6 идей развития IT в России

Несмотря ни на что, IT в России живет и развивается. Возможно, не так быстро, как хотелось бы, но все же процесс идет. Здесь, в преддверии Нового года хотелось бы обсудить ряд идей, которые способны подстегнуть и сделать нашу родную отрасль чуточку лучше.

Предлагаемые идеи не будут ультимативными серебряными пулями без изъяна и упрека, что-то они сделают хуже, а что-то лучше. Очень надеюсь, что второго окажется больше, и вы поддержите понравившиеся вам идеи на голосовании в конце статьи. Кроме того, хотелось бы увидеть ваши мысли, идеи и предложения в комментариях к этой статье.

Идея 1. Создание вендоронезависимой операционной системы

Проблема

Санкции в отношении российских компаний и уход с рынка иностранных поставщиков оказали довольно неприятное воздействие на IT-отрасль России. Но если посмотреть на сложившую ситуацию чуть шире, то можно заметить, что это не просто использование IT как рычага политического давления, а проявление куда более негативного явления, а именно цифровой диктатуры.

IT технологии давно переросли стадию детской забавы или увлечения для горстки гиков. Сейчас это социально значимые блага, свободный доступ к которым закрепляется на законодательном уровне. Все это приводит к тому, что производители и поставщики IT-продуктов выходят за рамки обычных организаций и становятся политической силой, способной оказывать на общество существенное влияние.

Разберем это утверждение на примерах:

- До санкций в отношении России мы видели, как социальная сеть Twitter помечает сообщения действующего президента США как дезинформацию.
- Затем по политическим мотивам его вообще заблокировали в большинстве соцсетей.
- Компания Apple монополизировала (есть информация, что скоро это должно закончиться) возможность установки софта на свои гаджеты. Затем, пользуясь сложившейся ситуацией, угрожает другим компаниям немотивированными блокировками.
- Владельцы самой большой в мире социальной сети могут предсказать поведение своих пользователей лучше, чем их родственники или друзья. Потом неожиданно получается, что поддерживаемые ими кандидаты выигрывают на выборах. Случайность?

Надо понимать, что все это лишь «цветочки», и дальше будет только хуже, если диктат вендоров и сервисов технически не ограничивать. Но давайте вернемся в Россию. Что сделали санкции в отношении нас? Они подтолкнули Правительство РФ к развитию национальных IT-решений и в первую очередь операционных систем. На текущий момент у нас почти два десятка «отечественных» операционных систем, разрабатываемых практически таким же количеством независимых команд. Для российских операционных систем действуют существенные протекционные преференции при госзакупках, а некоторым производителям выделяются многомиллиардные льготные госкредиты на развитие. С одной стороны это может показаться правильным решением, с другой стороны это путь в никуда и причин тут несколько.

1. В чем будет заключаться преимущество «российской ОС N» от иностранных Windows или MacOS? А будет оно только в том, что – система «отечественная» и защищена от санкций со стороны западных вендоров. Будут ли покупать подобную систему скажем в Казахстане, Беларуси или в Иране? Очень сомневаюсь. Доказательством этого скепсиса могут послужить уже провалившиеся отечественные IT-проекты, такие как русская альтернатива Википедии «Руниверсалис» или госпоисковик «Спутник». Причина этих провалов одна и таже – проекты не имели никаких преимуществ по сравнению с имеющимися сервисами, за исключением того, что были отечественными.
2. На текущий момент рынок отечественных операционных систем – это только Россия. Нас около 150 миллионов человек. Это крайне мало – всего около 2% от общей популяции homo sapiens на планете, большая часть из которой уже удовлетворены имеющимися системами. Тогда кто, скажите, будет писать софт и драйвера под наши операционки?
3. Вложение денег в одного из отечественных вендоров операционных систем не дает защиты от будущего цифрового диктата со стороны этого вендора.

На основании сказанного давайте сформулируем то, что нам все-таки нужно:

1. Мы хотим иметь операционную систему с защитой от западных санкций.
2. Мы хотим поддержать отечественных разработчиков.
3. Мы не хотим монополии или безальтернативности на рынке операционных систем.
4. Нам не нужны десятки несовместимых между собой операционных систем, крадущих пользователей друг у друга на и без того крохотном рынке.
5. Нашей операционной системе нужна изюминка или конкурентное преимущество по сравнению с имеющимися коммерческими и бесплатными операционными системами.
6. Нашей операционной системе нужна массовость, чтобы производители комплектующих выпускали под нее драйвера, а независимые разработчики – прикладное ПО.

Решение

Как вы заметили, в требованиях присутствуют взаимоисключающие пункты. Это действительно так. Удовлетворить всем им в рамках стандартного подхода по поддержке какого-либо национального продукта невозможно.

Но решение все-же есть, и заключается оно в разработке вендоронезависимой операционной системы. Реализовать ее можно путем создания открытой архитектуры, содержащей всю необходимую документацию, на основании которой любой вендор мог бы создать свой собственный дистрибутив операционной системы, и все подобные дистрибутивы были бы двоично совместимы (в рамках одинаковых процессорных архитектур) между собой.

Давайте посмотрим, как мы с таким подходом закроем ранее обозначенные требования:

1. На основании открытой архитектуры отечественные разработчики создают и поддерживают собственные дистрибутивы операционной системы.
2. Защита отечественных разработчиков, как и сейчас, происходит с применением протекционных мер по госзакупкам.
3. Разные вендоры создают разные дистрибутивы, конкурирующие между собой по качеству реализации, поддержки, а также по наличию дополнительных компонентов. В случаях, когда не требуется коммерческая поддержка или обязательная сертификация, могут использоваться бесплатные дистрибутивы, разрабатываемые студентами ведущих ВУЗов страны. Главное, что все эти системы будут совместимы между собой.
4. Открытые архитектуры разрабатываются для каждого сегмента использования: сервера, рабочие станции, гаджеты и т.д.
5. Основной изюминкой операционных систем, построенных по открытой архитектуре, будет защита от цифрового диктата. Скорее всего подобные операционные системы не будут лучшими операционными системами в мире и коммерческие аналоги будут их в чем-то обходить. Зато правительство любой страны может на их основе построить свою критическую инфраструктуру и будет уверено, что в будущем никакой вендор не сможет выкручивать ему руки.
6. Массовость будет достигаться за счет того, что операционными системами, построенными по открытой архитектуре, будут пользоваться как в России, так и за ее пределами. Например, в Казахстане IT-компании могут некоторое время попользоваться российским дистрибутивом, а потом, в случае необходимости, перейти, скажем, на белорусский или вообще разработать свой собственный. В современных реалия автаркия для России – это регресс. Нас для нее слишком мало

по сравнению с другими странами, которые кооперируются между собой. Соответственно, следуя по этому пути, мы не то что никогда их не догоним, а, наоборот, будем все больше и больше от них отставать. Поэтому нам нужны IT-продукты и технологии, которые будут востребованы не только в России, но и за ее пределами.

Для реализации этой идеи нужно сделать следующее:

1. Создать открытый консорциум, занимающийся развитием открытых архитектур операционных системы.
2. В него должны входить команды разработчиков «российских» операционных систем и отечественной микроэлектроники, а также основные потребители операционных систем: представители госкорпораций, финансового сектора, промышленности, представители регуляторов в области ИБ. Всеми правдами и неправдами необходимо завлекать в консорциум как можно больше иностранных представителей.
3. Консорциум должен выпустить первую открытую архитектуру для операционной системы определенного сегмента (сервера, рабочие станции, гаджеты и др.). Для этого можно провести обратный инжиниринг (reverse engineering) уже существующей операционной системы и взять его результаты за основу.
4. Консорциум должен обеспечить постоянное улучшение архитектуры с выпуском мажорных обновлений не реже одного раза в полгода.
5. Скорость, с которой работают действующие механизмы стандартизации, такие как Росстандарт или ISO, для развития операционных систем недостаточна.
6. Консорциум должен опубликовать и никаким образом не ограничивать доступ к документации на открытые архитектуры операционных систем.
7. Тут важно соблюдение принципа «хочешь заработать сам – дай заработать другим». Чем большее количество людей, пусть даже геополитических оппонентов, будет пользоваться системой, тем больше будет ее поддержка со стороны вендоров комплектующих и независимых разработчиков.
8. Консорциум должен разработать, опубликовать, а затем и постоянно дорабатывать сертификационные тесты на совместимость дистрибутивов с открытой архитектурой операционных систем.
9. Государство должно оставить преференции при госзакупках только операционным системам, доказавшим требуемый уровень совместимости с открытой архитектурой.

Идея 2. Минимизация легального пиратства

Проблема

После объявлений об уходе иностранных вендоров в России зазвучали голоса о легализации пиратства (вот и вот) покинувших российский рынок. Идеи эти во многом эмоциональны и не обдуманы. Слепая их реализация приведет к существенным негативным последствиям:

1. Это убьет российскую разработку ПО. Платные отечественные разработки не смогут конкурировать с ворованными импортными.
2. Упадут объемы продаж всего софта. Разрушится потребительская культура покупки софта. Зачем покупать, когда можно украсть?

3. Увеличится число взломов компаний, использующих пиратский софт. Весь современный софт оснащается защитой от нелицензионного использования. При легализации пиратства возникает вопрос, где брать взломщики этой защиты? Большинство пиратских сайтов и торрент-трекеров заблокированы Роскомнадзором. Кроме того, кто даст гарантии, что имеющиеся взломщики не сделаны геополитическими оппонентами и не содержат в себе вредоносный код?

При всем при этом возникают ситуации, когда без пиратства, к сожалению, не обойтись. Это касается:

1. импортного софта, распространяемого по подписке, в случаях, когда эту подписку невозможно легально продлить, и при этом нет российских аналогов.
2. а также драйверов устройств, которые вендор отказывается предоставлять (например, на данный момент нет легальной возможности получить драйвера под VMware ESXi для промышленных видеокарт NVidia Tesla) или разрабатывать под требуемую операционную систему (например, ту, что будет разработана в рамках реализации идеи 1). Вы можете спросить, причем тут драйвера и пиратство? Дело в том, что драйвера – это тоже софт, соответственно его использование регулируется лицензионным договором, так называемым «Соглашением с конечным пользователем» (End User License Agreement, EULA), которое мы все всегда принимаем не читая, ставя галочку и нажимая кнопку Next во время инсталляции. В подавляющем большинстве в EULA стоит запрет на исследование и обратный инжиниринг драйверов, а без этого невозможно разработать драйвера самостоятельно.

Решение

Легализовывать пиратство можно тогда, когда сделано все возможное, чтобы его избежать, но этого оказывается недостаточно, и страдают легитимные пользователи. Действовать при этом нужно следующим образом:

1. Легитимный пользователь софта, который из-за санкций не может продолжать пользоваться этим софтом, а русских аналогов его не существует, должен подать заявку в уполномоченный государственный орган.
2. На основании заявки уполномоченный орган осуществляет временное принудительное лицензирование (с юридической точки зрения) и санкционирует разработку системы нейтрализации защиты софта от нелицензионного использования (легальный взломщик).
3. На основании полученного разрешения легитимный пользователь самостоятельно или с привлечением третьих лиц разрабатывает и использует легальный взломщик, который при этом перестает считается вредоносной программой.
4. В отношении драйверов следует поступить более радикально. Нужно явно лишить всех вендоров права запрещать исследования и обратный инжиниринг драйверов. А в случаях, когда разработчик отказывается легально предоставлять спецификации устройства узаконить самостоятельную разработку драйверов на основании самостоятельно полученных спецификаций. Это даже не способ противодействия санкциям, а способ защиты «права на ремонт». Например, у вас есть замечательный старый сканер, а под новую операционку драйверов нет и не будет. Производитель фактически вынуждает вас выбросить работающую вещь на помойку, чтобы затем вы купили у него такую же (если не хуже), но новую.

Идея 3. Отмена экспортных ограничений в отношении средств защиты информации, не предназначенных для защиты гостайны

Проблема

Рынок отечественных ИБ продуктов практически полностью ориентирован на удовлетворение потребностей в сертифицированных ФСТЭК России или ФСБ России средствах защиты информации (СЗИ). Данные потребности генерируются государством путем принятия различных законов и подзаконных актов, требующих построения корпоративной системы защиты информации с использованием сертифицированных средств. В целом это неплохо – это внутренний протекционизм, позволяющий поддержать российские компании и сохранить отечественную школу разработки.

Проблема в другом. Действующее законодательство содержит нормы экспортного контроля, не позволяющие свободно экспортировать сертифицированные СЗИ зарубеж. Как следствие, потенциал роста отечественных вендоров фактически ограничен только российским рынком. Если для средств защиты гостайны эти ограничения понятны, хотя принцип защиты «безопасность через неясность (security through obscurity)» считается крайне спорным, то для других сертифицированных СЗИ наличие подобных ограничений вызывает недоумение.

Решение

Необходимо упразднить экспортные ограничения для средств защиты информации, не предназначенных для защиты гостайны. В первую очередь это касается криптографии, хотя справедливо и для остальных типов СЗИ.

На сегодняшний день мы имеем парадоксальную ситуацию. Сертифицированное средство криптографической защиты информации (СКЗИ) «КриптоПРО CSP» можно свободно скачать с сайта производителя, а вот вывезти ноутбук с ним за границу нельзя. Возникает резонный вопрос, чего Россия хочет добиться существованием подобных ограничений? История говорит о том, что они появились как ответ на аналогичные ограничения со стороны западных стран, но с тех пор прошла уйма времени. Шифровальные ГОСТы – то, что лежит в основе всех российских СКЗИ, стали открытыми. Соответственно, врагам, чтобы разобраться с тем, как мы шифруем данные, не нужно покупать наше СКЗИ, достаточно просто ознакомиться с открытыми документами.

Критики данного утверждения могут привести контрпример с продажей зарубеж аппаратного шифратора, разработанного с защитой от утечки по сторонним каналам (например, по каналу побочных электромагнитных излучений и наводок – ПЭМИН или TEMPEST, как говорят на западе). Требования, на основании которых строится данная защита, секретны, соответственно, продажа подобного шифратора зарубеж раскроет содержание секретного документа. Логика в этом утверждении есть, но она разбивается о текущие жизненные реалии:

1. В стране работают десятки международных компаний. Кто им запрещает купить, локально исследовать, а затем через Интернет передать вражеским спецслужбам сведения о подобном шифраторе?
2. Кто мешает рядовому гражданину Российской Федерации купить такой шифратор, сделать на него обзор и опубликовать в Интернете? К слову говоря, на Ютубе уже полно каналов (например, КРУПНОКАЛИБЕРНЫЙ ПЕРЕПОЛОХ), где идет детальный анализ действующих образцов российский вооружений, а секретов там гораздо больше, чем в нашем несчастном шифраторе.

Сертифицированная криптография изменяется очень медленно. Новые ГОСТы выходят редко, а основополагающим документам, таким как ПКЗ-2005 или Приказ ФАПСИ N 152, уже почти по 20 (!) лет. В свое время мне для удовлетворения их требований пришлось разработать open source систему учета криптоключей и шифросредств, так как в чистом виде эти документы исполнить не реально. Они не знают ни про ассиметричную криптографию, ни про передачу ключей по сетям связи, ни про распределенную генерацию ключей, ни про разделение секрета, а это то, с чем живет любая российская организация с крупной филиальной сетью.

Скажу честно, я понятия не имею о секретных требованиях к СКЗИ, но не думаю, что они меняются чаще ГОСТов или основополагающих документов. А раз так, то их содержимое уже скорее всего уже давно известно потенциальным врагам, ведь ни один секрет не может оставаться таковым вечно.

И после всего этого мы будет продолжать считать, что экспортный контроль позволяет обезопасить наши средства защиты от утечки в адрес вражеских спецслужб?

Второй глобальной целью экспортного контроля можно считать то, что «мы» продаем «им» только слабые шифраторы, чтобы затем «мы» смогли «их» прослушивать. Но опять-таки, существуют открытые ГОСТы, существуют открытые криптобиблиотеки, существуют открытые курсы по криптографии. Все те, кого мы хотим послушать, уже давно не пользуются промышленными шифраторами, а используют инструменты с открытым исходным кодом или вообще собственные разработки. История о наркобароне Эль Чапо, который построил собственную шифрованную сеть сотовой связи, – яркий тому пример.

На текущий момент действенный контроль спецслужбами криптокоммуникаций возможен только при непосредственном получении ключей шифрования либо при внедрении в процесс обработки информации на стадии, когда та находится в открытом виде. Война с Телеграмом или данные о закладках АНБ, опубликованные Сноуденом, тому явное подтверждение.

Ну и наконец, третьей целью экспортного контроля можно считать ограничение распространения СКЗИ как возможных компонентов для построения систем вооружений. В отношении программных СКЗИ подобное утверждение – полный абсурд, в чем мы убедились ранее. С программно-аппаратными комплексами чуть интересней, но не более. Сложно представить, в какой компонент вооружения можно было бы пристроить российский шифратор, причем таким образом, чтобы он прям дал оружию убер фишку, по сравнению с обычным ПК с работающим OpenVPN шлюзом. Единственно потенциально опасной вещью, которая пришла мне в голову, может быть сврехминиатюрная микросхема криптопроцессор, которую можно было бы встроить в дроны и боевую робототехнику. Но применительно к России это даже не смешно. Практически все

отечественные шифраторы построены на базе микропроцессоров общего назначения, либо используются ПЛИС Xilinix (поглощена AMD) или Altera (поглощена Intel). Создать на их базе аппаратный шифратор может любой грамотный выпускник ВУЗа соответствующей специальности.

Таким образом, можно с полной уверенностью утверждать, что существующие механизмы экспортного контроля сертифицированных СЗИ являются атавизмами времен первой холодной войны. При минимальной практической ценности они приносят государству существенные издержки, как в виде затрат на свою реализацию, так и в виде недополученной прибыли российских вендоров.

Пусть другие страны продают ослабленные продукты (даже если об этом открыто и не говорят), мы будем продавать то, чем пользуемся сами. Это даст нашей продукции конкурентное преимущество, а для страны послужит бонусом как в становлении «мягкой силы» (повышении влияния государства на другие страны не военными способами), так и в противодействии попыткам международной изоляции.

Идея 4. Легализация отсрочек для IT-специалистов

Проблема

Прошедшая частичная мобилизация привела к значительному оттоку IT-специалистов за границу. Часть оставшихся специалистов была мобилизована, других просто не призвали, а третьи получили отсрочку. Несмотря на то, что власть и СМИ во всю трубят о том, что IT-отрасль имеет стратегическое значение, механизмы предоставления отсрочек, мягко скажем, далеки от совершенства. Это, в свою очередь, порождает неуверенность IT-специалистов в завтрашнем дне и создает дополнительное давление на отток мозгов за границу.

Решение

Все имеющиеся механизмы отсрочки от частичной мобилизации должны быть прописаны на уровне федеральных законов. Люди должны четко понимать, попали они под отсрочку или нет. У них должно быть явное свидетельство предоставления отсрочки, понимание ее длительности и условий отзыва.

Следует отдать должное Минцифре России и лично министру Максуду Шадаеву за их неоценимый вклад в сохранение кадрового потенциала IT-отрасли России при проведении частичной мобилизации. На фоне других министерств и ведомств они сделали, пожалуй, максимум из того, что было в их силах в сложившейся на тот момент ситуации.

Однако, частичная мобилизация закончилась, аврала нет, и от «рабочих порядков» Министерства обороны РФ по предоставлению отсрочек следует перейти к правке федеральных законов и приданию всей этой процедуре видимой для граждан легитимности. Текущие механизмы предоставления отсрочек абсолютно не прозрачны.

Идея 5. Обучение навыкам коллективной работы IT-специалистов в ВУЗах

Проблема

В России существует хорошая высшая школа подготовки IT-специалистов. Проблема в том, что она готовит только специалистов-одиночек и совершенно не учит командной работе. Хабр завален статьями о том, как IT-специалисты не могут коммуницировать друг с другом, как они не могут распределить обязанности внутри команды, или о том, как они в принципе не могут ее сформировать. Множество этих проблем можно было бы избежать, если бы ВУЗ готовил к командной работе. Причем не просто преподавал бы ее на лекциях, а фактически заставлял по ее правилам жить.

Решение

В высшей школе должна быть легализована и поощряться практика коллективного выполнения курсовых и дипломных работ.

Подобные командные работы должны быть больше по объему и сложнее по содержанию, чем обычные курсовики или дипломы. Они должны обеспечивать видимый результат от каждого члена команды.

Но как этого добиться? Как вариант, можно перейти от обычных соло-курсовиков по одному предмету к групповым кросс-курсовикам сразу по нескольким.

Например, на третьем курсе студенты изучают «Вычислительные сети» и «Криптографию». По каждой из этих дисциплин у них запланирован обычный соло-курсовик, скажем, «Разработка системы удаленного управления компьютером» по сетям и «Разработка системы шифрования файлов» по криптографии. Эти соло-курсовики можно было бы объединить в один кросс-курсовик «Разработка системы удаленного управления компьютером с использованием шифрованных каналов передачи данных». При этом для обеспечения коллективной работы расширить задание кросс-курсовика, скажем, использованием нескольких сетевых протоколов (например, IPv4 и IPv6) и реализацией нескольких протоколов криптографической защиты данных.

Дипломные работы, в идеале, должны стать чем-то вроде мини-стартапа. Желательно, чтобы над ними трудились представители нескольких специальностей. Например, маркетологи с соответствующей специальности занимались бы анализом рынка и выявлением требований к продукту, экономисты бы делали бизнес-план стартапа, программисты, писали бы код, а менеджеры занимались бы координацией и планированием работ.

Подобный подход немного снизит индивидуальные навыки студентов по некоторым дисциплинам, но даст существенных толчок в развитии навыков коллективной работы. Тут будет все: и проблема сбора команды, и организация социального взаимодействия внутри команды, и переманивание участников между командами, и многое другое, с чем выпускникам придется столкнуться в реальной жизни. В идеале ВУЗы должны перестать плодить специалистов-одиночек, а перейти к выпуску готовых слаженных команд.

Ну и про наших любимых воробушков-социофобушков тоже не будем забывать. Возможность групповых работ должна оставаться именно возможностью, а не строгой обязаловкой.

Идея 6. Создание IT-судов

Проблема

Давайте взглянем на ряд более чем странных уголовных дел:

1. Суд в Томске вынес обвинительный приговор за использование защищённого мессенджера VIPole.
2. Россиянина приговорили к 2 годам лишения свободы и штрафу ₽100 тысяч за создание и продажу программы с SQLmap.

После ознакомления с материалами этих дел можно сказать, что текущий уровень судебной защиты по IT-делам оставляет желать много лучшего. Причина этого довольна банальна – судьи имеют слабое представление о работе информационных технологий и слишком сильно полагаются на мнения экспертов.

В представленных выше материалах можно заметить, что эксперты фактически являются переводчиками материалов дел с «компьютерного» непонятного для судьи языка на «общежитейский» понятный для судьи. После такого перевода судья и принимает те или иные решения. Важно то, что уровень влияния эксперта на решение судьи недопустимо высок.

Например, при рассмотрении дел по ст. 273 УК РФ краеугольным камнем справедливого судебного решения является правильная классификация того, является ли рассматриваемая программа вредоносной или нет. В материалах же второго дела мы видим, что это судьбоносное решение фактически принимает эксперт, причем мотивируя его результатами работы антивируса. С таким же успехом можно признать обычный кухонный нож оружием массового уничтожения, ведь он виновен в смерти гораздо большего числа людей, нежели любое другое оружие в истории человечества.

Ошибкой будет считать, что в вынесении подобных решений лежит персональная вина конкретных судей. Проблема IT безграмотности судов носит системный характер. Государству следует признать, что абсолютно невозможно подготовить весь имеющийся корпус судий в области IT технологий. Причем не просто прочитать им дополнительный набор лекций, а подготовить так, чтобы они достаточно глубоко разбирались в сути IT процессов, и большую часть судейского мнения выносили самостоятельно, а не как сейчас, с оглядкой на экспертов. Мало того, что судей нужно один раз обучить, их нужно затем постоянно дообучать, поскольку технологии не стоят на месте и то, что было пару лет назад острием научной мысли, сейчас уже прошлый век, а технологии скакнули далеко вперед.

Мне, например, очень интересно, как суд общей юрисдикции будет разбирать дела, связанные с цифровым рублем, который хотят запустить в ближайшее время. Ведь это не нал, не безнал, а вообще третья форма денег, суть которой на сегодняшний день не все банкиры понимают, что уж говорить о людях, далеких от IT и финансового сектора.

Решение

Как произошло ранее разделение врачей, строителей и других профессий по специализациям, так сейчас должно произойти разделение судей по областям, в пределах

которых они могут выносить качественные судейские решения. Должен появиться выделенный корпус IT-судей.

Судопроизводство должно уйти от территориального принципа подсудности к принципу разделения по специализациям. Все IT-шные дела (для начала ст. УК РФ: 272-274) должен судить отдельный корпус IT-судей, имеющий специальную подготовку, и постоянно совершенствующихся в области IT, другими делами при этом они заниматься не должны.

Создание корпуса IT-судей не отменяет института судебной экспертизы. Задача в том, чтобы на экспертов переложить рутинные вопросы, такие как, поиск артефактов преступления, сбор и систематизацию данных и прочее. Основное же мнение должен формировать судья самостоятельно. Как минимум он должен понимать, что программа форматирования диска, с помощью которой можно уничтожить все имеющиеся на компьютере данные, не является вредоносной, вне зависимости от того, что говорит по этому поводу антивирус.

Заключение

Спасибо, что дочитали до конца. Я очень сильно старался не растекаться мыслью по древу, но статья все равно получилась большой. По-хорошему по каждой идее нужно было бы выпускать отдельную статью, где более детально рассматривать все ее плюсы и минусы. Здесь же очень многое оказалось за кадром. Но что сделано, то сделано, в любом случае у нас есть комментарии. Прошу проголосовать за понравившиеся вам идеи. Хабр читает множество людей, среди которых есть те, кто обладает существенным политическим влиянием. Кто знает, может быть, что-то из предложенного мы в ближайшее время увидим реализованным в нашей повседневной жизни.