

Восемь смертных грехов профессиональных программистов

Дагаев Дмитрий Викторович,

Главный Эксперт,

АО «Русатом Автоматизированные системы
управления»

Консультант проекта Информатика-21,

Microsoft Certified Solution developer,

dvdagaev@yahoo.com

Восемь смертных грехов цивилизованного человечества

Основоположник этологии, лауреат Нобелевской премии Конрад Лоренц называл этологию «морфологией поведения животного». Рассматривая в («Восемь смертных грехов цивилизованного человечества») генетически обусловленное поведение людей и социальных групп, Лоренц выделял основные проблемы:

1. Перенаселение;
2. Опустошение жизненного пространства;
3. Бег наперегонки с самим собой;
4. Тепловая смерть чувства;
5. Генетическое вырождение;
6. Разрыв с традицией;
7. Индоктринируемость;
8. Оружие массового поражения.

Аналогичные нарушения функций социальных систем отражаются и на более узких IT-сообществах в части системы накопления и передачи знаний.

В данном докладе основное внимание будет уделено не программам, написанным людьми, а **людям, которые пишут программы**. Этология поможет нам понять, как формируются как специалисты системой обучения и почему эти человеко-машинные системы так функционируют.

1.Переизбыток почти надежных решений

Вы выберете надежное или почти надежное ПО в самолете? В автомобиле? В Вашем умном доме?

Что выдержит испытание временем? Есть подход *«от отрицания» via negativa*. Можно достоверно сказать, *от каких технологий следует отказаться*. Знание о том, что не стоит делать, более ценно и надежно.

Ужесточайте требования! Какие в мире самые жесткие требования к надежности ПО? Это - Стандарт МЭК 60880 для защиты АЭС, выдвигающие сплошные *требования отсутствия*:

- Нет ОС, либо ОС с небольшим числом функций;
- Ограничение прерываний;
- Ограничение числа итераций циклов;
- Исключение нетипизированных указателей.

Переизбыток решений в части свободных и рыночных продуктов (библиотек, графических систем, ОС) склоняет к слепому выбору (асимметрия информации).

Отсутствие фундаментальных основ, профессионализма в части выбора ОС, компиляторов, не допускает принятия ответственных решений.

Пример – сбор и обработка данных РВ 24x7, 100 мс

Надежно на A2 Oberon

Таймер с обработчиком прерывания

InstallHandler(TimerInterruptHandler, IRQ0);

TimerInterruptHandler содержит:

- Функцию обработки данных.

WatchDog контролирует завершение и может вызвать перезагрузку.

Почти надежно на OS Linux

ОС для загрузки задач (ядро, диск, загрузчик);

Стандартный прикладной процесс

while(1) { Handler(); Sleep(100ms); }

Процесс WatchDog;

Планировщик процессов;

Менеджер памяти.



Proportionality Triangle

Объем проекта фиксирован, цену минимизировать, качество – какое получится. Разработчики выберут вариант справа (ухудшающий отбор). Надежность как фактор не принимается в рассмотрение. **Отсутствие (асимметрия) информации** заставляет их верить, что вариант справа более дешевый, что неверно при долгом использовании.

2. Заполнение жизненного пространства токсичным мусором



Техника безопасности предписывает при работе с потенциально опасными радиоактивными отходами выставлять знак «Осторожно, радиация». Последствия отказов программ гораздо более серьезны!

Будущие разработчики **с самых азов** должны впитывать **принцип приоритета угроз** используемых технологий перед заявляемыми их преимуществами, в медицине известный как *primum non nocere* «не навреди».

Презумпция наличия угроз означает, что не наличие, а отсутствие угрозы нужно доказывать. Например, для программы с компилятором C++ необходимо доказывать отдельно каждый указатель в коде, а для Оберона гарантировано отсутствие угрозы на уровне компилятора.

Используемое при преподавании и в промышленности ПО (C, C++, библиотеки) помимо преимуществ, «современных подходов» и «технологий» несет в себе угрозы (угроз значительно больше!):

- Некорректные «висячие» указатели на динамическую память, которые могут привести к потере работоспособности всего ПО;
- Отсутствие контроля выхода за границы массивов и состояния стека, широко используемое в хакерских атаках на «переполнение стека».

Висячие
указатели

Границы
массива

Пример – Ariane 5 Flight 501



Отказ основного и резервного компьютера, приведший к потере спутника 4 июня 1996. Стоимость программы \$8 billion, полезная нагрузка спутника \$500 million.

“The greater horizontal acceleration caused a data conversion from a 64-bit floating point number to a 16-bit signed integer value to overflow and cause a hardware exception. *Efficiency considerations had omitted range checks for this particular variable*, though conversions of other variables in the code were protected. The exception halted the reference platforms, resulting in the destruction of the flight.”

Преобразование данных из 64-битного действительного числа в 16-битное целое привело к переполнению и вызвало аппаратное исключение. *По соображениям эффективности были опущены проверки диапазонов* для данной конкретной переменной.

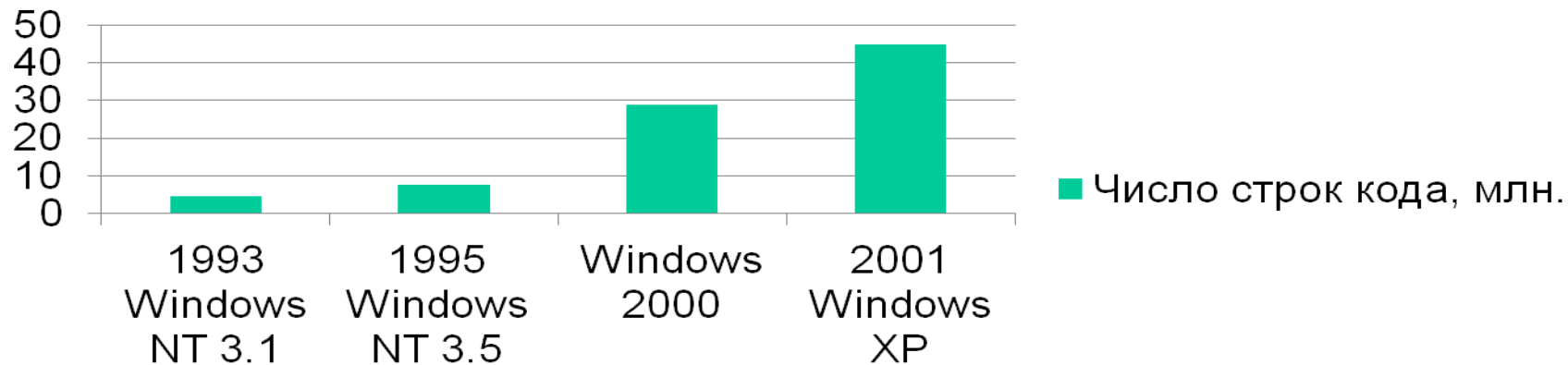
3. Бег наперегонки с самим собой

Последствия внутривидового отбора можно проиллюстрировать на примере маховых перьев самца фазана-аргуса (*Argusianus argus*)... Перспективы петуха иметь потомство находятся в прямом отношении к привлекательному действию его органа ухаживания на кур. Однако в то время как хвост павлина в полете складывается и вряд ли мешает ему, ... удлинение маховых перьев у самца аргуса делает его почти неспособным летать (К.Лоренц).



«Когда мощность системы измеряется числом ее возможностей, **количество становится более важным, чем качество**» (Н.Вирт).

Число строк кода, млн.



Пример – Необязательные возможности ядерной программы Ирана

Необязательная возможность	Объекты атаки Stuxnet
PROFIBUS (PROcess Field BUS) - это открытая промышленная сеть полевого уровня, отвечающая требованиям IEC 61 158/EN 50170. К сети PROFIBUS могут быть подключены контроллеры SIMATIC S7	Функционал ВП Stuxnet включает в себя: распространение на сменных носителях; мониторинг за работой ПО Simatic S7
WinCC - система HMI, программное обеспечение для создания человеко-машинного интерфейса, включает в себя средства проектирования системы отчетности на основе MS SQL Server	Выполнение SQL-запросов для сбора данных из таблиц определенного типа; отправка собранных данных через Интернет на серверы злоумышленников в зашифрованном виде
Работает под управлением операционных систем семейства Microsoft Windows	Выяснилось, что ВП меняет выходные частоты преобразователей и скорости соответствующих им моторов в течение месяцев , чтобы его работа была незаметна. При этом вирус то повышал частоту вращения ротора выше предельно допустимой, то резко снижал ее

4. Нетерпимость к неудовольствию

- Обучение на основе коммерческих продуктов (таких, как, MS Visual Studio) вызывает **привыкание и «нетерпимость к неудовольствию»**. Опыт показал, что программисты, выросшие только на определенных программных технологиях, теряют способность к продуктивной работе в другой среде.
- Зафиксированы случаи отказа программиста работать в определенной программной среде и переход на другую из-за отсутствия пошагового отладчика (при наличии других развитых средств отладки программных ошибок).
 - Удобство пользования библиотеками шаблонов приводит к шаблонному мышлению. Наличие шаблонных библиотек типа STL иногда ставится во главу угла при выборе программных средств. Даже профессиональные программисты путаются в базовых паттернах циклов вроде линейного поиска, не говоря уж о сбалансированных деревьях.
- Вместо интеллектуально ослабленных программистов нужно стремиться к идеалу «интеллектуально-управляемых программ» Дейкстры. Иначе мы и будем иметь продукты, разработчики которых толком не понимают их содержание.
- Привыкание к продуктам мейнстрима вызывает **агрессивную реакцию** на вторжение других людей в приписанную этим продуктам территорию (отладчик, оптимизирующий компилятор C++)

5. Редукционизм и генетическое вырождение

Редукционизм как следствие вырождения образования формирует **упрощенное представление о мире**, предлагаемое в качестве **примеров для обучения** исходит из идеального, иногда «типового» или «формального» подхода вместо глубокого изучения предметной области.

Идеальное представление – неограниченная память (с генерацией исключения):

```
using namespace boost;  
property_tree::tree pt;  
property_tree::read_xml("Name.xml", pt);
```

В реальной жизни последовательность может быть бесконечной и правильный доступ осуществляется через буфер и бегунок "rider".

```
New(file, "Name.txt");  
Set(rider, file, 0);  
Read(rider, x);
```

Ответственность за каждое условие и состояние в программе является абсолютным требованием для критически важных систем.

Абсолютно необходимым является обучение правильному написанию предусловий, постусловий и ответственному анализу вариантов входных данных.

Пример – Авария на Саяно-Шушенской ГЭС 17.08.2009



В результате расследования причин аварии на Саяно-Шушенской ГЭС установлено : «на гидроэлектростанции осуществляются **защиты по 10** технологическим параметрам, но среди них нет защиты по контролю вибрации. Отсутствие технологической (гидромеханической) **защиты по контролю вибрации** на гидроагрегате № 2 явилось причиной аварии, приведшей к катастрофическим последствиям».

Система не является управляемой Разумеется, профессионалам известно понятие управляемости, но иногда может возобладать «позитивный взгляд на мир».

Если вы поставили 10 операторов IF на 10 условий, то стоит ли ставить одиннадцатый IF?

6.Разрыв с традицией

«Самый верный способ потерпеть катастрофическое поражение — это воспроизводить методы противника» У.Черчилль

Последствия решения 1967 г. комиссии по вычислительной технике АН и Совета Министров СССР о переходе на копирование системных программных средств США (IBM/360 и далее) ощущаются и по сей день.

«Величайшая победа Запада в холодной войне» Э.Дейкстра

«Все приходилось переписывать, а то, что доставали, было древнее, плохо работало. Это был оглушительный провал» Б.А.Бабаян

Кризис ответственности – **какова цена полу-добровольного отказа от ответственности в ключевых отраслях системного программирования: ОС, компиляторы?**

Можно ли восстановить, что разрушалось десятилетиями? Проект «Оберон» (Н.Вирт, Ю.Гуткнехт) содержит написанные «с нуля» ОС, Компилятор и Графическую среду для целей обучения системному программированию. Информатика-21 предлагает методическую базу для школьного обучения и для прикладных программистов.

7. Индоктринируемость

Зависимость клиента более доходна, чем его обучение (Н.Вирт).

К.Лоренц указывает на «опасность индоктринирования человечества ложной системой ценностей, желательной лишь для манипулирующих им людей».

Язык программирования	Компания, продвигающая данную технологию на рынке	Расположение
Visual C++	Microsoft Corporation	Редмонд, США
Java	Oracle Corporation	Сан-Франциско, США
Go	Google, Alphabet Inc.	Калифорния, США
Swift	Apple Computer, Inc.	Купертино, США

Образование должно культивировать независимость разработчиков от индоктринирования. Нужна независимость используемых программных средств от компаний со своими коммерческими интересами с предпочтением имеющих научное обоснование и контролируемых разработчиками, которые готовы взять на себя ответственность.

Пример – попытка модификации ядра Linux

Для решения задачи очистки памяти в 3.* ядре Linux рассматривалась возможность модификации ядра.

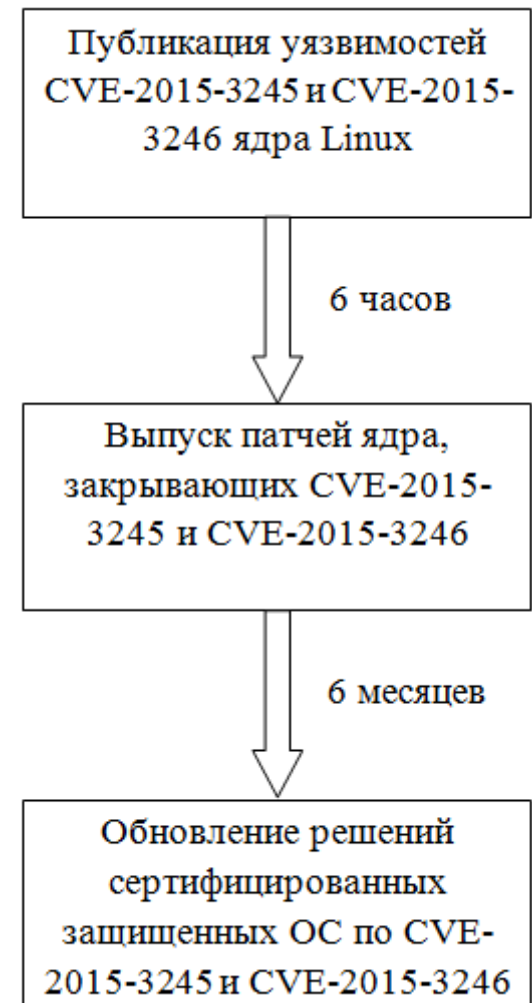
Автор столкнулся с единственным серьезным источником Mel Gorman «Understanding the Linux Virtual Memory Manager», которая дает описание к ядру 2.6. Для более поздних версий предлагается «to refer directly to the source with the polite acronym **RTFS** - Read The Flaming Source. It doesn't really stand for Flaming but there could be children watching». Читайте исходные тексты программ.

Фирмы производители заинтересованы в сохранении зависимости, а не в передаче знаний.

8. Кибер-оружие массового поражения

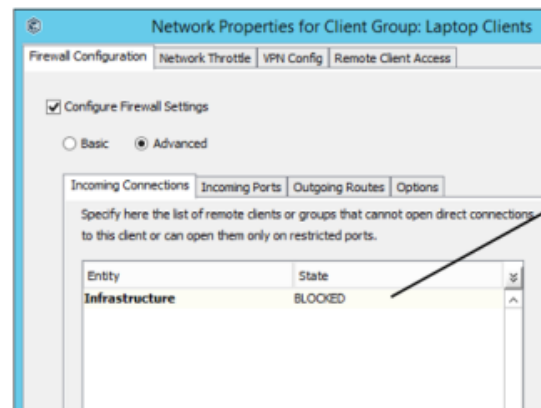
Эпоха кибер-войн уже началась. Требования в части кибербезопасности будут только ужесточаться, а специалисты расти в цене.

- Уже требования сертификации ФСТЭК предписывают детальный анализ блок-схем, диаграмм. Возможность корректной сертификации для импортных ядер Linux и компилятора gcc уже сейчас вызывает вопросы.
- Защита от несанкционированного доступа вызывает вопросы. После публикации в 2015 году уязвимостей CVE-2015-3245 и CVE-2015-3246 ядра Linux сначала, через несколько часов, появились исправления импортных разработчиков ядер, а уже гораздо позже в отечественные сертифицированные «защищенные» операционные системы эти исправления были добавлены.



Пример – Выбор защищенного решения шлюза для АСУТП

Настраиваемый в одном направлении Firewall



"Infrastructure" is BLOCKED from initiating communication with the group "Laptop Clients"

Почти киберзащищенное решение, позволяющее использовать двунаправленные протоколы связи (TCP).

Обычно выбирают такое решение (ухудшающий отбор).

Однонаправленный диод данных



Для выбора по-настоящему защищенного однонаправленного решения приходится отказаться от излишних требований в виде двунаправленных сетевых протоколов.

Вопросы и Приложения

Любителям Linux, GCC, Qt, Java



Либо Вы считаете себя Господом, либо Вам не доверяют. А вы им доверяете и готовы ставить это на объекты?

Приложение 1 – МЭК 60880

V.2cb Следует избегать использования универсального операционного программного обеспечения (операционных систем)

V.2cc Если операционная система необходима, то ее применение следует ограничить небольшим числом простых функций

V.2cd Операционная система должна содержать только необходимые функции

V.2dd Время прогона не должно существенно изменяться в результате изменения входных данных

V.2de Значение изменения времени прогона, которое может быть вызвано входными данными, должно быть документально оформлено

V.2dg Объем данных, считываемых в течение одного вычислительного цикла, должен быть постоянным

V.2e Необходимо ограничивать применение прерываний

V.2ea Прерывания могут использоваться, если они упрощают проект ПО и не делают верификацию чрезмерно сложной

V.2ed Если прерывания используются, то для непрерываемых частей необходимо иметь оценки максимального времени вычислений, чтобы можно

было рассчитать максимальное время, в течение которого прерывание запрещено

V.3c Содержимое памяти должно быть защищено или контролироваться

V.3db Следует проверять правильность передачи любого параметра, включая проверку типа параметров

V.3dc При адресации массива следует проверять его границы

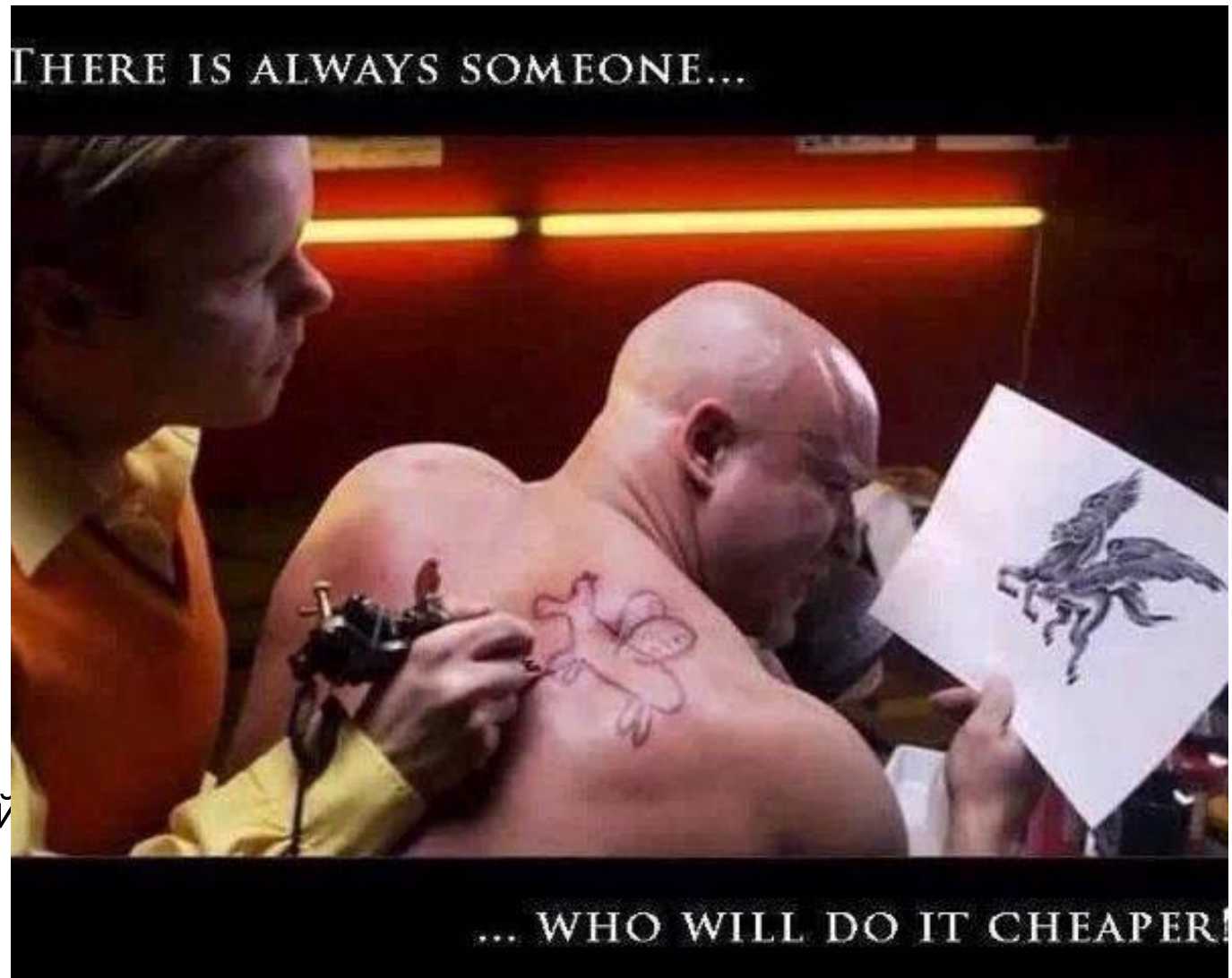
Приложение 2 – Ухудшающий отбор с минимизацией цены



Proportionality Triangle

Лукавый выбор при фиксированном объеме функций и минимизации цены.

Проблема в асимметрии информации, нужна калибровка системы отбора по эталонным выборкам до реальной «метрологической аттестации».



Приложение 3 – Управляемость и закон Эшби

	α	β	γ	δ
1	<i>b</i>	<i>d</i>	<i>a</i>	<i>a</i>
2	<i>a</i>	<i>d</i>	<i>a</i>	<i>d</i>
<i>D</i> 3	<i>d</i>	<i>a</i>	<i>a</i>	<i>a</i>
4	<i>d</i>	<i>b</i>	<i>a</i>	<i>b</i>
5	<i>d</i>	<i>a</i>	<i>b</i>	<i>d</i>

Закон необходимого разнообразия Эшби для обеспечения управляемости требует, чтобы каждому состоянию D находилось управляющее воздействие R. Это не выполняется в таблице 5x4 слева.

Такая система не является управляемой (ТАУ – критерии управляемости).

Для случая Саяно-Шушенской ГЭС отсутствует управляемость по одному из 11 параметров - защите по контролю вибрации.