

1. УДК 004.02
2. Обзор существующих подходов по аудиту электронных носителей информации
3. К.И. Салахутдинова (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург)
4. С.А. Арустамов (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург)
5. Основные части тезиса

Введение. Информационная безопасность (ИБ) в бизнесе является одной из его важнейших составляющих наравне с юридической, физической, экономической и организационно-кадровой безопасностью. По статистике в число наиболее вероятных инцидентов ИБ входит нарушение политики ИБ. Так нарушение пользователями требований установленной политики в сфере использования программного обеспечения (ПО), будь то устаревшая версия или не санкционировано установленное ПО, влечет к появлению уязвимости в дальнейшем эксплуатируемой злоумышленником. Такое ПО также может использоваться в целях получения собственной выгоды или являться объектом чужих авторских прав. Особенно стоит отметить важность аудита ПО в навигационных системах, где очень важным является состояние защищенности обрабатываемой информации, ведь исход инцидента ИБ может повлечь за собой большие убытки.

Средства аудита программного обеспечения. В настоящее время множество компаний обращаются к использованию систем управления ИТ-активами (ИТАМ-IT asset management), представляющие собой комплексные решения, нацеленные на физический учёт, финансовый контроль и соблюдение контрактных обязательств, связанных с ИТ-активами, на протяжении всего их жизненного цикла. Здесь под ИТ-активами подразумеваются все аппаратные и программные элементы ИТ-инфраструктуры, обеспечивающие деятельность бизнес-среды.

В свою очередь ИТАМ подразделяется на управление аппаратными активами (НАМ-Hardware Asset Management), охватывающее управление материальными составляющими ИТ-инфраструктуры: пользовательские компьютеры, сервера, телефоны и т.д.; и на управление программными активами (SAM-Software Asset Management), охватывающее управление не материальными составляющими ИТ-инфраструктуры: программное обеспечение, лицензии, версии, конечные точки инсталляции и т.д.

На рынке услуг представлено немало решений, позволяющих идентифицировать программные активы, управлять учетом, а также производить контроль их изменений и др. Из числа наиболее известных программных продуктов можно выделить Microsoft Assessment and Planning Toolkit (без агента), Lansweeper (с/без агента), SAManage (с агентом), AIDA64 Business Edition (с/без агента), Kaspersky Systems Management (с агентом). Большая часть предоставляемой информации собирается посредством следующих встроенных технологий инвентаризации программного, аппаратного окружений и операционной системы: Windows Management Instrumentation, Active Directory (без агента), Domain Services (AD DS), SMS Provider, lshw, dpkg -l и других технологий.

Недостатки такого подхода очевидны. При недостаточном уровне квалифицированности со стороны администратора системы, наличии способностей в сфере компьютерных технологий пользователей автоматизированных систем или при низкоуровневом подходе руководства к подбору кадров появляется возможность внести изменения в конфигурационные данные устанавливаемого программного обеспечения.