Security Engineering: часть 13. Новые вызовы.

Published: 25.06.2026 11:33 | Updated: 07.07.2026 13:57

На острие прогресса: Новые вызовы безопасности

Смена парадигмы угроз

Современная безопасность все чаще смещается от защиты классических периметров к защите сложных социо-технических систем. Ярким примером уязвимости новых платформ стал инцидент с блогом Light Blue Touch Paper, который использовал движок Wordpress. Несмотря на то, что разработчики оперативно закрывали уязвимости, блог был взломан российским «скрипт-кидди», который пытался разместить рекламу наркотиков. Этот случай подчеркивает главную проблему: мы все больше зависим от приложений, которые не успеваем полноценно оценивать на предмет безопасности.
Если раньше безопасность фокусировалась на защите данных и сетей, то сегодня «главным приложением» интернета становятся другие люди. Это порождает совершенно новые классы угроз, которые я отношу к «острию прогресса» (The Bleeding Edge). К ним относятся онлайн-игры, веб-приложения (аукционы, поиск, социальные сети), технологии обеспечения анонимности и электронные голосования.

Компьютерные игры: От Pong до виртуальных экономик

Компьютерные игры были одним из первых приложений для ЭВМ. Еще на первом полноценном компьютере EDSAC студенты писали игры, а исследователи ИИ создавали шахматные программы, полагая, что их решение приведет к созданию полноценного искусственного интеллекта. Сегодня игры — это индустрия, чьи обороты сопоставимы с кассовыми сборами голливудских блокбастеров, а переход игр в онлайн породил уникальные проблемы безопасности и читерства.

Типы читерства в играх

Читерство в играх существует столько же, сколько и сами игры, но онлайн-среда придала ему новый масштаб. Выделяют три основных типа обмана:

1. **Эксплуатация известных уязвимостей и правил.**
   Классический пример — игра в бридж. В офлайн-турнирах между партнерами ставят ширму, чтобы они не видели карт друг друга, но читеры могут передавать информацию через кашель или интонацию. В онлайн-бридже эта проблема решается протоколами, но появляется новая угроза: создание множественных идентичностей (Sybil-атаки). Если в игре можно легко создавать новые аккаунты, злоумышленник может получить преимущество, играя сам против себя.
2. **Стандартные кибератаки.**
   Игровые клиенты и серверы подвержены тем же угрозам, что и обычный софт: фишинг, DoS-атаки, чтение памяти и перехват данных. Например, 5% всего вредоносного кода, фиксируемого Symantec, нацелено именно на онлайн-игры (кража аккаунтов Gampass и Lineage).
3. **Новые тактики, порожденные сетевой средой (Неотактики).**
   В тактических шутерах успех должен зависеть от навыков игрока, а не от сетевых задержек. Однако из-за особенностей кэширования данных на клиенте возникает парадокс: игрок с более высокой задержкой (пингом) получает преимущество, если он первым выходит из-за угла. Его клиент уже «знает» о противнике, пока сервер и клиент жертвы еще обмениваются пакетами. Использование таких сетевых аномалий получило название «неотактик».

Боты, aimbot'ы и неавторизованный софт

Одной из самых persistent проблем являются боты и автоматизированные помощники. Aimbot'ы (программы для автоматического прицеливания) и wall hack'и (софт, делающий стены прозрачными) полностью разрушают баланс. Разработчики пытаются бороться с этим, защищая потоки данных и используя античит-сканеры, но гонка вооружений продолжается.
Интересное решение для борьбы с читерами предложила игра Call of Duty 4. В ней реализована система повторов действий (action replays), позволяющая жертве посмотреть на убийство глазами убийцы. Это не только выявляет использование aimbot'ов, но и снижает восприятие нечестной игры, что критически важно для удержания аудитории.

Виртуальные миры и виртуальные экономики

С появлением ММО (массовых многопользовательских игр) родилась новая экономическая реальность. Игровые предметы и валюты стали стоить реальных денег.

- **Фарминг:** Появились «золотые фермеры» (часто в странах с низкой оплатой труда, например, в Китае), которые часами добывают игровые ресурсы для продажи. Это породило организованную преступность. Например, в игре Lineage хакеры использовали украденные идентификаторы для создания сотен тысяч аккаунтов, с помощью которых похитили игровых ценностей на сумму около **$15 млн**.
- **Виртуальные миры:** Платформы вроде Second Life (разработчик Linden Labs) позволили пользователям создавать собственный контент и бизнес. Внутренняя валюта (Linden dollars) обменивается на реальные доллары. Однако виртуальные миры быстро столкнулись с реальным законодательством. После того как ФБР начало рейды на подпольные онлайн-казино, в Second Life произошел обвал рынка виртуальной недвижимости, а арендные ставки резко упали.

Виртуальные экономики также столкнулись с проблемой мошенничества и отмывания денег, что вынудило разработчиков внедрять системы верификации (например, привязку к кредитным картам), чтобы соответствовать законам о борьбе с отмыванием средств (AML).

Веб-приложения: eBay, Google и Социальные сети

По мере того как критические компоненты приобретают возможность общения, а бизнес переходит в онлайн, на передний план выходят веб-приложения. Разработчики часто относятся к безопасности как к второстепенной задаче, что приводит к появлению новых классов уязвимостей и эксплойтов, которых не существовало в классических «встроенных» системах.

Общие угрозы для веб-приложений

Одной из самых распространенных уязвимостей веб-сервисов является межсайтовый скриптинг (XSS). Языки сценариев, такие как JavaScript, позволяют сайтам взаимодействовать с пользователем, но также открывают дверь для внедрения вредоносного кода.
Еще одной серьезной проблемой становятся утечки данных из-за фишинга сотрудников. В ноябре 2007 года компания Salesforce.com признала, что фишинговая атака на одного из сотрудников привела к компрометации баз данных, в результате чего клиенты начали получать фальшивые счета. В другом инциденте банк SunTrust столкнулся с тем, что 40 000 его клиентов оказались скомпрометированы из-за подобных действий.

eBay и проблемы доверия

Площадка eBay и ее платежная система PayPal являются крупнейшими целями для фишеров и мошенников. Фишинг против PayPal работает по тем же схемам, что и против банков, но с важным отличием: клиенты PayPal не защищены законами, такими как американское Regulation E (которое перекладывает ответственность за мошенничество с кредитных карт на банк). Здесь клиенты вынуждены полагаться исключительно на добрую волю самой компании.
Помимо фишинга, на eBay процветают старые добрые мошенничества. Например, хитрецы рассылают письма пользователям, которые не выиграли аукцион (underbidders), предлагая им купить аналогичный товар напрямую, который в итоге оказывается подделкой или вовсе не отправляется.
С появлением репутационных систем (отзывов и рейтингов) появился и новый вид атак — **угон аккаунтов (account takeovers)**. Злоумышленники взламывают аккаунты продавцов с безупречной историей и высоким рейтингом, чтобы использовать их доверие для продажи несуществующих товаров.
Другой изощренный скам связан с **фальшивыми эскроу-сервисами (escrow scams)**. Мошенник продает, например, автомобиль и предлагает покупателю воспользоваться «безопасной сделкой» через сайт-эскроу. Покупатель переводит деньги на поддельный сайт, после чего мошенник исчезает вместе с деньгами.

Google: поиск, реклама и конфиденциальность

Безопасность Google — это колоссальная задача, учитывая масштабы компании. Одной из уникальных угроз стал **Google Hacking** — использование поисковых механизмов самой компании для поиска уязвимых серверов, открытых баз данных или конфиденциальной информации, оставленной разработчиками в открытом доступе.
Бизнес-модель Google строится на таргетированной рекламе, что породило специфические атаки:

1. **Клик-фрод (Click-fraud):** Конкуренты или злоумышленники многократно кликают по рекламе, чтобы истощить рекламный бюджет жертвы.
2. **Impression spam:** Конкуренты загружают страницы с рекламой, но не кликают по ней. Это искусственно занижает показатель кликабельности (CTR), заставляя алгоритмы Google понизить рейтинг объявления.

Также расцвел феномен **MFA (Made for Adsense) сайтов**. Мошенники создают «фальшивые институты» — копируют сайты реальных благотворительных или образовательных организаций, наполняют их контентом и размещают рекламу. Чтобы повысить свой рейтинг в поиске (PageRank), они даже обмениваются ссылками с реальными сайтами.
Огромной проблемой остается **конфиденциальность**. Поисковые истории и клики содержат колоссальный объем личных данных. Показательный случай произошел, когда компания AOL опубликовала (якобы анонимизированные) поисковые запросы пользователей. Журналисты легко вычислили конкретных людей просто по содержанию их поисковых запросов. Google, в свою очередь, постоянно балансирует между сохранением данных для бизнеса и требованиями законов о защите персональных данных.

Социальные сети: сложность политик и новые риски

Социальные сети (Facebook, MySpace и др.) радикально изменили способ общения, но они же принесли новые проблемы с безопасностью и приватностью. Государственные рекомендации часто сводятся к запугиванию родителей темой «хищников», однако исследования показывают, что Интернет не привел к росту похищений детей. Реальные проблемы лежат в другой плоскости:

- **Кибербуллинг:** Если раньше дети могли найти убежище от обидчиков дома, то теперь преследование следует за ними через экраны смартфонов и компьютеров.
- **Чрезвычайная сложность настроек приватности:** Политики безопасности в социальных сетях стали невероятно запутанными. Например, в Facebook пользователю приходилось пробираться через шесть экранов настроек, чтобы понять, кто и что может видеть. Путаница между механизмами opt-in и opt-out приводит к тому, что пользователи по ошибке делают личное публичным.
- **Проблема тегирования и чужих фото:** Пользователь не всегда контролирует свою цифровую тень. Яркий пример произошел в новогодние праздники 2008 года, после убийства Беназир Бхутто: британская пресса опубликовала фотографию ее сына и политического наследника Билала Бхутто, одетого в костюм дьявола на вечеринке в честь Хэллоуина. Это фото было найдено на странице одного из его друзей-студентов в Facebook.
- **Сторонние приложения:** Пользователи часто авторизуют сторонние игры и утилиты, давая им полный доступ к своему профилю. Это приводит к утечкам данных, так как безопасность стороннего разработчика может быть на нулевом уровне.
- **Угрозы публичного поиска:** Функции поиска внутри соцсетей могут индексировать данные, которые пользователи считали скрытыми. Исследователи назвали эту проблему «Go Fish», демонстрируя, как с помощью поисковых запросов можно извлекать закрытую информацию.

Социальные сети пытаются охватить почти все аспекты человеческого поведения, но именно эта тотальность делает их управление безопасностью кошмаром для инженеров. Пользователи оказываются втянутыми в сложную паутину настроек, где одна ошибка может привести к репутационным или даже физическим рискам.

Технологии обеспечения приватности и Электронные выборы

По мере того как бизнес и повседневная жизнь переходят в онлайн, огромные массивы информации начинают собираться корпорациями. Лицензионные серверы, DRM-системы и трекеры знают о пользователях всё. Но что делать тем, кому приватность нужна не просто из соображений комфорта, а для выживания, защиты коммерческой тайны или соблюдения прав человека?
Чтобы понять спектр проблем, рассмотрим семь гипотетических пользователей, чьи задачи требуют разных подходов к приватности:

1. **Эндрю** — миссионер в Техасе, чей сайт читают обращенные в его веру люди в Саудовской Аравии (где смена религии карается смертью). Ему нужно общаться так, чтобы саудовская тайная полиция не могла отследить факт переписки.
2. **Бетти** — 10-летняя дочь пользователя. Ей нужно оставаться анонимной в сети, чтобы избежать внимания хищников.
3. **Чарльз** — инженер в компании, работающей в режиме секретности (stealth mode). Он ведет блог в нарушение корпоративных правил и должен скрыть свое авторство.
4. **Дай** — правозащитница во Вьетнаме, контактирующая с профсоюзными активистами. Полиция регулярно ее досматривает.
5. **Элизабет** — аналитик в инвестиционном банке, изучающая цели для слияний и поглощений. Ей нужно скрывать факт исследования от целевых компаний.
6. **Фироз** — гей в Тегеране, где гомосексуальность карается смертной казнью. Ему нужно скачивать специфический контент без риска быть пойманным.
7. **Грациано** — магистрат в Палермо, создающий анонимную горячую линию для доносов на мафию. Он должен защитить информаторов от коррумпированных полицейских.

Анонимная электронная почта: Тайна обедающих криптографов и миксеры

Главная угроза для анонимности — это не обязательно взлом шифра, а **трафик-анализ**. Даже если сообщение зашифровано, сам факт общения между Эндрю и его последователями может выдать их.
В 1981 году Дэвид Чаум предложил концепцию «Тайны обедающих криптографов». Несколько криптографов ужинают за круглым столом. Кто-то из них тайно оплачивает счет, но они не хотят раскрывать, кто именно (возможно, чтобы избежать благодарности или, наоборот, мести). Протокол позволяет им математически гарантировать, что никто из участников не сможет вычислить плательщика, даже если все они сговорятся. Это обеспечивает **безусловную анонимность** отправителя и получателя.
На практике эта идея реализована в **сетях-миксерах (анонимных релейерах)**. Пользователь шифрует сообщение ключом релейера, указывает конечный адрес и отправляет пакет на релейер. Релейер расшифровывает пакет, видит следующий адрес (или конечного получателя) и пересылает его дальше. Таким образом, наблюдатель, контролирующий канал, видит лишь то, что пользователь связался с релейером, но не знает, что находится внутри или куда сообщение пойдет дальше.
Эволюция анонимных релейеров прошла несколько этапов:

- **Цифровые псевдонимы (Nymservers):** Позволяли пользователям получать и отправлять почту под вымышленными именами.
- **Цепочки релейеров:** Сообщение проходило через несколько узлов. Если один узел скомпрометирован (например, является «ловушкой» спецслужб), он видит только предыдущий и следующий узел, но не всю цепочку.
- **Mixmaster:** Стандарт, который фиксировал размер сообщений и использовал сложные маршруты, чтобы затруднить трафик-анализ по объему и времени пакетов.

Однако у таких систем были уязвимости. Спецслужбы могли запускать собственные узлы (honeypots) для сбора статистики, а хакеры могли проводить DoS-атаки на релейеры, заставляя их раскрывать информацию или просто выводя систему из строя.

Анонимный веб-серфинг: Tor

Для анонимизации веб-трафика был создан проект **Tor (The Onion Router)**, изначально разработанный Военно-морскими силами США. Идея заключалась в том, чтобы защитить коммуникации разведчиков и агентов, пропуская трафик через распределенную сеть узлов.

Как это работает: Клиентское ПО Tor строит цепочку из нескольких серверов. Данные шифруются послойно (как луковица). Первый узел снимает первый слой шифра и видит, куда идти дальше, но не видит содержимого. Второй узел снимает второй слой и так далее. Только последний узел (exit node) видит открытый трафик и отправляет его получателю.
Уязвимости Tor:

1. **Вредоносные exit-узлы.** Поскольку последний узел видит расшифрованный трафик, злоумышленник может запустить свой exit-узел и перехватывать незашифрованные данные. В одном из случаев таким образом были перехвачены пароли от веб-почты сотрудников нескольких посольств.
2. **Побочные каналы (Side channels).** Браузерные плагины (Flash, ActiveX) или скрипты могут инициировать прямые соединения, игнорируя прокси Tor и раскрывая реальный IP-адрес пользователя.
3. **Глобальные противники.** Спецслужбы (например, АНБ), контролирующие значительную часть магистрального интернета, могут коррелировать время и объем входящего и исходящего трафика на разных узлах, деанонимизируя пользователей.
4. **Анализ структуры веб-страниц.** Даже если трафик зашифрован, разные веб-страницы имеют уникальный «отпечаток» (размер загружаемых данных, тайминги запросов). Наблюдатель может определить, какую именно страницу посещает пользователь, просто анализируя паттерны трафика.

Конфиденциальные и анонимные телефонные звонки

Самый простой способ анонимной связи — **предоплаченные мобильные телефоны** (сим-карты, купленные за наличные). Однако и здесь есть риски. Например, лидеры «Аль-Каиды» были пойманы потому, что использовали сим-карты из одной и той же партии, купленной в Швейцарии, что позволило

спецслужбам вычислить их по метаданным.
Альтернатива — **VoIP (например, Skype)**. Skype шифрует трафик, но является централизованной системой. Правозащитники (как Дай) часто используют комбинацию: Skype для голоса, PGP для почты и Tor для скрытия факта использования Skype. Однако в условиях тотальной слежки важна и физическая безопасность: защита от прослушивающих устройств в комнате, использование одноразовых устройств и тщательное соблюдение оперативной маскировки.

Шифрование электронной почты (PGP)

Pretty Good Privacy (PGP) использует модель «Сети доверия» (Web of Trust), где пользователи лично подписывают открытые ключи друг друга, избегая необходимости в централизованных удостоверяющих центрах.
Однако PGP столкнулась с серьезной проблемой **юзабилити**. Исследование Уиттен и Тайгара («Почему Джонни не может шифровать») показало, что обычные пользователи не понимают, как правильно генерировать ключи, управлять ими и подписывать сообщения. В результате система либо не использовалась, либо использовалась с критическими ошибками.
Кроме того, никакая математика не защищает от **«криптоанализа с применением резинового шланга»** (вымогательства и пыток), когда злоумышленник просто требует передать ключ или пароль под угрозой расправы.

Стеганография и контрмеры для криминалистики

Если шифрование привлекает внимание (сам факт наличия шифротекста подозрителен), на помощь приходит **стеганография** — скрытие самого факта передачи данных.

- **MP3stego:** Скрытая передача данных в аудиофайлах MP3 путем модификации наименее значимых битов.
- **Стеганографические файловые системы:** Позволяют скрыть не только содержимое, но и существование файла. Диск выглядит заполненным случайным шумом, но при вводе правильного пароля «проявляются» скрытые данные.

Контрмеры для криминалистики: Чтобы скрыть свои действия от forensic-экспертов, пользователи применяют различные трюки. Например, удаление лицензионных ключей из Windows Media Player (что делает скачанные фильмы

нечитаемыми и выглядит как обычная ошибка, а не намеренное сокрытие улик), использование множества устройств или сокрытие данных в «слепых зонах» операционной системы.

Собирая всё воедино

Возвращаясь к нашим семи пользователям, можно увидеть, что идеального решения не существует:

- **Эндрю** (миссионер) не может использовать открытые каналы. Ему нужны сложные цепочки релейеров и стеганография.
- **Бетти** (дочь) нуждается в родительском контроле и обучении, а не в сложных криптографических инструментах.
- **Чарльз** (инженер) должен использовать анонимные сети (Tor) и псевдонимы, чтобы скрыть корпоративные следы.
- **Дай** (правозащитница) должна комбинировать шифрование (PGP), анонимизацию (Tor) и физическую осторожность.
- **Элизабет** (аналитик) может использовать корпоративные VPN и изолированные среды, но ей нужно скрывать паттерны своих запросов.
- **Фироз** (гей в Тегеране) вынужден использовать глубокие слои анонимизации и стеганографию, так как риск смертной казни крайне высок.
- **Грациано** (магистрат) должен защитить не только канал связи, но и базу данных информаторов от коррумпированных инсайдеров.

Главный вывод: **анонимность любит компанию**. Чем больше людей используют инструменты скрытия, тем эффективнее они работают. Идея «эскроу ключей» (передачи копий ключей государству) отвергается криптографами, так как это создает единую точку отказа и нарушает базовые принципы безопасности.

Электронные выборы

Переход к электронным системам голосования стал одной из самых острых проблем на стыке технологий и политики. Толчком послужили события во Флориде в 2000 году (выборы Буша против Гора), когда механические проблемы с бюллетенями вызвали масштабный кризис. В ответ Конгресс США выделил миллиарды долларов на модернизацию систем голосования, что привело к массовому внедрению **DRE (Direct-Recording Electronic)** — систем прямой электронной записи, где голосующий нажимает кнопки на экране, а машина

сохраняет результат.
Однако электронные выборы породили фундаментальный парадокс безопасности:

1. Избиратель должен быть уверен, что его голос **учтен**.
2. Избиратель **не должен иметь возможности доказать** никому другому, за кого именно он проголосовал (иначе становится возможным подкуп голосов или запугивание избирателей).

В традиционном бумажном голосовании это достигается тем, что бюллетень опускается в урну анонимно, но физический след остается для возможного пересчета. В электронных системах (DRE) машина просто записывает цифру в память.

Уязвимости электронных систем

Анализ показал, что DRE-машины крайне уязвимы для программных ошибок и целенаправленных атак:

- **Исследование Diebold (Университет Джонса Хопкинса):** Эксперты обнаружили, что программное обеспечение машин Diebold не имеет независимого аудита, содержит критические уязвимости и позволяет злоумышленнику с физическим доступом к машине (например, члену избирательной комиссии) подменить результаты голосования или внедрить вредоносный код, который «тихо» меняет голоса.
- **Флорида (2007):** Независимый обзор выявил, что машины не обеспечивают тайну голосования должным образом и могут быть скомпрометированы через сетевые интерфейсы или карты памяти.
- **Огайо (Отчет EVEREST):** Масштабное исследование подтвердило, что электронные системы не могут гарантировать ни точность, ни безопасность, ни возможность независимого пересчета голосов без бумажного следа.

Бумажные следы и альтернативы

Эксперты по безопасности (такие как Ави Рубин и Ребекка Меркури) настаивают на том, что любая электронная система голосования **обязана** генерировать верифицируемый бумажный след (VVPAT). Избиратель должен видеть на экране не только цифровой выбор, но и распечатанный бюллетень за прозрачным стеклом, подтверждать его, и только после этого бумажный след должен падать

в защищенную урну. Это позволяет провести ручной пересчет в случае спора.
Альтернативой DRE являются **системы оптического сканирования**, где избиратель заполняет бумажный бюллетень, а машина считывает его. Это сохраняет физический след, но снижает риски, связанные с уязвимостью сложного программного обеспечения сенсорных экранов.
Вывод, к которому пришло сообщество специалистов по безопасности, неутешителен для сторонников полной цифровизации: **электронное голосование (в формате DRE) несет в себе неприемлемые риски**. Без независимого, верифицируемого избирателем бумажного следа доверять результатам выборов, проведенных на «черных ящиках» (машинах с закрытым кодом), нельзя.

Итоги и взгляд в будущее

Инженер безопасности XXI века

Защита информации в компьютерных системах больше не является чисто научной дисциплиной — это полноценная инженерная практика. Инженер по безопасности XXI века несет ответственность за системы, которые постоянно эволюционируют и сталкиваются с меняющимся спектром угроз.
Чтобы оставаться эффективным, специалист должен постоянно повышать свою техническую грамотность: отслеживать новейшие атаки, осваивать новые инструменты и следить за изменениями в правовой и политической сферах.
Однако одной лишь техники недостаточно. Инженеру необходима твердая интеллектуальная база: понимание криптологии, контроля доступа, потоков информации, сетевых технологий и обнаружения сигналов.
Не менее важно понимать основы менеджмента: как работает бухгалтерский учет, финансы и бизнес-процессы клиента. Но самый главный навык — это умение управлять технологиями и эффективно участвовать в процессе эволюции систем для удовлетворения меняющихся бизнес-потребностей. Способность говорить на одном языке с бизнес-лидерами, а не только с другими инженерами, имеет решающее значение, а практический опыт играет огромную роль. Людей с таким сочетанием навыков вряд ли ждет безработица или скука.

Тень security-индустриального комплекса

Однако у профессии есть и темная сторона. Бурный рост security-индустриального комплекса после терактов 11 сентября 2001 года и откровенное нагнетание страха со стороны многих правительств стали серьезным шрамом на лице мира и этой профессии.
У инженеров есть долг помочь залечить эту рану. Сделать это можно несколькими путями:

1. **Исследования:** развитие таких дисциплин, как инженерия безопасности и экономика безопасности.
2. **Распространение знаний:** открытое обсуждение реальных механизмов и угроз.
3. **Экономический рост и образование:** именно бедные и необразованные слои населения в наибольшей степени подвержены влиянию демагогов, эксплуатирующих страхи.
4. **Участие в политических дебатах:** конечный и самый важный способ — напрямую взаимодействовать с людьми, которые определяют повестку дня и обсуждают новые угрозы, чтобы не допустить принятия иррациональных решений.

Проблемы для исследований

Несмотря на колоссальный прогресс, перед индустрией стоит ряд нерешенных задач. В первую очередь, срочно нужны новые идеи в области управления оценкой защищенности (evaluation).
На сегодняшний день мы используем совершенно разные и зачастую несовместимые инструменты для измерения уровня защиты, которую можно ожидать от:

- криптографических алгоритмов;
- технических механизмов физической защиты;
- сложного программного обеспечения;
- внутреннего контроля в организациях;
- и, с помощью исследований юзабилити, от людей.

Возникает ряд фундаментальных вопросов:

- Можно ли как-то объединить эти инструменты, чтобы критически важные элементы не выпадали из поля зрения?

- Можем ли мы разработать механизмы оценки лучше, чем Common Criteria, которые сами вендоры в частном порядке считают бессмысленной бюрократией?
- Возможно, стоит применить инструменты, которые экономисты используют для работы с несовершенной информацией: от моделей ценообразования рисков до теории фирмы.
- Нам также необходимы лучшие статистические инструменты для измерения и прогнозирования сбоев.
- И, наконец, мы должны браться за «табуированные» темы. Например, почему «Проблема 2000 года» (Millennium Bug) в итоге не привела к глобальным катастрофам?

Финальная мысль

Вокруг индустрии assurance (подтверждения соответствия) и evaluation выстроился целый бизнес, поддерживаемый горами налоговых денег. Энтузиазм ее адептов зачастую приобретает черты религиозного культа. К сожалению, людей, готовых писать «ересь» и подвергать сомнению устоявшиеся догмы этой индустрии, катастрофически не хватает. Именно за такими «еретиками» — будущее инженерии безопасности.