Security Engineering: часть 4. Экономика

Published: 09.06.2026 15:27 | Updated: 15.06.2026 10:18

Экономика

В предыдущих частях мы изучили как строить защиту (криптография, протоколы, контроль доступа), то эта часть объясняет, почему системы часто остаются незащищёнными, несмотря на наличие технических решений. Есть мнение, что многие провалы в безопасности происходят не из-за слабости математики или кода, а из-за **неправильных стимулов** (incentives). Безопасность — это не скалярная величина, а отношение власти. Технические меры бессильны, если экономические стимулы участников системы направлены против них.

1. Классическая экономика и информационные товары

Начнем с основ микроэкономики, применяя их к миру IT.

- **Монополия:** рынки ПО склонны к монополии из-за сетевых эффектов (чем больше людей используют Windows, тем выгоднее писать под неё софт). Монополист диктует цены и условия, часто игнорируя безопасность, так как у пользователей нет выбора.
- **Общественные блага (public goods):** безопасность часто является общественным благом. Если мой компьютер защищён от вирусов, это полезно и вам (я не заражу вас). Но поскольку я не получаю прямой выгоды от защиты других, я могу экономить на безопасности, перекладывая риски на соседей (экстерналии).
- **Информационная экономика:** предельные затраты на копирование ПО близки к нулю. Это создаёт проблемы ценообразования и ведёт к практике **ценовой дискриминации** (разные цены для разных групп) и **привязки** (lock-in), когда пользователю дорого перейти на другую платформу.

2. Теория игр (game theory)

Безопасность — это взаимодействие рациональных агентов (защитников и нападающих, или разных участников одной системы).

- **Дилемма заключённого:** часто всем выгодно сотрудничать (инвестировать в безопасность), но индивидуально выгоднее схитрить (сэкономить), надеясь на других. В результате все оказываются в проигрыше (небезопасная среда).
- **Эволюционные игры («ястребы и голуби»):** моделируют поведение в популяции. Если «агрессоров» (хакеров) становится слишком много, система вырабатывает иммунитет или меняет правила.
- **Слабое звено vs. сумма усилий:**
  -- Слабое звено (weakest link): безопасность всей системы определяется самым небрежным участником (например, пароль самого глупого сотрудника). Здесь трудно мотивировать всех быть идеальными.
  -- Сумма усилий (sum of efforts): безопасность растёт по мере вклада каждого (например, борьба со спамом или вирусами: чем больше людей обновляют антивирусы, тем безопаснее всем). Здесь стимулы работают лучше.

3. Экономика безопасности и надёжности

Почему Windows так небезопасна? Разбираем этот вопрос через призму экономики.

- **Жизненный цикл платформы:** на этапе захвата рынка (как было с Windows в 90-е) вендор жертвует безопасностью ради скорости выхода продукта и удобства для разработчиков приложений («комплементариев»). Безопасность тормозит развитие экосистемы.
- **Смена приоритетов:** когда монополия уже установлена, вендор начинает добавлять безопасность, но часто делает это так, чтобы усилить привязку пользователя (DRM, закрытые протоколы), а не защитить его данные.
- **Моральный риск (moral hazard):** если банк знает, что убытки от мошенничества с картами покроет страховка или сам клиент (из-за сложных условий договора), у банка нет стимула вкладываться в дорогую защиту. Напротив, в США (Regulation E), где банк несёт ответственность за спорные транзакции, банки инвестируют в безопасность гораздо активнее.

4. Глубокий анализ «рынка лимонов» (market for lemons) в безопасности

Концепция Джорджа Акерлофа о «рынке лимонов» (где продавцы знают о качестве товара больше, чем покупатели) является фундаментальной для понимания провалов в кибербезопасности.

- **Асимметрия информации:** производитель ПО знает о багах и уязвимостях своего продукта гораздо больше, чем покупатель. Пользователь не может «протестировать» безопасность программы перед покупкой так же легко, как он может проверить работу текстового процессора.
- **Гонка ко дну (race to the bottom):** поскольку покупатель не может отличить безопасный продукт от небезопасного, он не готов платить премию за безопасность. Это создаёт стимул для производителей экономить на тестировании и защите, выпуская дешёвые, но уязвимые продукты. Рынок заполняется «лимонами».
- **Пример с антивирусами:** пользователи часто покупают самый дешёвый антивирус или используют бесплатный, полагая, что «все они примерно одинаковы». Это снижает доходы компаний, инвестирующих в серьёзные исследования угроз, и вынуждает их либо снижать качество, либо переходить на модели монетизации, нарушающие приватность (продажа данных пользователей).
- **Решение через репутацию и стандарты:** единственный способ бороться с этим — создание механизмов сигнализирования качества (сертификаты, бренды, открытые аудиты). Однако, как показывает практика с оценками Common Criteria, эти механизмы сами могут стать объектом манипуляций, если стимулы оценивающих сторон также искажены.

5. Экономика приватности (privacy): парадокс поведения

Подчеркнем разрыв между декларируемыми ценностями людей и их реальным поведением.

- **Парадокс приватности:** опросы показывают, что люди заявляют о высокой ценности своей приватности, но на практике готовы обменять личные данные на незначительные выгоды (скидку в магазине, доступ к бесплатному приложению, удобный сервис).
- **Причины:**
  -- Непонимание долгосрочных рисков: люди плохо оценивают вероятностные риски будущего ущерба (кража личности, дискриминация при страховании) по сравнению с немедленной выгодой.
  -- Усталость от принятия решений: постоянные запросы на согласие (cookie banners, политики конфиденциальности) приводят к тому, что пользователи механически нажимают «Принять», не читая.
  -- Эффект безбилетника: пользователи надеются, что другие защитят экосистему, или что регуляторы решат проблему за них.
- **Ценовая дискриминация:** сбор данных позволяет компаниям практиковать совершенную ценовую дискриминацию (первой степени), назначая каждому пользователю максимальную цену, которую он готов заплатить. Это перераспределяет излишек потребителя в пользу производителя — экономически выгодно компаниям, но вредно для общества в целом. Есть утверждение, что именно желание избежать такой дискриминации должно мотивировать защиту приватности, но большинство людей этого не осознаёт.
- **Внешние эффекты (externalities):** утечка данных одного человека может навредить другим (например, через социальную инженерию с использованием украденной информации о друзьях жертвы). Рынок не учитывает эти негативные внешние эффекты, поэтому уровень защиты данных ниже социально оптимального.

6. Экономика DRM (Digital Rights Management): кто реально выигрывает?

История подтвердила догадки экспертов, что усиление DRM выгодно не правообладателям контента (музыкальным лейблам, киностудиям), а владельцам платформ.

- **Смена баланса сил:** изначально DRM продвигалась как защита авторов от пиратов. На деле же она стала инструментом контроля над рынком сбыта.
  -- Пример Apple iTunes: формат AAC с защитой FairPlay позволял воспроизводить музыку только на устройствах Apple (iPod, iPhone). Это создало огромную базу лояльных пользователей (lock-in), которые не могли легко перейти на конкурентов, не потеряв свою медиатеку. Выгоду получила Apple, а не музыкальные лейблы, которые были вынуждены продавать треки по фиксированной низкой цене ($0.99).
  -- Игровые консоли: производители консолей (Sony, Microsoft, Nintendo) используют криптографическую подпись кода, чтобы запрещать запуск непроверенных игр. Это позволяет им взимать лицензионные отчисления с каждого проданного диска, контролируя весь рынок программного обеспечения для своей платформы.
- **Аксессуар-контроль (accessory control):** DRM используется для создания искусственных монополий на расходные материалы.
  -- Принтеры: чипы в картриджах препятствуют использованию перезаправленных или сторонних картриджей.
  -- Мобильные телефоны: блокировка аккумуляторов или аксессуаров, работающих только с оригинальными устройствами.
- **Экономический итог:** DRM превращает продажу контента или устройств в аренду с ограниченными правами, позволяя вендорам извлекать ренту долгое время после первоначальной продажи. Это часто приводит к антимонопольным разбирательствам, но технологические барьеры остаются высокими.

7. Управление циклом исправлений (patching cycle): экономический взгляд

Конфликт интересов между исследователями безопасности, вендорами и пользователями определяет стратегию раскрытия уязвимостей.

- **Полное раскрытие (full disclosure):** исследователи публикуют детали уязвимости сразу.
  -- Плюсы: давление на вендоров заставляет их быстрее выпускать патчи. Пользователи узнают о риске и могут принять меры (например, отключить службу).
  -- Минусы: злоумышленники получают инструкцию по эксплуатации раньше, чем многие пользователи успеют обновиться.
- **Ответственное раскрытие (responsible disclosure):** исследователи сообщают вендору и ждут фиксированный срок (обычно 45–90 дней) перед публикацией.
  -- Плюсы: даёт время на разработку и тестирование патча.
  -- Минусы: вендоры могут затягивать процесс, игнорируя проблему, если нет общественной огласки.
- **Экономическое равновесие:** Экономисты безопасности утверждают, что полное раскрытие может быть вредным, если уязвимостей много и они независимы (злоумышленники просто переключаются на другую). Однако видно эмпирически, что угроза раскрытия ускоряет реакцию вендоров. Текущий консенсус склоняется к ответственному раскрытию с жёсткими дедлайнами, что создаёт баланс между стимулами вендоров и правом пользователей на информацию.

8. Стимулы и архитектура систем: почему безопасность часто «не та»

Экономические стимулы определяют не только качество защиты, но и её направленность.

- **Защита вендора vs. защита пользователя:**
  -- В эпоху доминирования Microsoft (Windows XP и ранее) компании было выгоднее сделать систему удобной для разработчиков приложений (разрешая запуск от имени администратора по умолчанию), чем безопасной для пользователя. Это ускорило рост экосистемы приложений, но создало огромную поверхность атаки.

-- Только когда репутационные потери от вирусов и червей стали угрожать доминирующему положению, Microsoft начала инвестировать в безопасность (инициатива Trustworthy Computing). Но даже тогда многие меры (например, UAC в Vista) были направлены скорее на сохранение совместимости, чем на радикальное повышение безопасности.

- **Перекладывание ответственности (liability dumping):**
  -- Банки и платёжные системы часто проектируют протоколы так, чтобы переложить риск мошенничества на клиента (например, через сложные условия использования чип-карт PIN или правила Verified by VISA). Если банк не несёт финансовых потерь от мошенничества, у него меньше стимулов инвестировать в предотвращение атак.
  -- Это приводит к ситуации, когда технически возможная защита не внедряется, потому что экономически выгоднее клиенту страдать от убытков.
- **Проблема «трагедии общин» (tragedy of the commons) в интернете:**
  -- Безопасность сети зависит от самого слабого звена (заражённого компьютера в ботнете). Отдельный пользователь не несёт полной стоимости ущерба, который его заражённый ПК наносит другим (спам, DDoS-атаки). Поэтому пользователи недостаточно инвестируют в защиту своих устройств.
  -- Решения требуют коллективных действий или регулирования (например, обязательная сертификация IoT-устройств), но лобби производителей часто сопротивляется этому.

Главный вывод

Безопасность — это не просто техническая задача, а экономическая и социальная.

1. **Стимулы правят балом:** пока выгодно производить небезопасное ПО или перекладывать риски на пользователей, системы будут уязвимы.
2. **Рынки несовершенны:** асимметрия информации и внешние эффекты приводят к недопроизводству безопасности. Требуется вмешательство регуляторов или создание новых рыночных механизмов (репутация, страхование киберрисков).
3. **Технология следует за деньгами:** DRM и архитектуры систем развиваются в сторону максимизации прибыли владельцев платформ, а не обязательно в сторону безопасности или прав конечных пользователей.

4. **Человеческий фактор рационален (в своём роде):** пользователи жертвуют приватностью и безопасностью не потому, что они глупы, а потому, что немедленные выгоды перевешивают абстрактные будущие риски, а затраты на защиту часто непропорционально высоки.

Инженер безопасности должен понимать эти экономические драйверы, чтобы предлагать решения, которые будут не только технически грамотными, но и экономически жизнеспособными, выравнивая стимулы всех участников экосистемы.