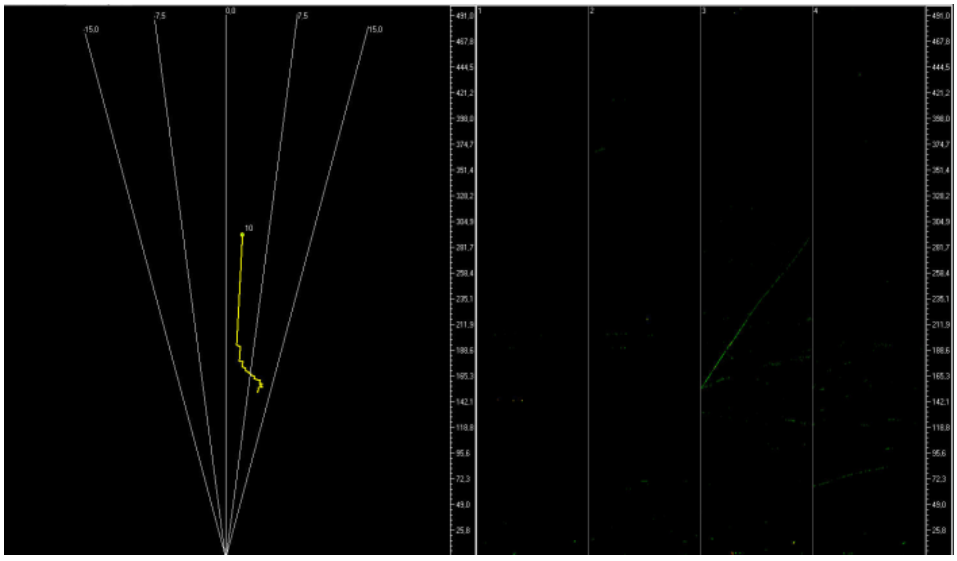

Рис. 6. Результаты работы алгоритма обнаружения движущихся объектов по эхосигналу

Алгоритм не требует большой вычислительной мощности центрального процессора и способен работать в режиме реального времени на существующих персональных компьютерах среднего ценового диапазона.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бакутин П.А., Жулина Ю.В., Иванчук Н.А.* Обнаружение движущихся объектов/ Под ред. П.А. Бакута. – М.: Сов. Радио, 1980. – 288 с.
2. *Деев В.В., Забродин Ю.М., Пахомов А.П. и др*. Анализ информации оператором-гидроакустиком/ – Л.: Судостроение, 1989. – 192 с.
3. Гидроакустическая энциклопедия/ Под общ. ред. В.И. Тимошенко. Ред. кол. Л.М. Бреховских, Н.А. Дубровский, О.В. Руденко и др. – Таганрог: Издательство ТРТУ, 1999. – 788 с.

УДК 004.056

Е.Ф. Стукалина, С.А. Ижболдин, К.М. Калашников

ОСНОВНЫЕ ВОПРОСЫ БЕЗОПАСНОСТИ СИСТЕМЫ 1С:ПРЕДПРИЯТИЕ 8.0

1С:Предприятие является самой распространённой учетной системой в России, но несмотря на это, до версии 8, её разработчики уделяли крайне мало внимания вопросам безопасности. В основном, конечно, это диктовалось ценовой нишей продукта и ориентацией на малые предприятия, где отсутствуют квалифицированные ИТ-специалисты, и возможная стоимость развёртывания и поддержки защищённой системы была бы непозволительно дорога для предприятия. С выпуском версии 8 акценты должны были поменяться: стоимость решений значительно возросла, система стала значительно более масштабируемой и гибкой – требования значительно изменились. Стала ли система достаточно надёжной и защищённой – это вопрос очень индивидуальный. Основная информационная система современного предприятия должна удовлетворять, как минимум, следующим требованиям безопасности:

- достаточно низкая вероятность сбоя системы по внутренним причинам;
- надёжная авторизация пользователей и защита данных от некорректных действий;
- эффективная система назначения прав пользователей;
- оперативная система резервного копирования и восстановления в случае сбоя.

Удовлетворяют ли решения на базе 1С:Предприятия 8.0 таким требованиям? Однозначного ответа не существует. Несмотря на значительные изменения в системе управления доступом осталось достаточно, много нерешённых вопросов. В зависимости от того, как разработана и настроена система, все эти требования могут не выполняться или выполняться в достаточной для данного внедрения мере, однако стоит обратить внимание (и это существенное следствие "юности" платформы), что для полного выполнения перечисленных условий приходится прикладывать поистине титанические усилия.

1С:Предприятие 8.0 поставляется в двух вариантах: файловый и клиент-серверный. Файловый вариант нельзя считать обеспечивающим информационную безопасность системы по следующим причинам:

- данные и конфигурация хранятся в файле, доступном на чтение и запись всем пользователям системы;
- авторизация системы очень легко обходится;
- целостность системы обеспечивается только ядром клиентской части.

В клиент-серверном варианте для хранения информации используется MS SQL Server, что обеспечивает:

- более надёжное хранение данных;
- изоляцию файлов от прямого доступа;
- более совершенные механизмы транзакций и блокировок.

Условно структуру клиент-серверного варианта 1С:Предприятие 8.0 можно представить на рис. 1.

Несмотря на значительные отличия файлового и клиент-серверного варианта системы, они обладают единой схемой контроля доступа на уровне прикладного решения, которые предоставляют следующие возможности:

- авторизация пользователя по паролю заданному в 1С;
- авторизация пользователя по текущему пользователю Windows;
- назначение ролей пользователям системы;
- ограничение выполнения административных функций по ролям;
- назначение доступных интерфейсов по ролям;
- ограничение доступа к объектам метаданных по ролям;
- ограничение доступа к реквизитам объектов по ролям;
- ограничение доступа к объектам данных по ролям и параметрам сеанса;
- ограничение интерактивного доступа к данным и исполняемым модулям;
- некоторые ограничения выполнения кода.

Рис.1. Структура клиент-серверного варианта 1С:Предприятие 8.0

В целом, используемая схема доступа к данным достаточно типична для информационных систем такого уровня. Однако применительно к данной реализации трёхзвенной клиент-серверной архитектуры есть несколько принципиальных аспектов, которые приводят к относительно большому количеству уязвимостей:

1. Большое количество этапов обработки данных, причем на каждом этапе могут действовать отличающиеся правила доступа к объектам.

2. Недостаточно отлаженные процедуры контроля передаваемых данных при переходе с уровня на уровень.

3. Недостаточно высокая средняя квалификация разработчиков и администраторов систем, доставшаяся в наследство от предыдущей версии.

4. Сравнительно небольшой возраст платформы.

Основные виды уязвимостей 1С:Предприятие 8.0:

1. Отсутствие авторизации при создании ИБ на сервере по умолчанию. Наибольшей уязвимостью из данного раздела является возможность почти неограниченно добавлять ИБ на сервер приложений, вследствие чего любой пользователь, получивший доступ к соединению с сервером приложений автоматически получает возможность запускать произвольный код на сервере приложений.

2. Использование кода, выполняемого на сервере. При использовании клиент-серверного варианта 1С, разработчик может распределять выполнение кода между клиентским и сервер-приложением. При этом в случае возникновения ошибки исполнения кода, выполняемого на сервере, сервер-приложение может завершить свою работу, тем самым, прервав работу пользователей не только с информационной базой, вызвавшей ошибку, но и со всеми базами, находящимися на этом сервере.

3. Использование компонентов Internet Explorer (IE). В 1С:Предприятие 8.0 появилась возможность отображать HTML-страницы. При этом используются компоненты IE. В случае заражения интернет-браузера вирусом, вредоносный код выполняется от имени процесса 1С.

4. Печать списков. Любой список (например, справочник или регистр сведений) в системе можно распечатать или сохранить в файл. Для этого достаточно использовать штатную возможность, доступную из контекстного меню.

5. Обмен данными в распределённой базе. Формат обмена данными достаточно прост и описан в документации. Если у пользователя есть возможность подменить несколько файлов, он может внести неавторизованные изменения в систему.

6. Отсутствие возможности шифрования передаваемых данных на участке «Сервер-приложения» – «Сервер базы данных» на уровне платформы 1С:Предприятие 8.0.

Конечно, в беглом обзоре нельзя указать все аспекты, связанные с безопасностью в 1С, но позволим себе сделать некоторые предварительные выводы. Конечно, идеальной данную платформу назвать нельзя – в ней, как и во многих других есть свои проблемы организации защищённой системы. Но это ни в коем случае не означает, что эти проблемы нельзя обойти, наоборот, почти все недостатки могут быть ликвидированы при правильной разработке, внедрении и использовании системы. Большинство проблем возникает из-за недостаточной проработки конкретного прикладного решения и среды его выполнения. Например, типовые решения без внесения значительных изменений просто не предполагают создание защищённой в достаточной мере системы. Но тем не менее некоторые архитектурные решения, связанные с обеспечением безопасности, нельзя назвать удачными.

Основной проблемой в данном случае является тот факт, что код платформы является закрытым и без участия разработчика (ЗАО «1С») решение данных вопросов оказывается не простым. С другой стороны, с выходом 1С:Предприятие 8.0, фирма «1С» стала позиционировать свои решения как средства для построения весьма крупных систем автоматизации. Но пока не будут решены критические проблемы с обеспечением безопасности, вряд ли крупные заказчики обратят внимание на систему 1С:Предприятие 8.0 для автоматизации своей деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гобец А, Гончаров Д., Козырев Д., Кухлевский Д., Радченко М.* Профессиональная разработка в системе 1С:Предприятие 8. Серия: 1С–Библиотека. – Изд-во «1С–Паблишинг, Питер», 2007.