процессов с административными полномочиями кроме верифицированных и будет исключен запуск иных программ с повышенными привилегиями.

Рассмотрим реализацию механизма делегирования прав подробнее. Для изменения прав процесса используется либо хранимый с правами LocalSystem пароль владельца, предоставляемый им самим при регистрации программы в службе и используемый в дальнейшем в системном вызове CreateProcessWithLogonW, либо перехват системных вызовов с использованием внедрения DLL в процесс [2]. В первом случае для запуска процесса требуется программа-посредник, также входящая в комплект программного комплекса, которая выполняется с правами пользователя-клиента и передает запрос службе. Служба проверяет целостность программы-посредника и обрабатывает запрос на основе таблицы предоставляемых полномочий, а затем запускает запрошенную программу с заданными в таблице полномочиями. В этом случае возможно использование псевдонимов программ. Одна и та же программа может иметь несколько псевдонимов для запуска с разными привилегиями. Во втором случае программа-посредник внедряется в системную оболочку, осуществляя перехват системного вызова CreateProcess. Перехват осуществляется подменой функции CreateProcess специальной реализацией, которая передает запрос системной службе. В случае неудачного или ошибочного запроса программа осуществляет вызов процесса, используя штатную версию CreateProcess. Целостность запускаемых программ проверяется с помощью подсчета хэш-сумм и времени последнего изменения. Поэтому при изменении исполняемого файла владелец должен переустановить программу. Следует отметить, что права устанавливать программы, изменяющие полномочия, могут быть предоставлены не всем пользователям, а пользователь, устанавливающий программу, может наделить ее только своими правами.

Таким образом, реализация данного механизма позволяет локально без использования ActiveDirectory реализовать делегирование административных полномочий и предоставить право избирательного делегирования своих полномочий непривилегированным пользователям, что повышает безопасность системы и позволяет снизить нагрузку на администратора системы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Дудаков Н. С., Пирогов Н. Е., Шумилов Ю. Ю.* Кроссплатформенная система безопасного управления хранением динамических данных // Безопасность информационных технологий. 2009. № 3. С. 12–15.
2. *Рихтер Дж., Назар К.* Windows via C++. Программирование на языке Visual C++ / Пер. с англ. М.: Издательство «Русская Редакция»; СПб.: Питер, 2008. – 896 с.

С. Д. Кулик, К. И. Ткаченко, И. А. Лукьянов

ИДЕНТИФИКАЦИЯ ИСПОЛНИТЕЛЯ ТЕКСТОВ ПО ЧАСТОТНО-ГРАММАТИЧЕСКИМ ХАРАКТЕРИСТИКАМ И СИНТАКСИЧЕСКИМ ОСОБЕННОСТЯМ

При разработке систем, являющихся объектами информационной защиты, встают задачи идентификации субъектов — пользователей данных систем (как авторизованных, так и пытающихся получить несанкционированный доступ). Предлагаемый в данной работе подход позволяет получить дополнительные сведения, необходимые для поддержки процесса принятия решения о тождественности субъектов (известного и неизвестного) по разнородным идентифицирующим факторам.

В настоящее время ведется разработка алгоритма, реализующего предложенный подход и полностью обеспечивающего принятие решения в заданном пространстве признаков. Также проводятся следующие исследования:

1. Исследование степени влияния объема обучающей выборки на ошибки идентификации.

2. Исследование значимости выделенных признаков при принятии решения о тождественности субъектов.

3. Выделение подпространства достаточных признаков, инвариантных при идентификации с помощью предложенного подхода.

4. Исследование ошибок различных методов и их комбинаций при решении задачи.

В настоящее время собрана выборка из свыше 4000 текстовых документов различных авторов, реализованы алгоритмы машинного обучения (SVM, Random Forest, ДСМ-метод, а также основанные на искусственных нейронных сетях) и алгоритмы лингвистического анализа (морфологический анализ и основанные на методе N-грамм).

Предлагаемый подход подразумевает выполнение нескольких этапов:

1. Грамматический анализ текстовых документов.

2. Построение биграммной и триграммной модели текстовых документов.

3. Подсчет частотных характеристик.

4. Обучение на выборке.

5. Анализ текстовых документов идентифицируемого исполнителя на основании результатов этапов 1–4.

Первый этап подразумевает приписывание признаков (таких как часть речи, род, число, падеж и т. д.) каждому слову текстового документа. Математическое описание метода, применяемого на первом этапе, дано в работе [1]. На втором этапе выделяются все пары, а затем — все тройки идущих подряд слов текстового документа в рамках каждого его предложения. При этом в записи выделяемых пар и троек конкретные словоформы заменяются соответствующими им грамматическими признаками, получаемыми по результатам этапа 1 (грамматическая абстракция). На третьем этапе вычисляются следующие выделенные характеристики:

1. Средняя длина предложений.

2. Средняя длина слов.

3. Частоты употребления частей речи в текстовом документе.

4. Частоты употребления более конкретных форм (например, в отличие от п. 3, глагол совершенного вида и т. д.).

5. Частота употребления конкретных слов, в том числе служебных (предлоги, союзы, частицы и т. д.).

6. Среднее количество употребления частей речи в предложении.

7. Частота употребления всех биграмм и триграмм в грамматической абстракции.

На четвертом этапе алгоритм машинного обучения (или комбинация нескольких алгоритмов) обучается на признаках, вычисленных на этапе 3 для каждого из текстовых документов с известным исполнителем. На этапе 5 на вход подается текстовый документ (или несколько документов), исполнителя которого необходимо идентифицировать. На выходе получается решение о принадлежности данного текстового документа данному исполнителю и дается вероятностная оценка уверенности в этом решении.

Выводы

Предложенный подход позволяет увеличить количество аналитической информации, используемой при принятии решения о тождественности субъектов (известного и неизвестного) по разнородным идентифицирующим факторам.

Если провести обучение обособленно для различных известных исполнителей, то подход позволяет установить, какому из M исполнителей наиболее вероятно принадлежит анализируемый текст (или тексты).

СПИСОК ЛИТЕРАТУРЫ:

1. *Кулик С. Д., Ткаченко К. И., Лукьянов И.* А. Методы морфологического анализа слов русского языка в системе фактографического вопросно-ответного поиска по законодательной и нормативной документации // Сборник трудов XIX Международной конференции «Информатизация и информационная безопасность правоохранительных органов», 25–26 мая 2010 г. М.: Академия управления МВД России, 2010. С. 377–381.

А. И. Лучник

СРАВНЕНИЕ КОМПОНЕНТОВ, РЕАЛИЗУЮЩИХ УДОСТОВЕРЯЮЩИЙ ЦЕНТР, В WINDOWS SERVER 2003 И WINDOWS SERVER 2008

Сертификаты нужны для надежной аутентификации, создания SSL-соединений, отправки S/MIME-сообщений и других действий, направленных на обеспечение безопасности. С каждым годом использование сертификатов растет. Для того чтобы удовлетворять новым требованиям, Microsoft переработала службу Certificate Services. В Windows Server 2008 службы сертификации теперь относятся к службам Active Directory. В состав роли Active Directory Certificate Services (AD CS) в Windows Server 2008 R2 входит шесть компонентов вместо четырех в Windows Server 2008 и двух в Windows Server 2003.

Основные изменения в AD CS Windows Server 2008 R2 затрагивают поддержку стандартов PKI [1], новых механизмов аутентификации [2, 3] и возможность запрашивать сертификаты в гетерогенных и территориально разнесенных средах [4]. Появилась возможность запрашивать сертификаты для сетевых устройств и для пользователей, находящихся в другом лесу или за пределами сети организации. Добавилась поддержка протокола OCSP. Были полностью переписаны библиотеки Crypto API и XEnroll.dll.

Широта распространения сертификатов приводит к необходимости реализации стандартных и гибких механизмов взаимодействия между разными информационными системами, а также к обеспечению поддержки современных надежных криптографических алгоритмов и вариантов многофакторной аутентификации.

СПИСОК ЛИТЕРАТУРЫ:

1. Стандарты PKI. URL: http://www.oasis-pki.org/resources/techstandards/.
2. Windows Biometric Framework. URL: http://www.microsoft.com/whdc/device/biometric/default.mspx.
3. Документация по Active Directory Certificate Services. URL: http://technet.microsoft.com/en-us/library/cc770357(WS.10).aspx.
4. *Kinder C., Radutskiy A., Corey S.* Cross-forest Certificate Enrollment with Windows Server 2008 R2. URL: http://www.microsoft.com/downloads/.