

Защита от дурака

Как программист пишет программу? Вернее, конечно, как ХОРОШИЙ программист пишет программу ДЛЯ ПОЛЬЗОВАТЕЛЯ? В очень грубом приближении происходит это так:

Первым делом ставится задача - что есть на входе и что нужно получить на выходе. Потом рассматриваются и выбираются средства, которыми можно этого добиться. Потом строится последовательность действий, которые будут выполняться при работе с программой, с учетом - внимание! - всех НЕПРАВИЛЬНЫХ действий, какие только может совершить НЕКВАЛИФИЦИРОВАННЫЙ пользователь; такие действия блокируются, т.е. при их выполнении программа либо завершает работу, либо возвращает на последнее совершенное "безопасное" действие, либо блокирует выполнение последующих действий до исправления ошибки. С последней из перечисленных предосторожностей мы встречаемся и в некоторой современной бытовой технике - микроволновка не включится, пока дверца открыта, а стиральная машина не начнет работать, если перекрыта подачи воды. Думаю, не за горами время, когда микроволновка станет отслеживать и наличие в ней при включении разрешенного содержимого, а стиральная машина - загрузку строго разрешенного количества белья. Но вернемся к программированию.

После того, как написание алгоритма программы и перевод его на выбранный язык программирования завершены, начинается то, что программисты очень не любят: тестирование. Это значит, что некто (сам программист или представитель заказчика) начинают вытворять с продуктом черт знает что. Само собой, проверяют, будут ли получены нужные результаты при вводе запланированных данных; но кроме этого совершают все мыслимые ошибки, лезут, куда левой ногой вздумается, нарушают все прилагающиеся инструкции. Если при этом на каком-то этапе какие-то действия приведут к выдаче неправильных результатов или к зависанию программы - она корректируется с учетом выявленных багов. Понимаете? НЕ ПОЛЬЗОВАТЕЛЮ УКАЗЫВАЮТ, ЧТО НЕЛЬЗЯ ДЕЛАТЬ ТО И ЭТО, а предусматривают, как быть, если он все-таки это сделает! Программист предусматривает, что должна сделать программа, если в качестве пользователя за нее сядет некто совершенно необучаемый или вообще орангутанг. Это и называется "защита от дурака", и если почему компания Microsoft и вызывает раздражение всех более-менее продвинутых пользователей, так это потому, что по части вылавливания багов и установки этой самой защиты ее программисты очень далеки от совершенства.

К чему это я? Разумеется, к нашей действительности. К жизни нашей скорбной, связанной с риском все учащающихся техногенных катастроф и прочих катаклизмов.

Сколько за последнее время сгорело людей, в том числе в свежееотремонтированных понтовых офисах с полностью установленной противопожарной сигнализацией? Сколько аварий с человеческими жертвами произошло в шахтах, в том числе снабженных суперсовременными системами безопасности? А самолеты? А АЭС, черт бы их побрал, и сопутствующие производства? А прочие "неприятности", связанные с "человеческим фактором"? И в результате всех этих печальных событий созываются комиссии, ответственные лица (начальники всех рангов) начинают перекладывать вину друг на друга, а безответственные (подчиненные) просто гибнут или остаются калеками. Более того - оставляя после себя жен, детей, престарелых родителей, которые зависели от повышенных ставок, выплачиваемых "за риск" или "за вредность". Какие уж пенсии и компенсации будут им начислены "в связи с утратой кормильца" и "за моральный ущерб" - то ведомо только вышеупомянутым начальникам да Господу Богу, но остается совершенно очевидным одно: эти суммы обязательно будут НИЖЕ, чем доходы от использования оборудования, технологий и помещений БЕЗ защиты от дурака. При этом уже не так важно, с непредусмотренной конструктивно или с существующей, но отключенной или заблокированной защитой случилась трагедия - важно другое: наши любимые, свято чтимые и берегаемые традиции считать жизнь человека менее важной, чем некое ДЕЛО, и полагаться на Святой Авоось, не просто живы - они цветут, как никогда ранее. Чудным удобением для них являются теория вероятностей и всеобщая "экономизация" образования.

Бедные, бедные математики, если бы они знали, как будут использовать "скороспелые" экономисты и управленцы разных уровней математический аппарат теорвера, они наверняка бы постарались засекретить

его грифом "до прочтения съест". В самом деле, как греет душу осознание того факта, что "вероятность аварии составляет сотые доли процента" - ну что это, сотые доли, так, ПРЕНЕБРЕЖИМО мало! Но при проекте, рассчитанном лет на 50 и более, да с пространственными характеристиками, выражающимися тысячами километров, да с наспех просчитанными моделями, в которых закладывались только очевидные факторы, к тому же самим заказчиком определяемые... "Вероятность аварии пренебрежимо мала!" - и разливаются ежегодно моря нефти от НЕПРЕДУСМОТРЕННЫХ в модели врезок, несработок или запоздавшем срабатывании датчиков, халатности персонала... "Вероятности аварии нет в принципе!" - и проводится эксперимент на "АБСОЛЮТНО НАДЕЖНОМ РЕАКТОРЕ" ЧАЭС... "Шахта оснащена современными средствами предупреждения!" - и после похорон шахтеров и собственно поставщиков противоаварийного оборудования начинают говорить о том, что оборудование-то отключили, чтобы не мешало работать, так что все в порядке, сами виноваты... Свалив аварии на "ошибки экипажей" продолжают эксплуатацию вылетающих резерв самолетов в режимах "экономии" - на запчастях, горючем, техобслуживании... А самое главное - ПОСЛЕ всего этого снова и снова тянут нефтепроводы по заповедным и охраняемым землям, продлевают эксплуатацию старых и строят новые энергоблоки все того же "чернобыльского типа", "приостанавливают" работу ряда шахт БЕЗ смены общего руководства и изменения принципа работы страховочного оборудования. Ошибки программ, приведших к сбоям с человеческими жертвами - их даже не анализируют на ошибки, не говоря уже о том, что продолжают эксплуатировать в прежнем режиме!

Что можно было бы сделать, если бы подобное происходило со стиралкой, микроволновкой или автомобилем? Установить блокировку на выполнение определенных действий пользователя. К примеру, превышение заданной для данного места скорости машиной вызывало бы плавное, но быстрое падение скорости с полной остановкой. Разрешенную скорость можно транслировать на собственно системы машины с центральных диспетчерских пунктов. На производстве, конечно, все это сложнее, а главное - дороже в разы, но, если все-таки считать мерой вещей не прибыли компании, а жизнь человеческую, то и такое сделать реально. Например, превышение ПДК некоего показателя вело бы к плавной, но быстрой остановке производственного процесса. В самолете не соответствующий оптимальному показатель при автотестировании систем просто не позволял бы запускать двигатель, а сбой показателя в полете вел бы к переключению автопилота на поиск ближайшего аэродрома и подаче аварийных сигналов. При этом аварийные системы должны быть надежно защищены от отключения как персоналом, так и в случае перебоев с питанием, а малейшая попытка вскрытия защиты или отключение ее от электросети должно тут же фиксироваться на пультах ближайших служб МЧС и милиции. И все - ВСЕ! - расчетные модели любых связанных с опасностью для жизни и здоровья даже ОДНОГО человека производств должны считаться с учетом всех - ВСЕХ! - известных на момент расчета вариантов неблагоприятного развития событий с учетом тяжести возможных последствий. Например, при даже самой маловероятной возможности взрыва некоей АЭС должно считаться все - от землетрясения или тайфуна в 12 баллов до нашествия злобных инопланетян с боевыми лазерами и биологическим оружием, от сошедшего с ума диверсанта категории 007 до прямого попадания метеорита размером с небольшой небоскреб, от попытки злостного самоубийства особо изощренным способом до появления дьявола. Пусть вероятность такого события будет минус стомиллиардной степени - оно должно быть учтено при расчете.

И еще одной защитой от дурака вполне могла бы стать практика отстранения этого самого дурака от управления процессами. Если на каком-то производстве происходит 2-3 однотипных ЧП, связанных с выводом из строя, отключением или неустановкой аварийного оповещения, блокиратора или систем мониторинга - руководство такого производства должно быть безоговорочно отстранено от занимаемой должности, с запрещением на длительный срок занимать какие бы то ни было руководящие посты.

Вообще говоря, последнее правило не худо было бы распространять и на руководство страной и регионами - 5-6 однотипных массовых выступления граждан по разным частям региона в течение, скажем, срока избрания - и руководство смещается без права на достаточно длительные сроки избираться или назначаться в качестве кого бы то ни было...

Автор: Анна Машерова, БАБР.RU © Babr24.com ОБЩЕСТВО, МИР 👁 12658 25.06.2007, 09:13 👤 388
URL: <https://babr24.com/?ADE=38589> Bytes: 8729 / 8729 Версия для печати Скачать PDF

 [Порекомендовать текст](#)

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)
- [ВКонтакте](#)

Связаться с редакцией Бабра:
newsbabr@gmail.com

Автор текста: **Анна
Машерова, БАБР.RU.**

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: [@babr24_link_bot](#)
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: [@bur24_link_bot](#)
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: [@irk24_link_bot](#)
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: [@kras24_link_bot](#)
эл.почта: krasylar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: [@nsk24_link_bot](#)
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: [@tomsk24_link_bot](#)
эл.почта: tomsk.babr@gmail.com

[Прислать свою новость](#)

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: [@babrobot_bot](#)
эл.почта: equatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)