



## Пути повышения безопасности и надежности систем аналитического контроля

А.С. Сафьянов, А.Г. Терещенко, А.М. Янин, В.А. Терещенко, А.Л. Юнак, С.В. Щелканов (НИИ высоких напряжений ТПУ)

*Лабораторная информационно-управляющая система (ЛИУС) "Химик-Аналитик" нашла широкое применение в лабораториях предприятий различных отраслей промышленности (энергетическая, химическая, нефтяная, металлургическая, атомная и др.). Показаны пути повышения безопасности и надежности системы, а также борьбы с угрозами в области информационной безопасности.*

Широкое использование автоматизированных систем на предприятиях страны поднимает на новый уровень проблему обеспечения высокой надежности и безопасности функционирования программно-аппаратных комплексов, осуществляющих управление различными по важности объектами предприятия. Надежность можно рассматривать как устойчивость производимых системой результатов во времени под воздействием условий внешней среды. Переложенная на автоматизированные системы ответственность предъявляет высокие требования к безопасности обрабатываемых данных и управляемых производственных процессов.

Лабораторная информационно-управляющая система (ЛИУС) "Химик-Аналитик" относится к системам класса LIMS (Laboratory Information Management System). Начиная с 2001 г. накоплен опыт эксплуатации и сопровождения ЛИУС "Химик-Аналитик" более чем в 100 лабораториях России. В связи с высокой востребованностью ЛИУС на российском рынке ее разработчикам приходится постоянно заниматься вопросами повышения информационной безопасности, контроля качества и надежности анализов [1].

Как представитель своего класса, ЛИУС "Химик-Аналитик" предназначена для автоматизации бизнес-процессов по различным объектам анализа и тематическим направлениям аналитических лабораторий, производственной деятельности самой лаборатории, обеспечения условий сертификации на соответствие требованиям нормативной документации.

ЛИУС является высокоэффективным концентратом лабораторных данных: обеспечивает структури-

рованное хранение, автоматизированную обработку и организацию оперативного и управляемого доступа. Регламент работы лабораторий предусматривает длительное хранение результатов проведенных исследований, стандарты ИСО и СМК подталкивают к протоколированию различных параметров внутренних процессов с возможностью их дальнейшего анализа в случае нестандартных ситуаций. Требования к независимости результатов лабораторных исследований предполагают внедрение в ЛИУС определенных бизнес-правил, таких как разграничение обязанностей и ответственности пользователей, предотвращение возможных попыток фальсификации результатов. Таким образом, обеспечение актуальности и достоверности содержимого БД ЛИУС является неременным условием обеспечения внутренней безопасности деятельности лаборатории и в конечном итоге влияет на весь комплекс интегрированных систем предприятия MES и ERP уровня, с которыми взаимодействует ЛИУС.

ЛИУС "Химик-Аналитик" на сегодняшний день состоит из следующих основных подсистем (блоков): справочники и классификаторы; лабораторные журналы; внутрилабораторный контроль качества результатов анализа; вспомогательные внутрилабораторные журналы; планирование и управление в лаборатории: пробами, оборудованием, документами и др.; учет реактивов и приготовление растворов; система менеджмента качества лаборатории (СМК); отчетные документы лаборатории; информационная безопасность.

Функционирование ЛИУС "Химик-Аналитик" обеспечивается средствами общего, специального и прикладного ПО:

- общесистемное (ОС; СУБД MS Access, Oracle, MS SQL Server);
- специальное – дизайнер (генератор) форм документов, настройка формул и алгоритмов инженерных расчетов с использованием встроенного языка программирования, формирование и ведение журналов вычислений инженерных расчетов, встроенный калькулятор инженерных расчетов;
- прикладное – средство Parser по преобразованию математических формул в программный код.

Таблица. Основные источники угроз информационной безопасности

Люди	Инциденты (сварии)	Природные факторы
1. Мотивация	1. Ошибка пользователя	1. Стихийные бедствия
2. Возможности	2. Ошибка администратора	2. Астрофизические явления
3. Намерения	3. Отказ аппаратного обеспечения	3. Биологические явления
4. Ресурсы	4. Ошибка ПО	-
5. Способности	5. Отказ промышленного оборудования	
-	6. Потеря актуальности БД	

В условиях широкого использования ЛИУС "Химик-Аналитик" в лабораториях предприятий различных отраслей промышленности (энергетическая, химическая, нефтяная, металлургическая, атомная и др.) наблюдается расширение ее функциональности и объемов автоматизации бизнес-процессов, лавинообразное возрастание числа версий и конфигураций, увеличиваются трудозатраты на сопровождение, гарантийное и постгарантийное обслуживание программного продукта. Одновременно обостряются проблемы оценки показателей качества и надежности, а также растет уровень и число угроз в области информационной безопасности.

На сегодняшний день собственный и мировой опыт внедрения систем класса ЛИУС акцентирует внимание на следующих видах угроз:

- потеря работоспособности системы;
- непреднамеренная порча и потеря информации;
- преднамеренная фальсификация данных;
- несанкционированный доступ к конфиденциальной информации лаборатории.

В соответствии с вышеуказанным подсистема "Информационная безопасность" выделяет в ЛИУС "Химик-Аналитик" ряд потенциальных источников угроз [2-4] (таблица).

Возможный ущерб от каждого источника угроз информационной безопасности различен и зависит от конкретных условий и мотивов его возникновения. Имеются разные подходы в классификации источников угроз и способов оптимальной их локализации в различных структурных элементах информационных систем (ПО, базы и хранилища данных, аппаратное и техническое обеспечение).

В условиях предприятия наиболее значимыми источниками угроз безопасности ЛИУС являются халатность сотрудников (как пользователей, так и технического персонала) и ошибки ПО, приводящие к частичной или полной потере работоспособности системы.

Многолетний практический опыт адаптации, гарантийного и после гарантийного обслуживания программного продукта ЛИУС "Химик-Аналитик" у различных заказчиков выявил следующие основные группы причин и факторы возникновения инцидентов, влияющих на основные показатели безотказной работы: случайная "ошибка пользователя"; ошибка ПО; ошибка администратора" заказчика; потеря актуальности БД.

Фактор "ошибка пользователя" можно разделить на две взаимодополняющих составляющих: недостаточная квалификация пользователей в области компьютерной техники и конкретно ЛИУС и человеческий фактор, последствием которого являются множественные ошибки вводимых в систему с клавиатуры данных. Одно из направлений сокращения влияния человеческого фактора — стыковка ЛИУС "Химик-Аналитик" с приборами, БД и системами аналитического контроля, входящими в состав КИС. На-

пример, в ОАО "Енисейская ТГК (ТГК-13)" (ранее ОАО "Красноярская генерация") в интересах МТЭЦ (г. Минусинск) осуществляется с заданным интервалом (4 часа) круглосуточный ввод показателей состояния водно-химических режимов (ВХР) на турбо- и котлоагрегате из БД АСУТП непосредственно в соответствующие лабораторные журналы ЛИУС. Обеспечивается оперативный расчет показателей электропроводности и кислотности пара и воды в 16 точках измерения. Получена существенная экономия трудозатрат в процессах отбора проб с последующим вводом результатов отбора проб в БД. Одновременно с точки зрения информационной безопасности практически ликвидировано влияние "человеческого фактора" на конечные результаты анализа и повышен уровень их надежности.

"Ошибка ПО" возникает как следствие упущений при тестировании конфигурации программного продукта со стороны исполнителя и заказчика. Выявляются условия в обработке данных, которые не были учтены и заложены в требованиях на автоматизацию существующих бизнес-процессов. В этих случаях процесс исправления программной ошибки может быть отложен до появления благоприятных условий по времени и ресурсам. Но достаточно часто ошибка выявляется, локализуется и оперативно устраняется с последующей отправкой patch (заплаток) заказчику по электронной почте или через сайт, с которого заказчик забирает "заплатку" самостоятельно.

"Потеря актуальности БД" ликвидируется за счет правильной организации формирования и ведения архивных копий БД ИТ-службами заказчика. В более сложных случаях БД восстанавливаются исполнителем и возвращаются заказчику. При этом установлено, что время восстановления работоспособности БД колеблется от нескольких часов до трех суток в зависимости от причин возникновения инцидента.

Отдельного внимания заслуживает направление по предотвращению ущерба, исходящего от факторов: "халатность сотрудников", "кража информации" и "сознательное или случайное искажение результатов анализа". Локализация указанных факторов возлагается на систему разграничения доступа. После завершения работ по адаптации ЛИУС к условиям конкретного заказчика и успешного тестирования полученной конфигурации ЛИУС обеспечивается настройка прав каждого пользователя во всех ключевых блоках и подсистемах. Разграничения и настройка прав по каждому элементу осуществляется для лаборатории, производственной группы внутри лаборатории и конкретного пользователя с предоставлением следующих прав работы с записями, журналами, документами и базами: создание, удаление, чтение, запись, чтение и запись, настройка форм, право на работу, сдача в архив. Отдельные права предоставлены на утверждение результатов в лабораторных журналах и снятие утверждения. Для отдельного документа предусмотрено: создание,

удаление, утверждение, финальное утверждение, отмена утверждения. Кроме того, обеспечивается настройка прав пользователей на работу с журналами либо только своей, либо еще и другой лаборатории. Указанные функции контроля и анализа обеспечивает программная "Утилита настройка прав пользователей ЛИУС". В условиях контроля качества сырья, готовой продукции или экологических показателей такие меры разграничения доступа можно считать оправданными.

Существенную помощь в организации мер безопасности оказывают и стандартные средства ограничения доступа СУБД (права доступа к объектам и операциям, определяемые администраторами предприятия и корпоративными правилами для СУБД).

Обеспечить надежность результатов анализа возможно посредством реализации в ЛИУС требований соответствующих стандартов. Для результатов анализа показателей, которые подразумевают ввод параллельных измерений, в лабораторных журналах ЛИУС "Химик-Аналитик" автоматизирована процедура контроля приемлемости единичных измерений в соответствии со стандартами ГОСТ Р ИСО 5725-2002 и МИ 2881-2004. Данная проверка позволяет исключить из использования в работе результаты анализа, у которых размах параллельных измерений превышает предел повторяемости. Таким образом, улучшается качество и безопасность ввода результатов анализа, а также контролируется, что достаточно актуально и важно, непосредственный исполнитель анализа.

Аналитическая лаборатория должна подтвердить доверие к полученным результатам анализа и предотвратить выдачу заказчику неудовлетворительных результатов, то есть полученных при нестабильном состоянии процедуры выполнения измерений. Для обеспечения качества и безопасности получения результатов по соответствующей методике выполнения измерений в лаборатории проводят внутренний контроль показателей качества результатов анализа, алгоритмы которого изложены в ГОСТ Р ИСО 5725-2005 и РМГ 76-2004 и автоматизированы в ЛИУС "Химик-Аналитик" в подсистеме "Внутрилабораторный контроль". При постоянном контроле процедуры выполнения измерений достигается максимальное качество и уменьшается риск в выдаче заказчику результатов анализа, которым нельзя доверять. Использование указанных бизнес-процессов доказывает компетентность лаборатории.

Дальнейшее улучшение показателей надежности, безопасности и снижение трудозатрат на сопровождение связано с выделением в рамках проекта ЛИУС "Химик-аналитик" отдельной подсистемы: "Сопровождение удаленного программного продукта с ис-

пользованием Web-технологий", которая должна обеспечить следующие задачи [5-8]:

- учет и накопление данных по работе с клиентами и заказчиками;
- учет распределения комплектов поставки и конфигураций ЛИУС по подразделениям;
- учет фактического времени адаптации и достигнутой эффективности;
- учет и анализ причин и трудоемкости устранения претензий (инцидентов), распределения претензий по структурным элементам ЛИУС, показателей надежности программного продукта ЛИУС "Химик-Аналитик", истории изменения версий структурных элементов;
- формирование и ведение на сайте [www.chemsoft.ru](http://www.chemsoft.ru) разделов "техническая поддержка" и "претензии".

Реализованный в ЛИУС "Химик-аналитик" комплекс мер по обеспечению безопасности и надежности функционирования аналитической лаборатории апробирован на ряде предприятий и позволяет успешно противостоять основным источникам внешних и внутренних угроз.

#### Список литературы

1. *Терещенко А.Г., Терещенко А.Г., Терещенко В.А.* Переход лабораторий на электронные документы при внедрении лабораторно-информационных систем // Партнеры и конкуренты. 2006. №3.
2. ISO 10181:1996-1-7. ВОС. Структура работ по обеспечению безопасности в открытых системах.
3. ISO 13335: 1996-1998-1-5. ИТ.ТО. Руководство по управлению безопасностью.
4. ISO 15408:1999-1-3. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
5. *Щелканов С.В., Терещенко В.А., Юнак А.Л.* Сопровождение удаленного программного продукта ЛИУС "Химик-Аналитик" с использованием Web-технологий. Проблемы и пути решения // XIII международная научно-практическая конференция студентов, аспирантов и молодых ученых "Современная техника и технология". Томск: Изд. ТПУ. 2007. Т.2.
6. *Щелканов С.В., Терещенко О.В., Юнак А.Л.* Сопровождение удаленного программного продукта ЛИУС "Химик-Аналитик" с использованием Web-технологий. Понятие "претензия" как основа улучшения качества // Там же. Томск: Изд. ТПУ. 2007. Т.2.
7. *Кошеутов А.В., Терещенко А.Г., Терещенко В.А.* Сопровождение удаленного программного продукта ЛИУС "Химик-аналитик" с использованием Web-технологий. База данных "Техническая поддержка". Направления развития // Там же. Томск: Изд. ТПУ. 2007. Т.2.
8. *Кошеутов А.В., Терещенко А.Г., Вылегжанин О.Н.* Сопровождение удаленного программного продукта ЛИУС "Химик-Аналитик" с использованием Web-технологий. Обзор и анализ методов классификации // Там же. Томск: Изд. ТПУ, 2007. Т.2.

*Сафьянов А.С. — инженер, Терещенко А.Г. — с.н.с., Янин А.М. — н.с., Терещенко В.А. — инженер, Юнак А.Л. — ведущий специалист,*

*Щелканов С.В. — инженер НИИ высоких напряжений Томского политехнического университета.*

*Контактный телефон/факс (3822) 41-70-13. E-mail: git@hvd.tpu.ru, http://www.chemsoft.ru*