



# Опасности 2000 года для промышленных предприятий

Лев Анзимиров, Владимир Айзин

По отношению к «проблеме 2000 года» (Y2K, «жук тысячелетия») инженеры промышленных предприятий делятся на две категории: тех, кто еще не тестировал свои микропроцессорные системы, и тех, кто уже столкнулся с опасностями, вызванными некорректной обработкой времени в промышленном оборудовании. Авторы этой статьи, естественно, сначала принадлежали к первой категории и относились к проблеме Y2K со снисходительным благодушием. Однако более глубокое знакомство с предметом заставило нас изменить мнение: проблема 2000 года — серьезнейшая угроза, и последствия ее будут тем тяжелее, чем меньше о ней осведомлены люди. В данной статье мы попытаемся рассказать о причинах проблемы Y2K, основных угрозах, которые она несет производственным предприятиям, и дать некоторые советы по предотвращению ее последствий.

## Происхождение проблемы 2000 года

Причины проблемы 2000 года общеизвестны. В 60-80-е годы в связи с высокой стоимостью оперативной и дисковой памяти ЭВМ и промышленных контроллеров программисты, экономя, кодировали обозначение года двумя символами, в результате чего компьютеры будут считать, что после 1999 года наступит не 2000, а 1900 год. Небрежные и малоквалифицирован-

ные программисты продолжали производить двухсимвольную кодировку года и в 90-е годы, когда о проблеме 2000 года стало широко известно. Поэтому любая программа, вне зависимости от года выпуска, должна считаться потенциально Y2K опасной до тех пор, пока не будет доказано обратное.

К важной проблеме 2000 года относятся неправильное исчисление високосности 2000 года (2000 год високосный, хотя многие компьютеры так не считают), а также переполнение счетчиков времени. Есть и еще ряд потенциально опасных дат в программах, которые используют число 9999 как символы остановки программы, для обозначения бесконечности либо несуществующей даты. Однако сбои, вызванные этими датами, вряд ли будут носить массовый характер — скорее всего они будут редки. Кстати, одну из таких дат 07/04/1999 (99 день 99 года) мы уже

благополучно пережили. В таблице 1. перечислены Y2K опасные даты.

Что же нам угрожает?

## Какое оборудование Y2K опасно?

Самый простой ответ: ВСЕ! Потенциальная опасность сбоев в Y2K критические дни сохраняется в любых устройствах, использующих микропроцессоры и таймеры. Y2K опасны **интеллектуальные датчики**, осуществляющие первичную обработку измеряемой информации. Для них типично использование метода скользящего среднего для вычисления средней температуры, давления, расхода и т.д. Сам по себе алгоритм скользящего среднего абсолютно безопасен, более того, в большинстве случаев для вычисления периода усреднения в нем используется не астрономическое время, а безопасный, с точки зрения проблемы 2000 года, алгоритм отсчета секунд. Однако, как показали про-

Таблица 1. Y2K опасные даты

Дата	Причина
Наибольшая опасность	
01/01/2000 (2001, 2002 и т.д.)	Использование двухсимвольной кодировки года
29/02/2000	«Несуществующая дата» — неправильное вычисление високосности 2000 года
«Завтра?»	Переполнение счетчиков времени
Скорее всего, опасность отсутствует	
07/04/99	99 день 99 года. Использование числа 9999 как символа остановки программы или бесконечности
09/09/99	9999. Использование числа 9999 как символа остановки программы или бесконечности

верки, до 12% встроенных устройств используют абсолютное время и соответственно являются потенциально Y2K опасными.

Y2K опасны и автоматические **исполнительные механизмы**, например задвижки. В Белой книге по проблеме 2000 года (см., например, [http://www.y2k.fcsm.ru/Official/Doc\\_Others/whitebook.html](http://www.y2k.fcsm.ru/Official/Doc_Others/whitebook.html)) говорится следующее: «Большинство [автоматических задвижек] содержит компоненты, чувствительные к воздействию проблемы 2000 года, особенно в том случае, если имеется установленная по времени самопроверка. Некоторые виды задвижек при этом дают сбой, оставаясь открытыми, другие — закрытыми». Автоматические задвижки используются повсеместно на взрыво- и пожароопасных производствах. Причем, чем опаснее процесс, тем он обычно более автоматизирован и тем более вероятны на нем аварии, связанные с проблемой 2000 года.

Опасность представляют **локальные регуляторы**, встроенные в автоматизированные устройства. Их работа основана на ПИД-алгоритмах, которые также используют время. Сразу оговоримся: в подавляющем большинстве случаев в регуляторах не используются абсолютные привязки ко времени, но никто не может гарантировать того, что они не используются никогда. Проверить это в большинстве случаев невозможно, так как обычно они не имеют внешних интерфейсов и работают как «черные ящики». Сбой работы регуляторов может вывести из строя всю установку либо целую автоматизированную линию. Локальные регуляторы применяются повсеместно, как на основном производстве, так и во вспомогательных системах: в отоплении, вентиляции, кондиционировании воздуха и т.д.

Полны опасностей и **программируемые логические контроллеры (ПЛК)**. В общем случае Y2K опасными компонентами ПЛК являются:

- 1) часы реального времени (RTC);
- 2) BIOS (если она есть);
- 3) операционная система (если она есть);
- 4) прикладное программное обеспечение.

Сбой в ПЛК, вызванный проблемой 2000 года, могут приводить к зависаниям, отказу в загрузке, неправильному исполнению алгоритмов или отработке команд.

Вероятность встретить несовместимый с 2000 годом ПЛК весьма высока, причем уважаемая торговая марка и солидная репутация производителя не

должны вводить в заблуждение. Как это ни парадоксально, но именно использование в промышленной автоматике наиболее надежной техники увеличивает опасность аварий, вызванных Y2K. Редкий контроллер, выпущенный в 90-х годах, имел расчетный срок службы менее 10 лет. Поэтому в промышленности вероятность встретить работающие устройства, произведенные в эпоху, когда отношение к проблеме 2000 года было безопасным, повышена! Хотя большинство промышленных систем дублированы, опасность представляет именно тотальный отказ, вызванный внешней по отношению к АСУ причиной (некорректной обработкой даты) и охватывающий как основные, так и резервные контуры управления. В обычных условиях подобные отказы крайне маловероятны и потому в существующих методах обеспечения отказоустойчивости в промышленности не учитываются.

Аналогично ПЛК **персональные компьютеры**, используемые для supervisory управления и сбора данных, имеют 4 потенциально опасных компонента:

- 1) часы реального времени (RTC);
- 2) BIOS;
- 3) операционная система;
- 4) SCADA-система, прикладное программное обеспечение пользователя и третьих фирм.

Проверка RTC и BIOS на совместимость с 2000 годом может быть осуществлена достаточно просто — многие фирмы предлагают специальные программы для автоматического тестирования ПК. Одну из них — 2000.exe бесплатно можно скачать с сайта [http://www.nstl.com/html/nstl\\_y2k.html](http://www.nstl.com/html/nstl_y2k.html). Проверка компьютера или PC-контроллера при помощи 2000.exe занимает несколько секунд, а результаты весьма поучительны: уже второй из проверенных нами офисных ПК оказался несовместимым.

Операционные системы проверить сложнее. Придется последовательно переводить часы компьютера через все опасные рубежи или полагаться на материалы производителей. Успокаивает одно: наиболее распространенные операционные системы Microsoft находятся под постоянным контролем миллионов пользователей. Замеченные ошибки исправляются. Нам не приходилось сталкиваться со сбоями в последних версиях этих операционных систем. Другое дело ранние версии: рекомендуется проверить, какого года выпуска операционные системы работают на ваших предприятиях, и по возможности обновить их. Информацию можно най-

ти по адресу <http://www.microsoft.com/technet/year2k/>. Менее распространенные специализированные ОС PB (особенно старые версии) нуждаются в серьезной проверке.

SCADA-системы как российского, так и иностранного производства полны Y2K-ошибок. Пусть вас не смущают солидные марки и громкие имена. Наиболее опасны старые версии SCADA, выпущенные для DOS/Windows 3.1x/Windows95 (16 бит), работающие в настоящее время на производственных предприятиях. Их необходимо проверять. Проверке подлежат следующие функции SCADA-системы:

1. Ввод данных:
  - 1.1. Диалоговый ввод.
  - 1.2. Импорт.
2. Вывод данных:
  - 2.1. Диалоговый вывод.
  - 2.2. Экспорт.
  - 2.3. Вывод в текстовые файлы.
3. Алгоритмы обработки данных.
4. Хранение и выборка данных.
5. Поиск.
6. Фильтрация.
7. Сортировка.
8. Выполнение календарных операций.

Так, например, мы провели тестирование текущих и ранних версий SCADA-системы Trace Mode 4.20 для DOS и Trace Mode 5 для Windows NT согласно вышеперечисленным пунктам. Наши испытания не установили наличия проблем 2000 года в этих SCADA-системах.

### Что может случиться на промышленном предприятии в Y2K опасные дни?

**Новогодняя ночь 01/01/2000.** Интервал интегрирования значений температуры, давления и других жизненно важных параметров, измеряемых с применением метода скользящего среднего, в 00:00:01 может измениться от 30 с до -100 лет. Соответственно значения измеряемых параметров резко упадут до очень низких величин. При этом либо сработают блокировки и система будет отключена, либо автоматические регуляторы попытаются компенсировать изменение параметров. К чему может привести повышение давления в котле, в котором оно якобы упало до нуля, а на самом деле находится в нормальном режиме, может представить каждый. А вот пример отключения системы термомониторинга на алюминиевом заводе в Новой Зеландии приводится в уже упомянутой Белой книге по проблеме 2000 года — там произошел перегрев и расплавление пяти блоков. К счастью, действие ошибки «2000» на алгоритмы



скользящего среднего непродолжительно — уже через 30 секунд все придет в норму.

В системах автоматического регулирования на основе ПИД-алгоритмов, в случае использования в них абсолютного времени, произойдет следующее: в 00:00:01 интервал интегрирования изменится от 30 с до -100 лет, при этом регуляторы выдадут управляющие воздействия, направленные на резкое изменение значения контролируемого параметра. Наибольшего управляющего воздействия следует ожидать в первый момент, т.е. все задвижки, клапаны и т.д. будут переведены в крайние положения — полностью открыты или закрыты. В результате технологический процесс будет выведен из-под контроля или остановлен противоаварийной системой. Неправильная работа ПИД-алгоритмов будет продолжаться несколько часов.

Программное обеспечение промышленных контроллеров и SCADA-систем может быть не рассчитано на обработку отрицательных интервалов времени. В роковой час они могут одновременно «зависнуть». Причем «зависнут» не только основные, но и резервные системы, что полностью парализует систему управления промышленным предприятием. Представьте себе ГРЭС, на которой 5000 управляемых технологических параметров одновременно перешли в состояние «свободного плавания»! Сторожевые таймеры перезапустят контроллеры, но они «зависнут» опять. Так будет продолжаться минимум 30 с, а возможно и больше, если для восстановления работоспособности программ потребуются более серьезное вмешательство. В связи с тем, что некоторые заведомо положительные величины 01/01/2000 могут стать отрицательными, оператор может получить неправильную информацию о техпроцессе (см. раздел про интеллектуальные датчики) и, соответственно, принять неверные решения по управлению. Кроме того, вероятно неправильная отработка команд, например, оператор открывает задвижку, а она, наоборот, закрывается. Что при этом произойдет?..

Есть еще одна категория сбоев, которую необходимо иметь в виду, — это устаревание паролей. Вполне вероятно, что первая смена, заступившая на вахту в 2000 году, не сможет произвести LOGIN — компьютер будет считать их права просроченными.

**29 февраля 2000 года 00:00\***. Наступил «несуществующий» день. Часть старых компьютеров просто не загрузится после этой даты. В других системах будет сбит календарь. В специализирован-

ных ОС PB и UNIX возможна «потеря дня», даже если BIOS вашего компьютера обрабатывает эту дату корректно и тест 2000.exe проходит без проблем. Начиная с этого дня, возможен конфликт в многоплатформенных комплексах, где QNX, UNIX работают вместе с MS-DOS и Windows, — эти операционные системы считают время из разных источников. Такие многоплатформенные «зоопарки» характерны для ряда наших предприятий.

## Практические рекомендации по выживанию

Как же защититься от угрозы 2000 года? Гарантию, естественно, дает только полный аудит всех микропроцессорных систем предприятия и замена их на Y2K безопасное. Однако это очень трудоемкий и капиталоемкий процесс. Крупному промышленному предприятию предстоит проанализировать 300-400 персональных компьютеров, 700-900 программных продуктов и встроенные микропроцессоры, число которых не поддается исчислению. Даже при наличии полной документации анализ одной программы высококвалифицированными специалистами занимает около 5 человеко/дней, а в обычных условиях эту цифру можно смело умножать на 2 или 3. Поэтому, скорее всего, реально мы можем говорить лишь о мерах по снижению риска. Каковы же они?

Как мы видели, наиболее опасный рубеж — это новогодняя ночь 2000 года. Поэтому совет номер один: в эту ночь переведите ваши системы на ручное управление. Этим вы значительно снизите риск аварии. В том случае, если это невозможно советуем краткосрочное (5-10 минут) отключение автоматики непосредственно перед Новым годом. Однако, имейте в виду следующее: часть компьютеров и промышленных контроллеров корректно проходит 01/01/2000, но сбрасывает счетчик времени при первой перезагрузке. В этом случае «жук тысячелетия» наступит вас, когда вы заново включите автоматику.

P.S. Кстати, не советуем в Новый год ездить на иномарках — современный автомобиль содержит множество микропроцессоров, часть из которых Y2K опасна. Также не советуем включать стиральные машины, домашние кондиционеры, мини-котельные и другое сложное домашнее оборудование. ●

\*По мнению редакции, этот день существует