пользователях СУБД, PDM и других систем, пользователей и администраторов сетевого активного оборудования.

Использование электронной подписи [6] позволяет решить проблему целостности и юридической значимости электронных КД. К сожалению, современное законодательство не дает четких ответов на вопросы типа и количества электронных подписей в документе, но внутренними стандартами предприятия и аналогичными нормативными документами можно установить данные параметры.

При соблюдении всех необходимых условий, особенно многофакторной аутентификации, разграничения прав доступа пользователей, использования электронной подписи и защищенных (шифрованных) каналов связи можно построить достойную предприятия АП СОИБ.

Работа выполнена при частичном финансировании Министерства образования и науки Российской федерации в рамках государственного контракта № 07.514.11.4131

СПИСОК ЛИТЕРАТУРЫ

1. *Левин А.И.* О сути изменений в стандартах ЕСКД // Информационные технологии в проектировании и производстве. 2006. №4. С. 11-15.
2. *Тимофеев П.А., Панасенко С.П.* Средства защиты критически важной информации // Вопросы защиты информации. 2006. № 3. С. 40-48.
3. *Белоусова Н.В., Грибановская Е.А., Картавцева С.Н., Савва Т.Ю., Черникова С.И.* Обеспечение комплексной защищенности информационных ресурсов, как задача информационного менеджмента // Информационные системы и технологии. 2008. №1-4. С. 153-155.
4. *Белопушкин В.И., Кириллычев А.Н.* Система информационной безопасности в корпоративных вычислительных сетях // Горный информационно-аналитический бюллетень (научно-технический журнал) Mining informational and analytical bulletin (scientific and technical journal). 2005. № 7. С. 223-229.
5. *Мигунов В.В., Кафиятуллов Р.Р.* Защита информации в комплексной САПР реконструкции промышленных предприятий // Известия Южного федерального университета. Технические науки. 2006. Т. 63. № 8. С. 136-139.
6. *Елисеев Н.И., Ржевский Д.А.* Обеспечение подлинности документированной информации // Известия Южного федерального университета. Технические науки. 2011. Т. 125. №12. С. 146-152.

PROVIDING OF INFORMATION SECURITY OF DESIGN DOCUMENTATION FOR AVIATION INDUSTRY COMPANIES

© 2012 I.V. Zhaldak, N.A. Karmanovich

Ulyanovsk State University

Presents the basic requirements for building information security system of the life cycle support information system of design documentation for aviation industry companies.
keywords: information security, design documentation, aviation industry.

Ivan Zhaldak, Director of Regional Teaching and Research Center of Information Security Problems. E-mail: zi@ulsu.ru
Nikolay Karmanovich, Research Associate of Regional Teaching and Research Center of Information Security Problems. E-mail: kna@ulsu.ru