А. В. Артамонов
Санкт-Петербургский государственный политехнический университет

ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА DOCUMENTUM

В работе исследуются возможности обработки электронно-цифровой подписи в системе Documentum для решения прикладных задач.

В задачах по автоматизации документооборота одной из частых подзадач является обеспечение работы с электронно-цифровой подписью.

Базовая функциональность Documentum содержит следующие возможности [1, 2]:

• Electronic signature. Изначально применимо только к документам в PDF-формате. Подпись полностью создается Content Server'ом. От пользователя требуется только ввести пароль;

• Digital signature. Основное средство расширения стандартной функциональности. Подпись полностью создается клиентским по отношению к Content Server'у приложением. Content Server обеспечивает специализированное хранение и выполняет аудит;

• Simple signoffs. Простейшее средство подписания. Content Server просто добавляет запись в журнал аудита с данными о том, кто и когда подписал.

В ходе исследования были выявлены следующие недостатки:

• не предоставляется возможность реализации «квалифицированной цифровой подписи», отвечающей законодательству Российской Федерации;

• применяется только для документов в PDF-формате;

• не учитываются атрибуты документов;

• нет механизма экспорта/импорта для подписанных документов;

• требуется лицензия Trusted Content Services;

• не поддерживается на платформах Linux и HP Itanium.

Результаты исследования показали, что для устранения недостатков необходима собственная реализация интерфейса Digital Signature. Разрабатывается архитектура такой подсистемы.

СПИСОК ЛИТЕРАТУРЫ:

1. Documentum Content Server Fundamentals 5.3, EMC Corporation.
2. DFC Development Guide 5.3, EMC Corporation.

А. Н. Атаманов
Московский инженерно-физический институт (государственный университет)

ДИНАМИЧЕСКАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматриваются проблемы получения адекватной информации об уровне информационных рисков в условиях постоянно развивающейся информационной среды. Предлагается комплексный

подход к автоматизации процессов анализа рисков и оценки эффективности систем защиты информации с целью получения оптимальных решений по защите информационных систем.

На сегодняшний день очевиден существенный разрыв между уровнем развития информационных технологий и существующей нормативно-правовой базой, а также большинством формальных систем и критериев оценки эффективности систем защиты информации в сложных информационных системах. Все большую проблему начинают представлять угрозы, связанные со сложностями формализации задачи обеспечения информационной безопасности. Именно эти проблемы возникают при попытке создания эффективных антивирусов или систем обнаружения вторжений и сетевых атак. В связи с этим особую актуальность приобретает аудит информационной безопасности, включающий в себя комплексный анализ угроз и рисков и предполагающий помимо формальных и объективных проверок параметров информационной системы также вынесение обоснованного субъективного суждения аудитора или группы аудиторов относительно эффективности системы защиты информации и возможных угроз.

Непрерывный аудит определяется как методология или среда, позволяющая внутреннему или внешнему аудитору выносить суждения по значимым вопросам, основываясь на серии созданных одновременно или с небольшим промежутком времени отчетов. Возможность сообщать о снижении эффективности системы защиты в реальном (или максимально близком к реальному) времени может дать существенные преимущества.

При использовании традиционной модели между окончанием исследования системы и выпуском отчета по результатам аудита зачастую проходит много времени, что может значительно уменьшить ценность данных аудита. Это, в свою очередь, способно (в случае аудита информационной безопасности) привести к нарушению конфиденциальности, целостности или доступности защищаемой информации.

На сегодняшний день, основываясь на современных методиках и достижениях в области систем анализа, баз данных, интеллектуальных агентов и др., возможно создать автоматизированную систему, объедяющую в себе инструменты для идентификации активов, проведения базовых опросов, количественного анализа рисков, для которых уже накоплен достаточный объем статистики или существуют экспертные оценки, систему создания и регулярного вычисления метрик безопасности на основе данных мониторинга, систем обнаружения вторжений и сетевых аномалий и др. Таким образом, возможно создание инструмента, позволяющего аудитору облегчить выполнение многих процессов при изучении системы и составлении отчетов, что, в свою очередь, может существенно уменьшить время, затрачиваемое на составление отчетов. Помимо этого, автоматизировав процесс учета угроз, связанных с появлением новых уязвимостей в типовом ПО, возможно решить задачу непрерывного аудита — создать среду, позволяющую аудитору формировать отчеты по состоянию информационной безопасности, основываясь на серии отчетов, составленных за короткий промежуток времени в полуавтоматическом режиме.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO/IEC 17799:2005. Code of practice for Information Security Management. Женева: ISO, 2005.
2. BSI/IT Baseline Protection Manual. Берлин: Bundesamt fьr Sicherheit in der Informationstechnik, 2001.
3. Model Curricula for Information Systems Auditing at the Undergraduate and Graduate Level. Illinois: ISACA, 2000.
4. *Симонов С. В.* Анализ рисков, управление рисками // Jet Info. 2003. № 1.
5. *Астахов А.* Аудит безопасности информационных систем. URL: http://www.isaca.ru (2002).
6. *Петренко С. А.* Аудит информационной безопасности корпоративных систем Internet/Inranet // Системы безопасности. 2002. № 10–11 (41).

7. Standards Board of ISACA. Continuous Auditing: Is It Fantasy Or Reality. URL: http://www.isaca.org/Content/ContentGroups/Journal1/20023/Continuous_Auditing_Is_It_Fantasy_or_Reality_.htm (16.01.2007).
8. *Scarfone K., Mell P.* Nist Special Publication 800-94, 2007: «Guide to Intrusion Detection and Prevention Systems».
9. *Zurutuza U., Uribeetxeberria R.* A methodology for continuous computer security auditing. Mondragon: Mondragon University Press, 2004.
10. *Searcy D., Woodroof B.* Continuous Auditing: Leveraging Technology // The CPA Journal. 2003. № 5.
11. CORAS project. URL: http://coras.sourceforge.net/ (21.01.2007).
12. AS/NZS 4360. Risk Management. Канберра: Australian Standard, 2006.

А. В. Бабаш
Российский государственный социальный университет, Москва

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИПТОГРАФИИ

Указываются способы построения приближенных моделей шифрующих автоматов с целью построения методов их криптоанализа.

Одна из проблем криптоанализа и синтеза шифров состоит в построении «удачных» приближенных моделей функционирования шифрсистем. Удачная модель строится исходя из заданной шифрсистемы-оригинала и определяется условиями и целями задачи. Например, целью может быть определение ключа по заданной информации или открытого текста. Удачность модели трактуется как возможность нахождения решения поставленной задачи сначала для разработанной модели системы и возможность эффективного использования этой информации для решения начальной задачи для оригинала. Простейшим примером удачной модели является модель гомоморфного образа шифрующего автомата с меньшим числом состояний, чем у оригинала. Перечислим основные идеи подхода.

1. Обобщение гомоморфизма шифрующих автоматов путем замены отображений в определении гомоморфизма на а) бинарные отношения и б) автоматные отображения.

2. Использование следствий функционирования шифрсистемы. Например, использовать не сам известный шифртекст, а значение некоторой функции от него.

3. Использование в качестве моделей «слабых» шифрующих автоматов, близких по расстоянию Хэмминга к табличному заданию оригинала. Слабого автомата в том смысле, что нахождение решения исходной задачи для него не слишком трудоемко и это решение с приемлемой вероятностью является и решением для оригинала.

4. Использование в качестве модели «слабых» шифрующих автоматов, выходные последовательности которых близки в метрике Хемминга к выходным последовательностям оригинала.

В докладе конкретизируются данные идеи построения приближенных моделей автомата в терминах теории автоматов. Некоторые из основных результатов представлены в работах списка литературы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Бабаш А. В.* Автоматные отображения слов, размножающие искажения в метриках Хемминга и Левенштейна не более, чем в K раз // Дискретная математика. 2002. Том 14. Вып. 3.