УДК 65.011.56+004.056.57

Аудит систем управления экономическими объектами в авиастроении

Новиков А.Н.

Московский городской университет управления Правительства Москвы,

Сретенка ул., 28, Москва, 107045, Россия

e-mail: dalia888@rambler.ru

В статье предлагается технология проведения аудита систем управления авиационными промышленными предприятиями и организациями на предмет качества систем, их безотказности и защищенности обрабатываемой в них управленческой информации.

Формулируется перечень основных этапов проведения аудита, их результаты и возможные рекомендации по совершенствованию систем управления на основе проведенного анализа.

Ключевые слова: система управления экономическим объектом, информационная безопасность, ИТ-аудит, эффективность системы управления.

Введение

Современное развитие вычислительной техники и методов хозяйствования привели к внедрению информационных технологий во все экономические процессы. Управление любым промышленным экономическим объектом в настоящее время во многом обеспечивается процессами обработки информации с использованием автоматизированных систем управления. Чем сложнее вид деятельности

организации, тем больше роль информационной системы в его функционировании. В такой наукоемкой отрасли, как авиационно-промышленный комплекс (АПК), информационные системы обеспечивают весь жизненный цикл продукции: от проектирования и производства до конца эксплуатации изделий.

В системах управления экономическими объектами важнейшее место занимают вопросы обеспечения безотказной работы систем и защиты обращающейся в них информации. Для решения этих проблем применяется аудит информационных систем и технологий (ИТ-аудит), представляющий собой комплекс мероприятий, проводимых в рамках обеспечения устойчивости протекания процессов управления объектом [1].

Основная цель ИТ-аудита — оценка рисков, связанных с использованием информационных технологий, оценка качества системы их контроля и выработка рекомендаций по принятию корректирующих мер в областях, где риски должны быть снижены.

С учетом возрастающей роли автоматизированных систем управления на предприятиях АПК и роста объемов управленческой информации всё большее значение приобретают проблемы обеспечения функционирования АСУ, а, следовательно, и процедуры аудита информационных систем и технологий.

ИТ-аудит включает в себя четыре основных направления:

- аудит информационной системы;
- аудит технологической инфраструктуры;
- аудит информационной безопасности;
- аудит информационной службы организации [2–4].

Какие вопросы должны рассматриваться в рамках каждого из направлений ИТ-аудита на предприятиях АПК? На какие аспекты функционирования ИС следует обратить внимание при оценке качества системы и рисков ее использования, и какие рекомендации по совершенствованию систем управления могут быть даны в наиболее распространенных случаях? Рассмотрим поочередно предложенные направления ИТ-аудита.

Аудит информационной системы предприятия АПК

Это направление аудита должно иметь целью сформулировать понятие о том, отвечает ли потребностям авиационно-промышленного предприятия функционирующая информационная система (ИС).

В технологию аудита ИС автор считает необходимым включить следующие работы:

- анализ соответствия существующей АСУ бизнес-процессам предприятия (включает в себя анализ организационной структуры предприятия, иерархических связей; анализ внутреннего документооборота и системы учета; анализ соответствия модулей используемой АСУ реальным потребностям подразделений);
- анализ существующих информационных сервисов и поддерживающих их программных продуктов;
- исследование существующей информационной системы на предмет соответствия заложенным требованиям, стоимости сопровождения и развития

ИС, соответствия ИТ-процессов стандартам ISO 9000, обеспечения информационной безопасности;

- определение проблемных мест информационной системы;
- анализ производительности системы, полноты ее функциональности, безопасности, целостности ИТ-процессов и других показателей;
- выработка рекомендаций по улучшению информационной системы.

Результатом аудита ИС должно являться описание выявленных несоответствий между структурой ИС и потребностями производства авиационной техники, существующих проблем и рисков развития ИС, а также рекомендации по устранению выявленных проблем с оценкой затрат на выполнение предложенных рекомендаций и планом работы.

Полученные рекомендации по оптимизации и дальнейшему развитию АСУ кладутся в основу для построения стратегии автоматизации предприятия АПК и определения наиболее эффективных путей вложения в ИТ.

Здесь следует отметить, что используемая на многих предприятиях АПК информационная система BAAN (рис. 1), как и другие системы, не является специализированной системой управления авиационно-промышленными предприятиями. *В стандартной АСУ не произведена адаптация к особенностям авиационного предприятия*, в том числе к длительному циклу производства, распределению производства по многим предприятиям группы и другим.

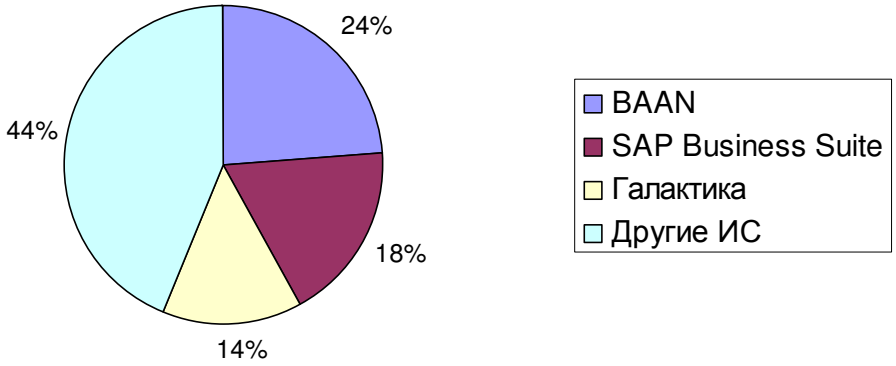

Рис. 1. Примерное соотношение используемых на предприятиях АПК информационных систем управления предприятием (по результатам исследования 18 предприятий АПК)

Кроме того, использование зарубежных систем не позволяет обращаться к разработчикам за дополнительными услугами по доработке, формализации бизнес-процессов предприятия, консультированию по рационализации организационной структуры предприятия АПК и прочим видам ИТ-консалтинга. Это оставляет предприятие АПК один на один с проблемами сопровождения эксплуатируемой системы управления.

В проведенном исследовании **автор выделил две проблемы информатизации управления производством авиационной и ракетно-космической техники**.

Первая проблема заключается в ***обеспечении соответствия структуры и функциональных возможностей АСУ особенностям жизненного цикла продукции предприятия АПК***.

Одним из основных принципов построения АСУ является модульность структуры. Различные функциональные задачи решаются отдельными модулями

системы. В связи с этим структура и состав таких модулей должны соответствовать особенностям жизненного цикла продукции.

Сложность продукции предприятий АПК и длительность предэксплуатационных этапов ее жизненного цикла (концептуального обоснования, проектирования, создания и испытаний) обусловливают многозадачность систем управления и сложность их модульной структуры. Состав основных модулей системы управления авиационно-промышленным предприятием и их соответствие этапам жизненного цикла (ЖЦ) авиационной и ракетно-космической продукции представлены на рис. 2.

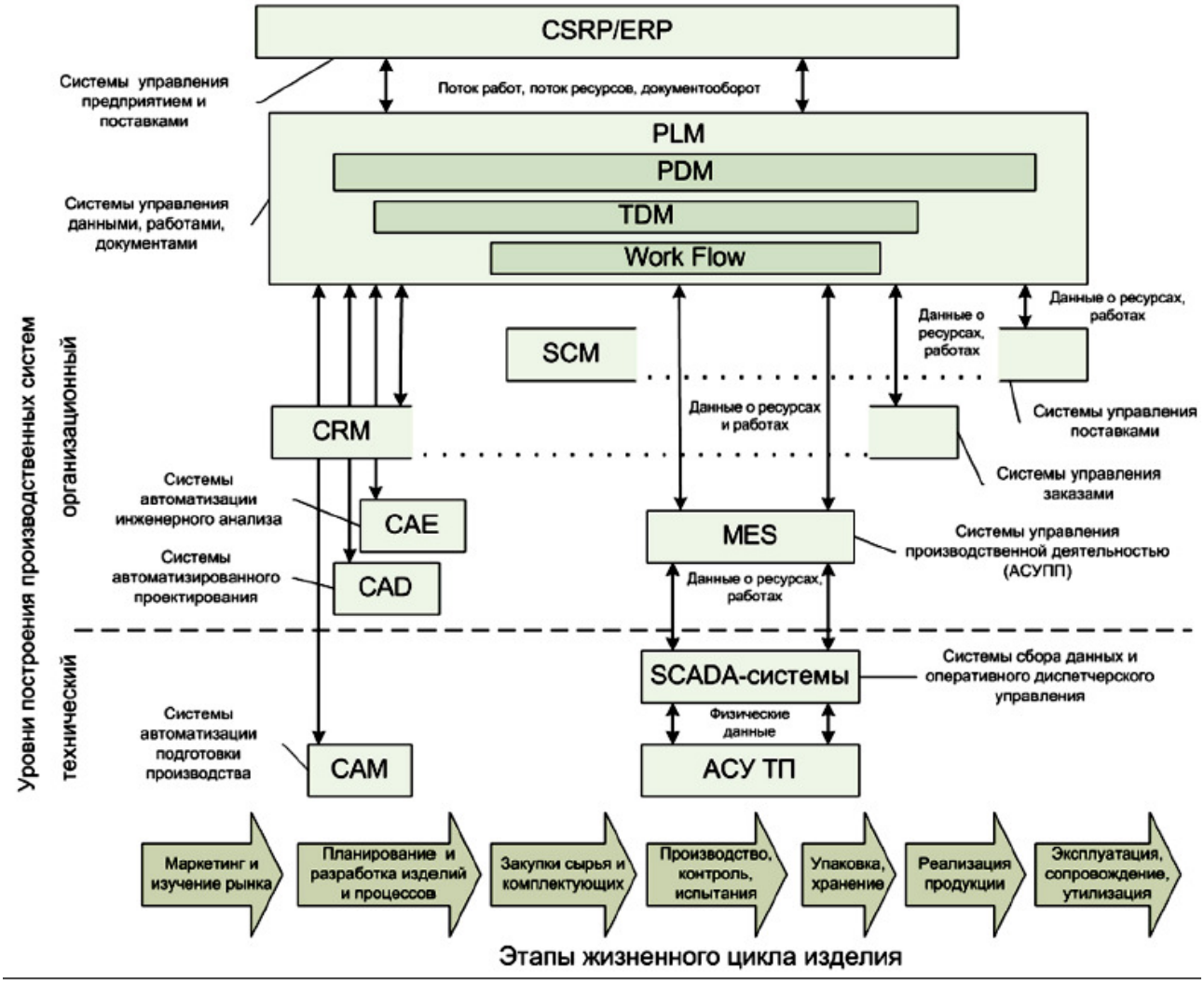

Рис. 2. Соответствие модулей системы управления предприятием АПК этапам жизненного цикла предприятия

Источник: Российская энциклопедия CALS. Авиационно-космическое машиностроение. — Под ред. А.Г. Братухина. — М.: ОАО «НИЦ АСК», 2008.

Соответственно, одной из задач аудита ИС предприятия АПК — специфичной для данной отрасли промышленности — следует поставить анализ соответствия функций модулей ИС процессам и стадиям жизненного цикла продукции. Следует получить ответ на вопрос: в достаточной ли мере и на протяжении ли всего требуемого периода осуществляется поддержка CALS-технологиями процессов и стадий ЖЦ авиационной продукции.

При этом ***предлагается рассматривать понятие жизненного цикла в двух аспектах***: как в отечественной методологии, подразумевающей *поэтапную структуризацию жизненного цикла* (в том числе, по ГОСТ 34.601-90), так и в зарубежной методологии, рассматривающей *жизненный цикл как совокупность основных, вспомогательных и организационных процессов*, распределенных во времени и частично взаимно параллельных (в том числе, стандарт ISO/IEC 12207:1995).

Вторая проблема заключается в ***обеспечении совместимости АСУ различных предприятий, входящих в состав кооперации*** по разработке и созданию авиационной и ракетно-космической техники.

Сложность продукции предприятии АПК и распределенный характер процессов проектирования и производства авиационной техники обусловливают

потребность в коммуникации многих участников этих процессов. В ходе проектирования и создания продукции происходит многократный переход проектной документации, сведений о производимой продукции и ее комплектующих от одного участника процесса к другим. Это вызывает *проблему совместимости различных информационных систем и их сведения в единую информационную среду проектирования и производства конечного продукта*.

В качестве примера можно привести производственную кооперацию «ОКБ Сухого» с другими разработчиками и производителями в рамках создания авиационной продукции (рис. 3). Можно видеть, что связь между системами осуществляется путем экспорта-импорта данных об изделии и процессах его проектирования и создания. Для того чтобы эти процессы происходили оперативно и передаваемая информация отображалась корректно и могла быть использована в дальнейшем, ***в ходе аудита информационной системы следует дать заключение о сопоставимости системы управления аудируемого предприятия с АСУ предприятий-смежников.***

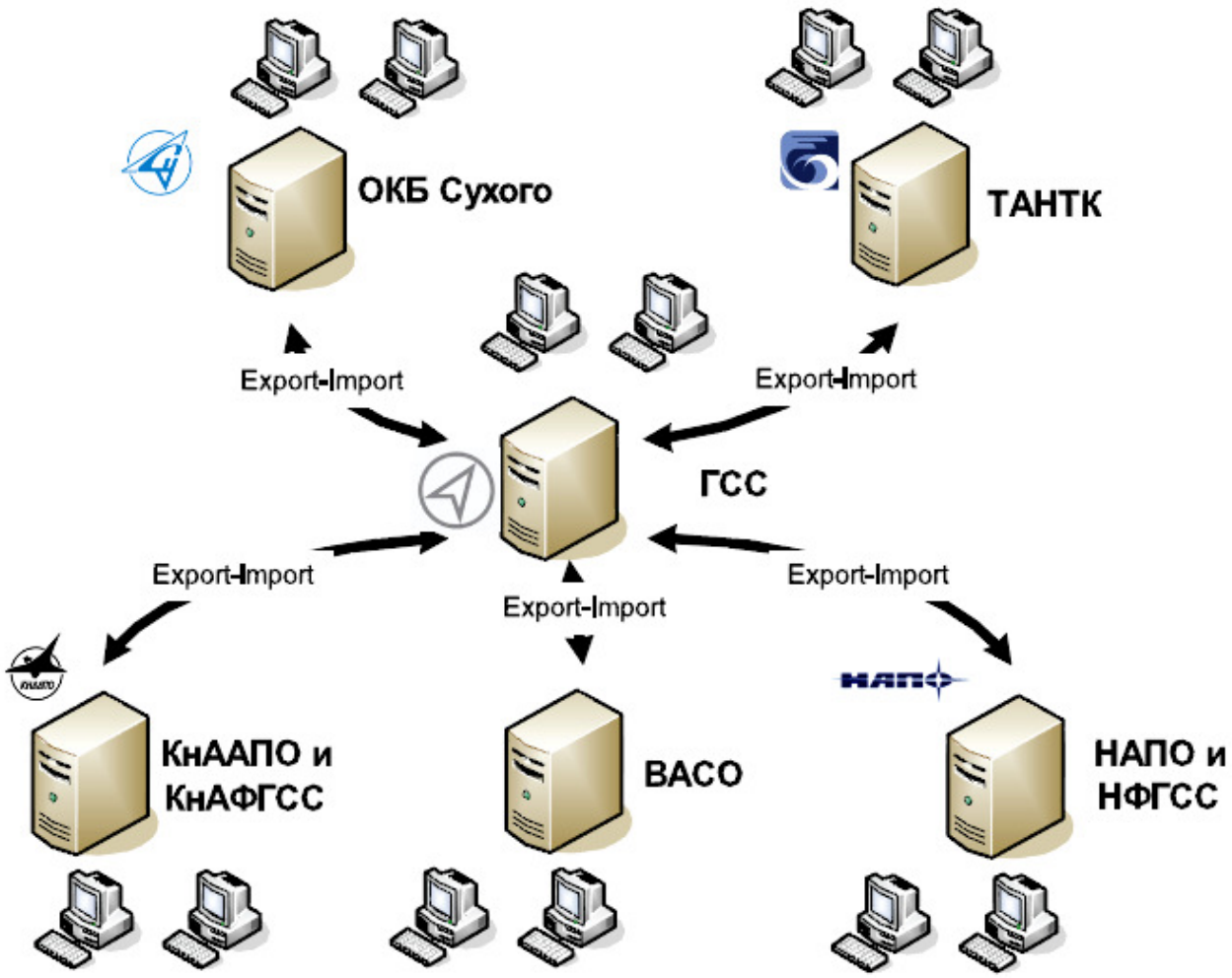

Рис. 3. Схема информационного взаимодействия АСУ «ОКБ Сухого» с системами смежных предприятий кооперации

Источник: Российская энциклопедия CALS. Авиационно-космическое машиностроение. — Под ред. А.Г. Братухина. — М.: ОАО «НИЦ АСК», 2008.

Аудит технологической инфраструктуры АСУ

Под технологической инфраструктурой понимается совокупность технологических платформ, аппаратно-программных комплексов, сетей и средств коммуникации, входящих в состав системы управления предприятием [5].

Аудит технологической инфраструктуры необходим организациям с высокой зависимостью производства от информационных технологий, к каковым в первую очередь относятся авиационные промышленные предприятия, конструкторские бюро и научные организации. Кроме того, ***в рамках производимого в настоящее время на предприятиях АПК переоснащения существующей материально-технической базы также следует пересмотреть и провести модернизацию технологической инфраструктуры***.

По мнению автора, ***этапы проведения технологического аудита должны включать***:

1. Предварительный анализ объекта аудита:

- изучение документации по технологической инфраструктуре;
- согласование графика проведения работ;
- разработка и согласование методики сбора данных и проведения измерений;
- получение данных о функционировании инфраструктуры;
- изучение нормативно-распорядительных документов в области ИТ и защиты информации.

2. Обследование и тестовые испытания функционирования технологической инфраструктуры в соответствии с методикой аудита информационных технологий, разработанной и согласованной на предыдущем этапе:

- документирование технологической инфраструктуры;
- проведение измерений;

- оценка нагрузок, существующих и прогнозируемых узких мест, степени их влияния на функционирование оборудования и технологической инфраструктуры.

3. Обработка результатов и комплексный анализ собранной информации, определение степени соответствия инфраструктуры требованиям обеспечения управления проектированием и производством авиационной техники (в зависимости от типа рассматриваемого предприятия АПК):

- комплексный анализ собранной информации, выявление тенденций;
- определение степени соответствия инфраструктуры требованиям и специфике деятельности авиастроительного предприятия;
- выработка рекомендаций по оптимизации инфраструктуры и предупреждению кризисных ситуаций в технологической инфраструктуре.

По результатам аудита технологической инфраструктуры должны быть сформированы:

- актуализированная документация по технологической инфраструктуре;
- отчёт о текущем состоянии технологической инфраструктуры, в т.ч. данные о существующих технологических проблемах;
- заключение о соответствии технологической инфраструктуры требованиям и специфике авиационного предприятия;
- рекомендации по решению существующих проблем, включая технико-коммерческие предложения по реорганизации и модернизации технологической инфраструктуры;

- требования к смежным системам;
- рекомендации по форме хранения и актуализации результатов аудита.

В большинстве случаев технологическая инфраструктура предприятий АПК слаборазвита, характеризуется использованием устаревшей техники и оборудования. Это объясняется крайне низкими затратами авиационно-промышленных предприятий на капитальные вложения и материальное переоснащение.

Текущий объем финансирования покрывает только 45–65% общей потребности в финансировании технического развития предприятия, причем эта доля снижается по мере старения технологической базы. Процент износа машин и оборудования на ОАО «МКБ «Факел» составляет около 80%, зданий и сооружений – 55%; процент износа на ОАО «НАЗ «Сокол»: здания – 40%, сооружения – 65%, машины и оборудование – 70%, инвентарь – 85%. Согласно инвестиционной политике ОАО «ОАК», основными объектами вложения средств в 2007-2015 годах являются переход к проектированию, подготовке производства и производству на основе информационных технологий, технологическое перевооружение под проведение НИОКР и производство в новых секторах рынка (например, беспилотных системах).

В соответствии с Государственной программой Российской Федерации «Развитие авиационной промышленности» на 2013-2025 годы планируется увеличение объемов инвестиций. Из 1 204 671 млн. руб., планируемых к расходованию за счет средств федерального бюджета, большая часть будет вложена в предприятия АПК уже в ближайшие 5 лет: 2013 г. – 78 304 млн. руб., 2014 г. – 107

027 млн. руб., 2015 г. – 123 520 млн. руб., 2016 г. – 156 393 млн. руб., 2017 г. – 166 861 млн. руб. [6]

Это должно привести к росту технологичности производства, в том числе обеспечению его современными информационными системами и качественной ИТ-инфраструктурой.

Аудит информационной безопасности

В настоящее время серьезной ***проблемой для промышленных предприятий оборонного комплекса, в том числе АПК, является уязвимость систем управления предприятием для различных угроз*** целостности, конфиденциальности и доступности информации. В современных условиях растущей информатизации управления экономическими объектами именно защита информации как основы для принятия управленческих решений является первостепенной задачей при совершенствовании систем управления, а построение надежной системы информационной безопасности невозможно без предварительного аудита существующих средств защиты информации и самой архитектуры информационной системы на предмет выявления возможных каналов утечки информации, угроз ее порчи и потери. Это обусловливает актуальность процедур аудита информационной безопасности в системах управления экономическими объектами.

Аудит информационной безопасности системы управления авиастроительным предприятием должен охватывать следующие направления:

- аудит сетевой безопасности;

- аудит безопасности технических компонентов системы [6].

Важность сетевой безопасности для предприятий АПК обуславливается не только секретностью передаваемой информации, но и разобщенностью предприятий–разработчиков и производителей авиационной техники в силу особенностей производственного цикла, кооперации, сложности продукции авиастроения и организации самого АПК.

Аудит сетевой безопасности (сетевой аудит) основывается на тестовом несанкционированном проникновении в информационную систему. Целью сетевого аудита является выявление слабых мест в системе безопасности сетевого режима работы информационной системы (ее сетевых компонентов).

Его проведение должно включать следующие этапы.

1. Предварительный сбор информации об информационной системе из средств открытого доступа, например, официальных Интернет-ресурсов разработчиков используемой на предприятии АСУ, публикаций в прессе. В ходе обследования требуется собрать сведения о:

- топологии системы;
- типах средств администрирования системы;
- адресации в системе (IP-адреса, имена пользователей);
- сетевых протоколах и межсетевых экранах;
- механизмах аутентификации пользователей системы.

2. Получение информации из контактов с пользователями системы без использования технических средств.

3. Прослушивание серверов DNS, используемых в системе.

4. Определение топологии сети на базе имеющейся информации об IP-адресах и именах ПК с использованием специальных программных средств для отслеживания маршрутов, сканирования портов (выявление открытых портов), определения активных сетевых служб.

5. Анализ уязвимости парольной подсистемы в виде попыток вскрытия паролей с целью выявления слабых паролей.

6. Сокрытие следов проводившихся попыток вскрытия системы (удаление записей, связанных с осуществлённым проникновением, из системных журналов).

7. Анализ безопасности модемных соединений в виде прозвона телефонных номеров из диапазона исследуемой организации с целью выявления несанкционированных соединений.

8. Анализ безопасности сетевой инфраструктуры на предмет возможности подключения прослушивающих устройств (в первую очередь актуально для кабельных систем).

По результатам проведения аудита сетевой безопасности нужно сформировать заключение о подверженности сетевых компонентов ИС и системы в целом различным типам сетевых атак и предложить меры по снижению уязвимости системы.

Среди типов сетевых атак нужно предусмотреть возможность наиболее распространенных из них (рис. 4) [7].

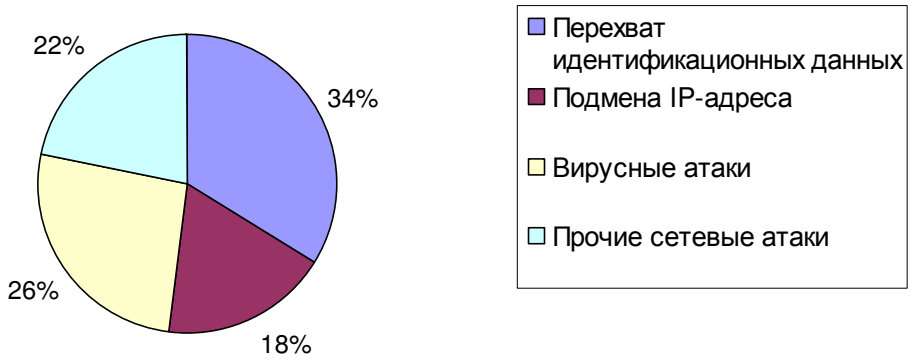

Рис. 4. Распространенность типов сетевых атак с целью кражи либо порчи информации

Источник: Kaspersky Security Bulletin 2011. Развитие угроз в 2011 году

Перехват имен пользователей (логинов) и паролей (сниффинг) — один из самых распространенных видов угроз информационной безопасности. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам. Перехват осуществляется специальной программой — снифферо́м, перехватывающей все сетевые пакеты, которые передаются через определенный домен.

Для снижения уязвимости системы для перехвата (сниффинга) пакетов данных можно предложить такие меры:

- Использование одноразовых паролей, основанное на комбинации постоянного значения (например, вводимого кода пользователя) и переменного уникального одномоментного однократного пароля.
- Временная коммутация.

- Анти-снифферы — специальные аппаратные или программные средства, распознающие снифферы, работающие в сети.
- Шифрование [8, 9, 10].

Вторым типом распространенных угроз является использование доверенного IP-адреса злоумышленником от лица санкционированного пользователя (IP-спуфинг). Оно может осуществляться как просто для передачи в систему ложной или вредоносной информации, так и для извлечения информации из системы (это уже более сложный для реализации вариант).

Для борьбы с IP-спуфингом можно использовать:

- Системы контроля и управления доступом (СКУД).
- Дополнительные методы аутентификации – например, двухфакторная аутентификация с использованием одноразовых паролей [10].

Атаки на пароли системы могут быть произведены как описанными выше методами, так и простым перебором паролей либо с помощью вирусов типа «троянского коня». Для повышения защищенности паролей можно использовать:

- специальные программы определения степени защищенности пароля;
- прикладные программы, шифрующие список паролей, который можно хранить в карманном компьютере.

Атаки на уровне приложений за счет использования известных слабостей серверного программного обеспечения, позволяют получить доступ к компьютеру от имени пользователя, работающего с приложением (обычно привилегированного администратора с правами системного доступа).

Чтобы снизить уязвимость системы для атак подобного типа, можно использовать:

- просмотр лог-файлов операционных систем и сетевых лог-файлов и их анализ с помощью специальных аналитических приложений;
- использование самых свежих версий операционных систем и приложений и самых последних коррекционных модулей;
- использование систем распознавания атак (IDS), использующих профили (сигнатуры) стандартных атак или типов атак [10, 11].

Одной из самых вредоносных для системы атак является отказ в доступе, когда в результате действий злоумышленников происходит блокирование системы для нормальной работы пользователей. Для борьбы с этим типом атак можно использовать:

- функции анти-спуфинга — включение фильтрации подключающихся адресов;
- функции анти-DoS — эти функции уменьшают число полуоткрытых каналов в любой момент времени;
- ограничение объема трафика [10, 11].

Сетевая разведка, переадресация портов и другие виды сетевых атак на информационную систему также являются важными аспектами, которые *необходимо учитывать при формировании рекомендаций по повышению защищенности ИС в ходе аудита сетевой безопасности* [12].

Вторая часть аудита информационной безопасности — **аудит безопасности технических компонентов системы —** должен включать:

1. анализ соответствия технических компонентов системы нормативным срокам работы устройств;
2. выявление критических для работоспособности системы узлов и анализ возможностей их дублирования;
3. разработку резервной системы для экстренных ситуаций;
4. формирование рекомендаций по повышению степени безопасности технических компонентов системы.

На предприятиях АПК в силу упоминавшейся выше недостаточности капиталовложений в технологическую инфраструктуру и техническое обеспечение отставание общего технологического уровня авиационно-промышленного предприятия проявляется, в первую очередь, в вопросах информационных технологий, в том числе информационной безопасности и морального устаревания используемых программных средств и вычислительной техники. Использование предприятиями АПК устаревшего программного обеспечения несет угрозу взлома и компрометации информации современными средствами, а устаревшей вычислительной техники — угрозу отказов в работе, а также недостаточную по сравнению с современной техникой возможность резервирования и восстановления системной информации.

Аудит информационной службы авиационного предприятия

Аудит информационной службы предприятия — это независимая оценка организации и автоматизации процессов работы ИТ-службы и выработка

рекомендаций по повышению качества ее работы и снижению затрат на эксплуатацию [13].

Для объективного аудита ИТ-подразделения необходимо приглашать сторонних специалистов. Но ***для предприятий АПК эта задача осложняется секретностью многих данных, хранящихся в АСУ***, поэтому выбор привлекаемых специалистов должен быть произведен с высокой степенью ответственности.

В задачи приглашенных специалистов по аудиту информационной службы предприятия АПК должны войти следующие мероприятия:

- оценка квалификации персонала информационной службы авиастроительного предприятия;
- оценка современности используемого оборудования и программного обеспечения;
- анализ эффективности распределения должностных обязанностей между специалистами информационной службы;
- анализ области ответственности ИТ-службы и круга решаемых ею вопросов;

Отдельным важным этапом аудита ИТ-подразделения должен быть анализ целесообразности ***использования аутсорсинга для оказания услуг по сопровождению работы системы управления предприятия АПК***. Для этого следует произвести классификацию услуг, предоставляемых информационной службой в отношении прочих подразделений организации.

Услуги, предоставляемые информационной службой предприятия, нужно разделить на следующие две группы:

- потенциально инсорсинг — группа ИТ-сервисов, выполнение которых должно обязательно обеспечиваться внутренними ИТ-подразделениями предприятия (в первую очередь, связанные с обработкой секретной информации);
- потенциально аутсорсинг — группа ИТ-услуг, которая может быть потенциально передана внешним исполнителям — провайдерам ИТ-услуг.

Выделяемые потенциально в аутсорсинг ИТ-сервисы должны быть доступны на открытом рынке с требуемыми характеристиками по уровню качества и стоимости. Критерием эффективности предлагаемых на рынке ИТ-услуг следует считать снижение эксплуатационных расходов либо повышение качества при сохранении неизменного уровня расходов.

Основным результатом данной классификации должно являться упорядоченное и структурированное описание задач, которые решаются с использованием информационных ресурсов. На основании полученных данных следует произвести анализ целесообразности предоставления тех или иных услуг внутренней службой и внешними поставщиками услуг (аутсорсинг). На основании выбора модели предоставления услуг выполняется доработка процессно-организационной структуры предприятия АПК.

В настоящее время на подавляющем большинстве предприятий АПК аутсорсинг информационных услуг полностью отсутствует, все функции выполняются внутренними специалистами, квалификация которых как в силу отсутствия возможностей доступа ко многим современным ИТ, так и в силу низкой оплаты труда и высокого среднего возраста персонала зачастую является недостаточной.

По результатам аудита ИТ-подразделения формулируются рекомендации по развитию информационной службы предприятия и подбору персонала.

В результате аудита ИТ-подразделения должно быть сформировано представление о качестве и производительности информационной службы авиастроительного предприятия, уровне используемых ИТ-сервисов и связанных с текущей организацией процессов рисках.

Текущее состояние организации информационной службы на большинстве предприятий АПК следует признать неудовлетворительным. Оно осталось почти без изменений с тех пор, когда в обязанности информационной службы входило лишь поддержание работоспособности вычислительной техники на предприятии. В настоящее же время эти функции должны быть значительно расширены; к ним следует отнести и разработку ИТ-стратегии предприятия, и мониторинг рынка ИС и ВТ, и формирование технических заданий на разработку профессиональных отраслевых программных продуктов для предприятий АПК, и участие в доработке и сопровождение эксплуатации функционирующих АСУ, и ряд других функций. Таким образом, этот раздел отчета об аудите системы управления предприятием АП может оказаться самым важным для повышения эффективности функционирования ИС предприятия, и при этом наименее затратным в реализации.

Выводы

Значение аудита систем управления любых типов экономических объектов сложно переоценить. Его целью является выявление слабых мест организации информационной системы, которые приводят как к неэффективной работе системы принятия решений, так и к реализации угроз информационной безопасности.

Особенную важность в связи с этим приобретает аудит информационных систем в организациях оборонного сектора экономики, в том числе авиационно-промышленного комплекса. Наукоемкое производство требует обработки и хранения колоссальных объемов информации, справиться с которыми способна только вычислительная система. При этом важнейшей задачей становится обеспечить надежное хранение и оперативную обработку информации. Решению этой задачи и способствует аудит системы управления предприятием АПК.

В статье выявлен ряд специфичных проблем информационных систем управления предприятиями авиационно-промышленного комплекса.

Предложена технология проведения комплексного аудита различных аспектов функционирования системы управления предприятием авиационно-промышленного комплекса, на основе которой в дальнейшем может быть разработана стратегия развития информационных систем и технологий для предприятия АПК.

Библиографический список

1. Об информации, информационных технологиях и о защите информации: Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ.
2. http://www.isaca.org (дата обращения 11.11.2012)
3. http://citforum.ru/consulting (дата обращения 11.11.2012)
4. http://www.methodware.com (дата обращения 10.11.2012)
5. *Олейник А.И., Сизов А.В.* ИТ-Инфраструктура. — М.: Издательство ГУ ВШЭ, 2012. – 134 с.
6. Государственная программа Российской Федерации «Развитие авиационной

промышленности» на 2013-2025 годы : Электронный ресурс (http://www.minpromtorg.gov.ru/ministry/fcp/10, дата обращения 27.11.2012)

7. Kaspersky Security Bulletin 2011. Развитие угроз в 2011 году : Электронный ресурс (http://www.securelist.com, дата обращения 27.11.2012)
8. *Партыка Т.Л., Попов И.И.* Информационная безопасность. — 3-е изд., перераб. и доп. — М.: ФОРУМ, 2008. – 432 с.
9. *Попов В.Б.* Основы информационных и телекоммуникационных технологий. Основы информационной безопасности. Кн. 2 : Учебное пособие. Гриф Ученого совета Института информатизации. — М.: Финансы и статистика, 2005. – 128 с.
10. *Садердинов А. А., Трайнев В.А., Федулов А.А.* Информационная безопасность предприятия: Учебное пособие. — 3-е изд. — М.: Дашков и К", 2006. – 335 с.
11. *Корнеев И.К., Степанов Е.А.* Защита информации в офисе: Учебник. — М.: Проспект, 2007. – 336 с.
12. Обеспечение информационной безопасности бизнеса. Под ред. А.П. Курило. — М.: Альпина Паблишер, 2011. – 392 с.
13. *Гузик С.* Стандарт CobiT. Управление и аудит информационных технологий. Особенности проведения внешнего аудита ИТ : Электронный ресурс (http://citforum.ru/consulting/standart_cobit/article1.1.2003677.html, дата обращения 12.11.2012)
14. Российская энциклопедия CALS. Авиационно-космическое машиностроение. — Под ред. А.Г. Братухина. — М.: ОАО «НИЦ АСК», 2008. – 608 с.