Экономика информационной безопасности – и не только

## Росс Андерсон и Тайлер Мур

## Компьютерная лаборатория, Кембриджский университет

## 15 JJ Thomson Avenue, Кембридж CB3 0FD, Великобритания

Краткий обзор

Экономика информационной безопасности в последнее время стала бурно развивающейся дисциплиной. Поскольку распределенные системы собираются из машин, принадлежащих принципалам с разными интересами, стимулы становятся столь же важными для обеспечения надежности, как и технический дизайн. Новое поле дает ценную информацию не только по темам «безопасности», таким как конфиденциальность, ошибки, спам и фишинг, но и по более общим областям, таким как надежность системы (дизайн одноранговых систем и оптимальный баланс усилий программисты и тестировщики) и политика (в частности, управление цифровыми правами). Эта исследовательская программа начала распространяться на более общие вопросы безопасности (такие как стратегия правоохранительных органов) и на взаимодействие между безопасностью и социальными науками. Совсем недавно он начал взаимодействовать с психологией, как по психолого-экономической традиции, так и в ответ на фишинг. Целью этой исследовательской программы является новая структура для анализа проблем информационной безопасности, которая является одновременно принципиальной и эффективной.

# 1. Введение

Примерно с 2000 года люди начали понимать, что сбои в безопасности вызваны плохими стимулами, по крайней мере, так же часто, как и плохим дизайном. Системы особенно склонны к сбоям, когда человек, охраняющий их, не несет полной стоимости отказа. Теория игр и микроэкономическая теория становятся важными для инженера по безопасности, как и математика криптографии четверть века назад. Растущее использование механизмов безопасности для таких целей, как управление цифровыми правами и вспомогательный контроль, которые обеспечивают власть над владельцами систем, а не защищают их от внешних врагов, создает множество стратегических проблем. Там, где интересы владельца системы противоречат интересам разработчика ее машины, экономический анализ может пролить свет на варианты политики.

Мы рассматриваем последние результаты и живые исследования в области

экономики информационной безопасности. Наша цель — представить несколько многообещающих приложений экономической теории и идей к практическим проблемам информационной безопасности. В разделе 2 мы рассматриваем основополагающие концепции: несогласованные стимулы при проектировании и развертывании компьютерных систем и влияние внешних факторов. В разделе 3 обсуждаются приложения информационной безопасности, в которых экономический анализ дал интересные сведения: уязвимости программного обеспечения, конфиденциальность и разработка механизмов пользовательского контроля для поддержки новых бизнес-моделей. Метрики представляют собой еще одну проблему: рисками нельзя управлять лучше, пока они не могут быть лучше измерены. Большинство пользователей не могут отличить хорошую защиту от плохой, поэтому разработчики не получают вознаграждения за усилия по укреплению своего кода. Некоторые схемы оценки настолько плохо управляются, что «одобренные» продукты менее безопасны, чем случайные. Страхование также проблематично; в

локальные и глобальные корреляции, демонстрируемые различными типами атак, в значительной степени определяют, какие виды страховых рынков осуществимы. Таким образом, рынки киберрисков, как правило, неконкурентны, недостаточно развиты или специализированы.

Экономические факторы также объясняют многие проблемы с конфиденциальностью. Ценовая дискриминация, экономически эффективная, но вызывающая социальные споры, одновременно становится более привлекательной для торговцев и легче реализуемой благодаря техническому прогрессу. Проблемы конфиденциальности также создают множество внешних факторов. Например, спам и «кража личных данных» влекут за собой значительные социальные издержки. Механизмы информационной безопасности или сбои также могут создавать, разрушать или искажать другие рынки: актуальным примером является управление цифровыми правами на онлайн-рынках музыки и программного обеспечения. Наконец, мы рассматриваем варианты государственной политики для борьбы с рыночными сбоями в Разделе 4, где мы анализируем регулирование и структуру механизмов.

В заключение мы обсудим несколько открытых исследовательских задач: изучение влияния безопасности сетевой структуры на взаимодействие, надежность и устойчивость.

1. основополагающие концепции

Экономические мыслители раньше хорошо осознавали взаимодействие между экономикой и безопасностью; богатые страны могли позволить себе большие армии и флоты. Но в настоящее время веб- поиск по «экономике» и «безопасности» выдает относительно мало статей. Основная причина в том, что после 1945 года экономисты отдалились от людей, занимающихся стратегическими исследованиями; Считалось, что ядерное оружие отделяет национальное выживание от экономической мощи [1], а вторичным фактором могло быть то, что США противостояли СССР из-за безопасности, а Япония и ЕС — из- за торговли. Восстановление соединения было оставлено на усмотрение специалистов по информационной безопасности.

* 1. Несогласованные стимулы

Одно из наблюдений, вызвавших интерес к экономике информационной безопасности, было сделано в банковской сфере. В США банки обычно несут ответственность за расходы, связанные с мошенничеством с картами; когда клиент оспаривает транзакцию, банк должен либо показать, что он пытается ее обмануть, либо вернуть ей деньги. В Великобритании банкам было намного проще: им обычно сходило с рук утверждение, что их системы «защищены», и сообщение клиентам, которые жаловались, что они, должно быть, ошибаются или лгут. «Счастливые банкиры», можно подумать; тем не менее, британские банки тратили больше средств на безопасность и чаще страдали от мошенничества. Это могло быть тем, что экономисты называют эффектом морального риска: сотрудники британских банков знали, что жалобы клиентов не будут восприняты всерьез, поэтому они стали ленивыми и небрежными, что привело к эпидемии мошенничества [2].

В 1997 году Эйрес и Левитт проанализировали систему предотвращения угона автомобилей Lojack и обнаружили, что как только порог автовладельцев в городе был установлен, количество угонов автомобилей резко сократилось, поскольку торговля угнанными автомобилями становилась слишком опасной [3]. Это классический пример*экстернальность*, побочный эффект экономической сделки, который может иметь положительные или отрицательные последствия для третьих сторон. Кэмп и Вольфрам опирались на это в 2000 году, чтобы проанализировать уязвимости информационной безопасности как негативные внешние факторы, такие как загрязнение воздуха: тот, кто подключает небезопасный компьютер к Интернету, не несет полных экономических издержек, связанных с этим, не больше, чем кто-то сжигает уголь. Они предложили торговать кредитами уязвимости так же, как углеродными кредитами [4].

В том же 2000 году Вариан обратил внимание на рынок антивирусного программного обеспечения. Люди не тратили на защиту своих компьютеров столько, сколько следовало бы по логике вещей. В то время типичной полезной нагрузкой вируса была атака на отказ в обслуживании веб-сайта Amazon или Microsoft. В то время как рациональный потребитель вполне может потратить 20 долларов, чтобы остановить вирус, уничтожающий его жесткий диск, вряд ли он сделает это только для того, чтобы защитить богатую корпорацию [5].

Теоретикам права давно известно, что ответственность должна возлагаться на ту сторону, которая может наилучшим образом справиться с риском. Тем не менее, куда бы мы ни посмотрели, мы видим плохое распределение онлайн- рисков, что приводит к нарушениям конфиденциальности и затяжным регуляторным спорам. Например, системы медицинской документации покупаются директорами больниц и страховыми компаниями, чьи интересы в ведении счетов, контроле затрат и исследованиях не совсем совпадают с интересами пациентов в отношении конфиденциальности. Это несоответствие стимулов привело в США к HIPAA, закону, устанавливающему стандарты конфиденциальности в информационных технологиях здравоохранения. Бом и др. [6] задокументировали, сколько банков использовали онлайн-банкинг как средство переложить на своих клиентов многие транзакционные риски, которые они ранее несли во времена банковского обслуживания на основе чеков; обновленную информацию об ответственности в платежных системах см. в [7].

Асимметричная информация играет большую роль в информационной безопасности. Мур показал, что мы можем классифицировать многие проблемы как проблемы со скрытой информацией или со скрытыми действиями [8]. Классический случай скрытой информации —

«рынок лимонов» [26]. Акерлоф получил Нобелевскую премию за следующее простое, но глубокое открытие: предположим, что в городе продается 100 подержанных автомобилей: 50 автомобилей в хорошем состоянии по 2000 долларов каждый и 50 «лимонов» по 1000 долларов. Продавцы знают, что есть что, а покупатели нет. Какова рыночная цена подержанного автомобиля? Вы можете подумать, что 1500 долларов; но по такой цене хорошие машины продаваться не будут. Таким образом, рыночная цена будет близка к $1000. Скрытая информация о качестве продукта — одна из причин, по которой плохие продукты безопасности вытесняют хорошие. Когда пользователи не могут отличить хорошее от плохого,

Проблемы со скрытым действием возникают, когда две стороны хотят заключить сделку, но ненаблюдаемые действия одной из сторон могут повлиять на результат. Классический пример – страхование, где страхователь может вести себя опрометчиво без наблюдения со стороны страховой компании. Мы находим ту же общую проблему в сетях. Сетевые узлы могут скрывать злонамеренное или антиобщественное поведение от своих сверстников; маршрутизаторы могут незаметно отбрасывать выбранные пакеты или фальсифицировать ответы на запросы маршрутизации; узлы могут перенаправлять сетевой трафик для прослушивания разговоров; а игроки в системах обмена файлами могут скрывать, делятся ли они с другими, поэтому некоторые могут

«бесплатно ездить», а не помогать поддерживать систему. Как только проблема рассматривается в этом свете, проектировщики могут свести к минимуму возможность скрытых действий или упростить выполнение подходящих контрактов.

Это помогает объяснить эволюцию одноранговых систем. Ранние системы, предложенные учеными, такие как Eternity, Freenet, Chord, Pastry и OceanStore, требовали от пользователей случайного выбора файлов других пользователей [9]. Эти системы так и не получили широкого распространения. Более поздние системы, которые действительно привлекали большое количество пользователей, такие как Gnutella и Kazaa, вместо этого позволяют одноранговым узлам обслуживать только контент, который они загрузили для собственного использования, вместо того, чтобы обременять их чужими файлами. Сравнение между этими архитектурами изначально было сосредоточено на чисто технических аспектах: стоимости поиска, извлечения, связи и хранения. Однако анализ стимулов тоже оказался плодотворным.

Во-первых, система, построенная как ассоциация клубов, снижает вероятность скрытых действий; члены клуба имеют больше возможностей оценить, какие участники вносят свой вклад. Во-вторых, у клубов могут быть совершенно разные интересы. Хотя одноранговые системы теперь рассматриваются как механизмы для обмена музыкой, ранние системы были разработаны для защиты от цензуры. Система может служить ряду совершенно разных групп — может быть, китайским диссидентам, критикам саентологии или поклонникам садомазохистских образов, которые разрешены в Калифорнии, но запрещены в Теннесси.

Ранние одноранговые системы требовали, чтобы такие пользователи обслуживали файлы друг друга, так что в конечном итоге они защищали свободу слова друг друга. Но не могут ли такие группы бороться усерднее, чтобы защитить своих коллег, а не людей, вовлеченных в борьбу, в которой они не заинтересованы?

Данезис и Андерсон представили модель Red-Blue для анализа этого [10]. У каждого узла есть предпочтение среди типов ресурсов, например, левые политические тексты против правых, в то время как цензор будет пытаться навязать свои собственные предпочтения. Его действие подойдет одним узлам, но не другим. Модель протекает как игра с несколькими раундами, в которой узлы устанавливают бюджеты на оборону, влияющие на вероятность того, что они победят цензора или будут подавлены им. При разумных предположениях авторы показывают, что разнообразие (когда каждый узел хранит свой предпочтительный набор ресурсов) работает лучше при атаке, чем солидарность (когда каждый узел хранит один и тот же набор ресурсов). Разнообразие заставляет узлы охотно выделять более высокие оборонные бюджеты; чем больше разнообразие, тем быстрее рухнет солидарность перед лицом нападения. Эта модель была ранним предприятием на границе между экономикой и социологией; он проливает свет на общую проблему разнообразия и солидарности, которая недавно привлекла к себе внимание из-за вопроса о том, противоречит ли растущее разнообразие современных обществ солидарности, на которой основаны современные системы социального обеспечения [11].

* 1. Безопасность как внешний эффект

Информационные отрасли имеют много различных типов внешних эффектов. Они, как правило, имеют доминирующие фирмы по трем причинам. Во-первых, часто существуют сетевые внешние факторы, из-за которых ценность сети растет более чем линейно по количеству пользователей; например, любой, кто хочет продать с аукциона некоторые товары, обычно обращается в крупнейший аукционный дом, так как это привлечет больше участников торгов. Во-вторых, часто существует техническая блокировка, связанная с функциональной совместимостью, и рынки могут быть двусторонними: фирмы-разработчики программного обеспечения разрабатывают для Windows, чтобы получить доступ к большему количеству клиентов, а пользователи покупают машины с Windows, чтобы получить доступ к большему количеству программного обеспечения. В-третьих, информационные отрасли, как правило, сочетают высокие фиксированные и низкие предельные издержки: производство первой копии программы (или DVD) может стоить миллионы, а последующие копии почти бесплатны. Эти три особенности по отдельности могут привести к отраслям с доминирующими фирмами; вместе они еще более вероятны.

Это не только помогает объяснить подъем и господство операционных систем, от System/360 через DOS и Windows до Symbian; это также помогает объяснить закономерности недостатков безопасности. В то время как поставщик платформы завоевывает господствующее положение на рынке, он должен обращаться как к поставщикам программного обеспечения, так и к пользователям, и безопасность может встать у них на пути. Таким образом, поставщики начинают с минимальной защиты; как только они стали доминирующими, они добавляют меры безопасности, чтобы более жестко заблокировать своих клиентов [12]. Мы обсудим это более подробно позже.

Дополнительные внешние факторы влияют на инвестиции в безопасность, поскольку защита часто зависит от усилий многих принципалов. Хиршлейфер рассказал историю Анархии, острова, защита от наводнений

были построены отдельными семьями и защита которых зависит от самого слабого звена, то есть от самой ленивой семьи; он сравнил это с городом, защита которого от атаки межконтинентальных баллистических ракет зависит от единственного лучшего оборонительного выстрела [13]. Вариан расширил это до трех случаев, представляющих интерес для надежности информационных систем, где производительность зависит от минимальных усилий, наилучших усилий или суммы усилий [14].

Корректность программы может зависеть от минимальных усилий (самый нерадивый программист вносит уязвимость), а тестирование программных уязвимостей может зависеть от суммы усилий всех. Безопасность также может зависеть от максимальных усилий — действий, предпринятых отдельным сторонником, таким как архитектор безопасности. Когда это зависит от суммы индивидуальных усилий, бремя, как правило, ложится на плечи агентов с самым высоким соотношением выгод и затрат, в то время как остальные действуют бесплатно. В случае минимальных усилий доминирует агент с наименьшим соотношением выгод и затрат. По мере добавления дополнительных агентов системы становятся более надежными в случае совокупных усилий, но менее надежными в случае самого слабого звена. Каковы последствия? Что ж, софтверным компаниям следует нанимать больше тестировщиков ПО и меньше, но более компетентных программистов. (Конечно,

Эта работа вдохновила других исследователей на рассмотрение взаимозависимых рисков. В недавней влиятельной модели Кунройтера и Хила отмечается, что человек, принимающий защитные меры, создает положительные внешние эффекты для других, что, в свою очередь, может отбить у них желание инвестировать [15]. Это понимание имеет последствия далеко за пределами информационной безопасности. Решение одного владельца квартиры установить спринклерную систему снизит риск возникновения пожара у его соседей и снизит вероятность того, что они сделают то же самое; авиакомпании могут принять решение не проверять багаж, переданный другими перевозчиками, которые, как считается, заботятся о безопасности; и люди, думающие о вакцинации своих детей, могут вместо этого отказаться от коллективного иммунитета. В каждом случае возможно несколько широко варьирующихся равновесий, от полного принятия до полного отказа.

Кац и Шапиро проанализировали, как сетевые внешние факторы влияют на внедрение технологии: они приводят к классической S-образной кривой внедрения, в которой медленное раннее внедрение уступает место быстрому развертыванию, как только количество пользователей достигает некоторой критической массы [16]. Сетевые эффекты также могут влиять на первоначальное развертывание технологии безопасности, польза от которой может зависеть от количества пользователей, которые ее примут. Стоимость может превышать выгоду до тех пор, пока не будет принято минимальное количество; так что каждый может ждать, пока другие начнут первыми, и технология никогда не будет развернута. Недавно Озмент и Шехтер проанализировали различные подходы к преодолению таких проблем самонастройки [17].

Эта задача особенно актуальна. Ряд основных интернет-протоколов, таких как DNS и маршрутизация, считаются небезопасными. Существуют лучшие протоколы (например, DNSSEC, S-BGP); задача состоит в том, чтобы их усыновить. Два широко распространенных протокола безопасности, SSH и IPsec, оба преодолели проблему начальной загрузки, предоставив существенные внутренние преимущества внедряющим фирмам, в результате чего их можно было внедрять по одной фирме за раз, а не требовать, чтобы все переходили сразу. Развертывание факсимильных аппаратов было аналогичным: многие компании изначально покупали факсимильные аппараты для подключения своих офисов.

# приложения

## Экономика уязвимостей

Было много споров о «безопасности с открытым исходным кодом» и, в более общем плане, о том, является ли активный поиск и раскрытие уязвимостей социально желательным. Андерсон показал в 2002 году, что при стандартных предположениях о росте надежности открытые системы и проприетарные системы так же безопасны, как и друг друга; раскрытие системы в равной степени помогает атакующим и обороняющимся [18]. Таким образом, открытый секретный вопрос может быть эмпирическим и включать степень, в которой данная реальная система следует стандартной модели.

Рескорла утверждал в 2004 году, что для программного обеспечения со многими скрытыми уязвимостями удаление одной ошибки мало влияет на вероятность того, что злоумышленник позже обнаружит другую [19]. Поскольку эксплойты часто основаны на уязвимостях, обнаруженных с помощью исправлений, он выступал против раскрытия информации и частых исправлений, если только те же самые уязвимости не могут быть обнаружены повторно. Это подняло вопрос о том, соответствует ли программное обеспечение стандартной модели надежности независимых уязвимостей. Озмент обнаружил, что для FreeBSD уязвимости коррелируют в том смысле, что они могут быть обнаружены заново [20]. Озмент и Шехтер также обнаружили, что скорость раскрытия уникальных уязвимостей для базовой и неизменной операционной системы FreeBSD снизилась за шестилетний период [21]. Эти результаты показывают, что раскрытие информации об уязвимостях может улучшить безопасность системы в долгосрочной перспективе. Раскрытие уязвимостей также помогает мотивировать поставщиков исправлять ошибки [22]. Арора и др. показали, что публичное раскрытие информации заставляет поставщиков быстрее реагировать на исправления; количество атак увеличилось с самого начала, но количество зарегистрированных уязвимостей со временем уменьшилось [23].

Это обсуждение вызывает более глубокий вопрос: почему вообще существует так много уязвимостей? Полезная аналогия может быть проведена при рассмотрении неудач крупных программных проектов: уже много лет известно, что примерно 30% крупных проектов разработки терпят неудачу [24], и эта цифра, похоже, не меняется, несмотря на усовершенствование инструментов и обучения: люди только что создали много в наши дни катастрофы больше, чем в 1970-х годах. Это говорит о том, что неудача проекта в основном связана не с техническим риском, а с окружающими социально-экономическими факторами (к этому вопросу мы вернемся позже). Точно так же, когда речь идет о безопасности, разработчики программного обеспечения имеют лучшие инструменты и обучение, чем десять лет назад, и способны создавать более безопасное программное обеспечение, но экономика индустрии программного обеспечения не дает им особого стимула для этого.

На многих рынках установка «отправить во вторник и получить правильную версию 3» является совершенно рациональным поведением. Многие рынки программного обеспечения имеют доминирующие фирмы благодаря сочетанию высоких фиксированных и низких предельных издержек, сетевых внешних факторов и привязки к клиенту, отмеченных выше [25], поэтому победа в рыночных гонках имеет первостепенное значение. В таких гонках конкуренты должны апеллировать к дополняющим, таким как разработчики приложений, которым мешает безопасность; и безопасность, как правило, является рынком лимонов в любом случае. Таким образом, поставщики платформ начинают с недостаточной безопасности, а те, которые они обеспечивают, обычно разрабатываются таким образом, что затраты на соблюдение требований перекладываются на конечных пользователей [12]. Как только доминирующее положение установлено, поставщик может добавить больше безопасности, чем необходимо, но спроектировать таким образом, чтобы максимально зафиксировать клиента [27].

В некоторых случаях безопасность даже хуже, чем рынок лимонов: даже производитель не знает, насколько безопасно его программное обеспечение. Таким образом, у покупателей нет причин платить больше за защиту, а поставщики не склонны в нее вкладываться.

Как это можно решить? Экономисты предложили два новых подхода к показателям безопасности программного обеспечения: рынки уязвимостей и страхование.

Рынки уязвимостей помогают покупателям и продавцам установить реальную стоимость обнаружения уязвимости в программном обеспечении. Начнем с того, что в некоторых стандартах указана минимальная стоимость разного рода технических компромиссов; одним из примеров являются банковские стандарты для торговых терминалов [28]. Другим примером является вознаграждение за обнаружение ошибок: Дон Кнут предложил вознаграждение людям, обнаружившим ошибки в его программном обеспечении для набора текста, а Mozilla Foundation предлагает 500 долларов за критические уязвимости безопасности в Firefox. Кэмп и Вольфрам предположили в 2000 году, что рынки могут работать здесь лучше [4], а Шехтер развил это в предложение для открытых рынков в отчетах о ранее не обнаруженных уязвимостях [29]. Две фирмы, iDefense и Tipping Point, сейчас открыто покупают уязвимости, так что рынок действительно существует (цены, к сожалению, не публикуются). Их бизнес- модель заключается в предоставлении данных об уязвимостях одновременно своим клиентам и пострадавшему поставщику, чтобы их клиенты могли обновлять свои брандмауэры раньше всех. Однако стимулы здесь неоптимальны: организации рынка ошибок могут повысить ценность своего продукта за счет утечки информации об уязвимостях, чтобы навредить тем, кто не является подписчиком [30].

Было предложено несколько вариантов рынков уязвимостей. Бёме утверждал, что производные программы могут быть лучше [31]. Контракты на программное обеспечение будут заключаться парами: по первому выплачивается фиксированная сумма, если к определенной дате в программе не будет обнаружено уязвимостей, а по второму выплачивается другая сумма, если уязвимость обнаружена. Если эти контракты можно продавать, то их цена должна отражать консенсус в отношении качества программного обеспечения. Поставщики программного обеспечения, инвесторы компаний-разработчиков программного обеспечения и страховые компании могут использовать такие производные инструменты для хеджирования рисков. Третья возможность, предложенная Озментом, состоит в том, чтобы спроектировать рынок уязвимостей как аукцион; это недавно было реализовано швейцарской фирмой WabiSabiLabi [32].

Одним из критических замечаний ко всем рыночным подходам является то, что они могут увеличить количество выявленных уязвимостей, мотивируя большее количество людей на поиск недостатков. Поэтому при их разработке следует проявлять некоторую осторожность.

Альтернативный подход – страхование. Андеррайтеры часто используют экспертов-оценщиков для проверки ИТ-инфраструктуры и управления фирмы-клиента; это предоставляет данные как застрахованному, так и страховщику. В долгосрочной перспективе страховщики учатся более точно оценивать риски. Однако сейчас рынок киберстрахования недостаточно развит и недостаточно используется. Одной из причин, по мнению Бёме и Катарии [33], является взаимозависимость риска, которая принимает как локальные, так и глобальные формы. ИТ-инфраструктура фирм подключена к другим объектам, поэтому их усилия могут быть подорваны сбоями в других местах. Кибератаки часто используют уязвимость в программе, используемой многими фирмами. Взаимозависимость может сделать некоторые киберриски непривлекательными для страховщиков, особенно те риски, которые имеют глобальную, а не локальную корреляцию, такие как черви и вирусные атаки,

Многие авторы призывали к тому, чтобы программные риски перекладывались на поставщиков; и, несмотря на заявления об отказе от ответственности в лицензионных соглашениях с конечным пользователем программного обеспечения (EULA), законы о защите прав потребителей как в США, так и в ЕС позволяют людям предъявлять иски о телесных повреждениях, а в некоторых случаях и о возмещении ущерба в результате сбоя программного обеспечения. Но это все еще не распространено. (Мы вернемся к этому позже.) Если это так, то было бы интересно посмотреть, смогут ли крупные поставщики платформ, такие как Microsoft, купить страховку. Даже на уровне фирм-клиентов коррелированный риск заставляет фирмы недостаточно инвестировать как в технологии безопасности, так и в кибербезопасность.

страхование [34]. В любом случае рынкам киберстрахования может не хватать объема и ликвидности, чтобы стать эффективными.

* 1. Экономика конфиденциальности

Постоянная эрозия личной неприкосновенности разочаровывает как политиков, так и практиков. Люди говорят, что ценят конфиденциальность, но поступают иначе. Технологии повышения конфиденциальности были предложены для продажи, но большинство из них потерпели неудачу на рынке. Почему это должно быть?

Конфиденциальность — это один из аспектов информационной безопасности, который интересовал экономистов до 2000 года. В 1978 году Познер определил конфиденциальность как секретность [35], а в следующем году распространил это понятие на изоляцию [36]. В 1980 году Хиршлейфер опубликовал основополагающую статью, в которой утверждал, что неприкосновенность частной жизни заключается не в уходе от общества, а в том, что неприкосновенность частной жизни является средством организации общества, возникающим в результате эволюции территориального поведения; интернализованное уважение к собственности — это то, что позволяет автономии сохраняться в обществе. Эти дебаты о конфиденциальности в 1970-х годах привели в Европе к общим законам о защите данных, в то время как США ограничились несколькими отраслевыми законами, такими как HIPAA. Аппетит экономистов к работе над конфиденциальностью в последнее время еще больше подогрелся Интернетом, бумом доткомов и бурным ростом торговли личной информацией о онлайн-покупателях.

Ранний современный взгляд на приватность можно найти в статье Вэриана 1996 года, в которой приватность анализировалась с точки зрения информационных рынков [38]. Потребители не хотят, чтобы их раздражали неуместные маркетинговые звонки, а маркетологи не хотят тратить усилия впустую. Тем не менее, оба разочарованы из-за затрат на поиск, внешних факторов и других факторов. Вариан предложил дать потребителям право на информацию о себе и позволить им сдавать ее в аренду маркетологам с условием, что она не будет перепродана без разрешения.

Недавнее распространение сложных, информационно-емких бизнес-моделей требует более широкого подхода. В 2003 г. Одлызко утверждал, что эрозия конфиденциальности является следствием желания взимать разные цены за аналогичные услуги [39]. Технология одновременно увеличивает как стимулы, так и возможности для ценовой дискриминации. Компании могут анализировать онлайн-покупки и взаимодействия для получения данных, раскрывающих готовность людей платить. От систем управления прибылью авиакомпаний до сложных и постоянно меняющихся цен на программное обеспечение и телекоммуникации, дифференцированное ценообразование экономически эффективно, но вызывает все большее недовольство. Acquisti и Varian проанализировали рыночные условия, при которых персонализированная ценовая дискриминация выгодна [40]: она может процветать в отраслях с большим разбросом потребительской оценки услуг,

Acquisti и Grossklags решили специфическую проблему, почему люди выражают большое предпочтение конфиденциальности во время интервью, но показывают гораздо меньшее предпочтение в своем поведении как онлайн, так и офлайн [41]. Они обнаруживают, что людям в основном не хватает информации, чтобы сделать осознанный выбор, и даже когда они это делают, они часто обменивают долгосрочную конфиденциальность на краткосрочные выгоды. Левенштейн развил это до более полного психолого-экономического анализа (тема, к которой мы вернемся позже) [42]. Сочетая это «гиперболическое дисконтирование» с неприятием потерь, адаптацией и неопределенностью предпочтений, он предсказывает большую часть наблюдаемого поведения: люди изначально будут сопротивляться любой потере конфиденциальности, но быстро адаптируются и не будут очень мотивированы, чтобы получить новые формы конфиденциальности.

постепенно привыкайте к уровням слежки, которые были бы неприемлемы, если бы их вводили быстро. Тем не менее, новые технологии увеличивают риски, устраняя сигналы; так что в конечном итоге нам может понадобиться либо больше регулирования, либо большая терпимость к индивидуальным особенностям.

Свайр утверждал, что мы должны измерять затраты на вторжение в частную жизнь более широко [44]. Если оператор телефонных продаж звонит 100 потенциальным клиентам, продает трем из них страховку и вызывает раздражение у 80, то в обычном анализе учитывается только выгода для троих и для страховой компании.

Однако постоянное раздражение заставляет миллионы людей выходить из справочника, не отвечать на телефонные звонки во время обеда или прослушивать звонки через автоответчик. Долгосрочный общественный вред может быть значительным. Несколько эмпирических исследований подтвердили это, изучив оценки людей приватности. Вила и др. далее охарактеризовал экономику конфиденциальности как рынок лимонов [43], утверждая, что потребители игнорируют будущую ценовую дискриминацию, предоставляя информацию продавцам.

Вот вам и факторы, повышающие вероятность вторжения в частную жизнь. Какие факторы делают их менее таковыми? Кэмпбелл и др. обнаружили, что цена акций компаний, сообщающих о нарушении безопасности, с большей вероятностью упадет, если в результате нарушения произойдет утечка конфиденциальной информации [45]. Acquisti, Friedman и Telang провели аналогичный анализ нарушений конфиденциальности [46]. Их первоначальные результаты менее убедительны, но все же указывают на негативное влияние на цену акций, за которым последует возможное восстановление.

Ответные меры регулирующих органов (впервые принятые в Европе) в основном сводились к тому, чтобы требовать от компаний предоставления потребителям возможности либо «согласиться», либо «отказаться» от сбора данных. В то время как защитники конфиденциальности обычно поддерживают политику отказа, поскольку она приводит к более низким показателям сбора данных, Букарт и Дегриз выступают за отказ на основании конкуренции [47]: доступность информации о покупательских привычках большинства клиентов, а не нескольких клиентов, может помочь конкурентам выйти на рынок.

Эмпирически существуют большие различия в показателях «отказов» между различными типами потребителей, но их мотивы не всегда ясны. Вариан и др. проанализировали черный список телефонных продаж Федеральной комиссии по связи США по округам [48]. Они обнаружили, что образованные люди чаще регистрируются: но связано ли это с тем, что богатые домохозяйства получают больше звонков, потому что они больше ценят свое время или потому, что лучше понимают риски?

Стимулы также влияют на разработку технологии обеспечения конфиденциальности. Создатели систем анонимности знают, что они зависят от сетевых внешних факторов: чем больше пользователей, тем больше трафика для сокрытия действий от врага [49]. Интересным случаем является Tor [50], который анонимизирует веб-трафик и делает упор на удобство использования для увеличения скорости внедрения. Она была разработана на основе системы связи ВМС США, но в конечном итоге к участию были приглашены все пользователи Интернета, чтобы увеличить размер сети, и теперь это самая крупная известная система анонимной связи.

## Поощрения и развертывание механизмов безопасности

Страхование — не единственный рынок, затронутый информационной безопасностью. Некоторые очень громкие дебаты были сосредоточены на DRM; звукозаписывающие компании годами настаивали на внедрении DRM в компьютеры и бытовую электронику, в то время как активисты по защите цифровых прав выступали против них. Какой свет может пролить на эти дебаты экономика безопасности?

Многие исследователи поставили дискуссию в гораздо более широком контексте, чем просто звукозаписывающие компании и загрузчики. Вариан указал в 2002 году, что DRM и подобные механизмы были

также о связывании, объединении и ценовой дискриминации; и что их беспрепятственное использование может повредить конкуренции [51]. В статье Самуэльсона и Скотчмера изучалось, что может пойти не так, если технические и юридические ограничения подорвут право на обратное проектирование программных продуктов для обеспечения совместимости. Он обеспечил научную основу для большей части работы по антиконкурентным последствиям DMCA, механизмам контроля авторских прав и механизмам информационной безопасности, применяемым к новым бизнес-моделям.

Механизмы Trusted Computing (TC) подверглись серьезному анализу и критике. Фон Хиппель показал, что большинство инноваций, стимулирующих экономический рост, не ожидаются производителями платформ, на которых они основаны; ПК, например, был задуман как средство для работы с электронными таблицами, и если бы IBM смогла ограничиться этим, огромные возможности были бы упущены. Кроме того, технологические изменения на рынках ИТ обычно носят кумулятивный характер. Если существующие фирмы могут злоупотреблять технологиями безопасности, чтобы усложнить жизнь новаторам, это создаст всевозможные ловушки и порочные стимулы [53]. Андерсон указал на возможность конкурентного злоупотребления механизмами ТС; Например, путем передачи контроля над пользовательскими данными от владельца машины, на которой они хранятся, создателю файла, в котором они хранятся, возможность блокировки значительно возрастает [27]. Лукабо и Сикер обсудили существующую историю индустрии, которая пострадала из-за технической блокировки, связанной с безопасностью [54]. Операторы кабельной индустрии США привязаны к своим поставщикам телевизионных приставок; и хотя они в значительной степени договорились о прямых затратах на это при выборе поставщика, косвенные затраты были большими и неуправляемыми. Инновации пострадали, и кабельное телевидение отстало от других платформ, таких как Интернет, поскольку у двух поставщиков платформ по отдельности не было стимула вкладывать средства в улучшение своих платформ. Лукабо и Сикер обсудили существующую историю индустрии, которая пострадала из-за технической блокировки, связанной с безопасностью [54]. Операторы кабельной индустрии США привязаны к своим поставщикам телевизионных приставок; и хотя они в значительной степени договорились о прямых затратах на это при выборе поставщика, косвенные затраты были большими и неуправляемыми. Инновации пострадали, и кабельное телевидение отстало от других платформ, таких как Интернет, поскольку у двух поставщиков платформ по отдельности не было стимула вкладывать средства в улучшение своих платформ. Лукабо и Сикер обсудили существующую историю индустрии, которая пострадала из-за технической блокировки, связанной с безопасностью [54]. Операторы кабельной индустрии США привязаны к своим поставщикам телевизионных приставок; и хотя они в значительной степени договорились о прямых затратах на это при выборе поставщика, косвенные затраты были большими и неуправляемыми. Инновации пострадали, и кабельное телевидение отстало от других платформ, таких как Интернет, поскольку у двух поставщиков платформ по отдельности не было стимула вкладывать средства в улучшение своих платформ.

Экономические исследования были применены к самой звукозаписывающей индустрии, и результаты оказались тревожными. В 2004 г. Оберхольцер и Штрумпф опубликовали ставшую теперь известной работу, в которой исследовали, как соотносятся загрузки музыки и продажи пластинок [55]. Они показали, что загрузки не наносят существенного вреда музыкальной индустрии. Даже в самой пессимистичной интерпретации требуется пять тысяч загрузок, чтобы вытеснить продажу одного альбома, в то время как альбомы, пользующиеся большим спросом, действительно выигрывают от обмена файлами.

В янва фирма Apple). Контент-индустрия насмехалась, но к концу года музыкальные издатели протестовали против того, что Apple получает слишком большую долю денег от онлайн-продаж музыки. По мере того, как власть в цепочке поставок перешла от крупных музыкальных компаний к поставщикам платформ, власть в музыкальной индустрии, по-видимому, переходит от крупных компаний к независимым, точно так же, как дерегулирование авиакомпаний благоприятствовало производителям самолетов и бюджетным авиакомпаниям. Это поразительная демонстрация предсказательной силы экономического анализа. Борясь с несуществующей угрозой,

* 1. Защита компьютерных систем от рациональных противников

Практики информационной безопасности традиционно предполагали два типа пользователей: честные, которые всегда ведут себя так, как им приказано, и злонамеренные, стремящиеся нанести ущерб любой ценой. Но системы часто подрываются тем, что экономисты называют*стратегический*пользователи: пользователи, которые

действовать из корысти, а не из злого умысла. Многие системы обмена файлами страдают от «фрирайда», когда пользователи скачивают файлы, не загружая свои собственные. Это совершенно рациональное поведение, учитывая, что пропускная способность для загрузки обычно более ограничена, а пользователи, загружающие файлы, подвергаются более высокому риску судебного преследования. Совокупный эффект — снижение производительности.

Еще одна неприятность, причиняемая корыстными пользователями, — это спам. Стоимость передачи спамеру настолько низка, что приемлем крошечный процент успеха [57]. Кроме того, хотя спам влечет за собой значительные расходы для получателей, спамеры не ощущают этих расходов. Бёме и Хольц изучили биржевой спам и выявили статистически значимое увеличение цен на рекламируемые акции [58]. Фридер и Зиттрейн независимо друг от друга обнаружили аналогичный эффект [59].

Некоторые сетевые протоколы могут быть использованы эгоистичными пользователями в ущерб общесистемной производительности. В TCP, протоколе, используемом для передачи большинства интернет-данных, Akella et al. обнаружили, что эгоистичное обеспечение механизмов управления перегрузкой может привести к субоптимальной производительности [60].

Исследователи использовали теорию игр для изучения негативных последствий эгоистичного поведения для систем в целом. Куцупиас и Пападимитриу назвали «ценой анархии» отношение полезности равновесия по Нэшу в наихудшем случае к социальному оптимуму [61]. Цена анархии стала стандартным мерилом неэффективности эгоистичного поведения в компьютерных сетях. Рофгарден и Тардос изучали эгоистичную маршрутизацию в перегруженной сети, сравнивая уровни перегрузки в сети, где пользователи выбирают кратчайший путь, доступный для перегрузки, когда планировщик сети выбирает пути для максимизации потока [62]. Они установили верхню3ю границу4по цене анархии, когда издержки заторов линейны; кроме того, в общем, общая задержка эгоистичной сети не больше, чем оптимальная маршрутизация потока вдвое большего трафика.

Другие темы, которым препятствует эгоистичная деятельность, включают создание сети, где пользователи решают, создавать ли дорогостоящие ссылки для сокращения путей или бесплатно пользоваться более длинными непрямыми соединениями [63, 64, 65]; беспроводное совместное использование спектра, когда поставщики услуг конкурируют за получение каналов от точек доступа [66]; и заражение компьютерными вирусами, когда пользователи несут высокие затраты на заражение себя, а преимущества получают незащищенные узлы [67].

Чтобы объяснить личную заинтересованность пользователя, ученые-компьютерщики предложили несколько механизмов с учетом неформального понятия «справедливости». Для борьбы со спамом Дворк и Наор предлагают прикреплять к электронным письмам «доказательство работы», что легко сделать для нескольких писем, но непрактично для флуда [68]. Лори и Клейтон критикуют схемы «доказательства работы», демонстрируя, что дополнительная нагрузка может быть обременительной для многих законных пользователей, в то время как отправители спама могут использовать ботнеты для выполнения вычислений [69]. Кроме того, интернет-провайдеры могут быть не готовы блокировать трафик с этих скомпрометированных машин. Сержантов и Клейтон анализируют стимулы интернет- провайдеров к блокированию трафика от других интернет-провайдеров с большим количеством зараженных машин и подкрепляют это данными [70]. Они также показывают, насколько иррациональны и контрпродуктивны некоторые существующие стратегии блокировки спама.

Системы репутации широко предлагались для преодоления безбилетника в одноранговых сетях. Самый известный полевой пример — отзывы об онлайн-аукционах eBay. Делларокас утверждает, что мягкость механизма обратной связи (только 1% оценок отрицательные) способствует стабильности на рынке [72]. Сержантов и Андерсон используют теорию социального выбора, чтобы рекомендовать улучшения в предложениях системы репутации [73]. Фельдман и коллеги моделируют такие системы как повторяющуюся игру «дилемма заключенного», где пользователи в каждом раунде чередуются между ролями клиента и сервера [71]. В последнее время исследователи начали

рассмотреть более формально, как построить справедливые системы, используя проектирование механизмов. Мы обсудим эти разработки в разделе 5.1.

# Роль правительств

Мир информационной безопасности регулировался с самого начала, хотя поначалу заботы правительства не имели ничего общего с политикой конкуренции. Первым фактором была проблема нераспространения. Правительства использовали экспортные лицензии и манипулировали финансированием исследований, чтобы ограничить доступ к криптографии как можно дольше. В 2000 году от этих усилий в значительной степени отказались. Вторым фактором были трудности, с которыми даже правительство США в течение многих лет сталкивалось при приобретении систем для собственного использования, когда информационная безопасность стала охватывать и безопасность программного обеспечения. Таким образом, в 80-х и 90-х годах политика поощряла исследования в области безопасности, препятствуя исследованиям в области криптографии.

## Первые дни

Ландвер описывает усилия правительства США с середины 1980-х годов по решению проблемы лимонов в бизнесе программного обеспечения для обеспечения безопасности [74]. Первой попыткой исправить ситуацию была правительственная схема оценки — «Оранжевая книга», но это принесло свои проблемы. Стремление менеджеров к новейшему программному обеспечению ослабило требования к сертификации: поставщики должны были просто показать, что они инициировали процесс сертификации, который часто так и не был завершен. Оценки также проводились за государственный счет государственными служащими АНБ, которые, избегая риска, не торопились; оцениваемые продукты часто были непригодно устаревшими. Были также проблемы взаимодействия с системами союзников, поскольку такие страны, как Великобритания и Германия, имели свои собственные несовместимые схемы.

Это побудило правительства стран НАТО установить «Общие критерии» в качестве преемника

«Оранжевой книги». Большинство оценок проводятся коммерческими лабораториями и оплачиваются поставщиком, который должен быть мотивирован печатью успешной оценки. Общие критерии страдают от различных проблем, в первую очередь от неблагоприятного отбора: поставщики ищут оценщика, который поможет им легче всего добраться, а национальные агентства, которые сертифицируют оценочные лаборатории, очень неохотно отзывают лицензию, даже после скандала, из-за опасается, что доверие к схеме будет подорвано [75].

Регулирование все чаще оправдывается предполагаемыми провалами рынка в отрасли информационной безопасности. Европейский Союз предложил Политику сетевой безопасности, в которой изложен общеевропейский ответ на атаки на информационные системы [76]. Это начинает использовать экономические аргументы о несостоятельности рынка, чтобы оправдать действия правительства в этом секторе. Предлагаемые решения знакомы и включают в себя все, от повышения сознания до дополнительных оценок Common Criteria.

Другим явным использованием экономики безопасности в разработке политики были комментарии правительства Германии к Trusted Computing [77]. В них изложены проблемы, связанные с сертификацией и лазейками, защитой данных и вопросами экономической политики. Они оказали огромное влияние на то, чтобы убедить Trusted Computing Group включить и принять правила членства, которые снижали риск того, что ее программа будет дискриминировать малые и средние предприятия. Недавно Генеральная комиссия по конкуренции Европейской комиссии рассматривала экономические последствия механизмов безопасности Vista.

Среди академических ученых в области регулирования Барнс изучает стимулы, с которыми сталкиваются создатели вирусов, поставщики программного обеспечения и пользователи компьютеров [78], и рассматривает различные политические инициативы, направленные на то, чтобы сделать компьютеры менее подверженными заражению, от вознаграждения тех, кто обнаруживает уязвимости, до наказания пользователей, которые не принимают минимальные стандарты безопасности. Гарсия и Горовиц отмечают, что разрыв между социальной ценностью провайдеров интернет- услуг и доходами, связанными с их незащищенностью, продолжает увеличиваться [79]. Они утверждают, что если так будет продолжаться, могут стать вероятными обязательные стандарты безопасности.

Мур представляет интересный нормативный вопрос из криминалистики. В то время как ПК используют стандартные форматы дисков, мобильные телефоны используют проприетарные интерфейсы, которые затрудняют восстановление данных с телефонов; средства восстановления существуют только для самых распространенных моделей. Так что преступники должны покупать немодные телефоны, а полиция должна продвигать открытые стандарты [80].

* 1. Саморегулирование

Жесткое регулирование может привести к высоким затратам — либо напрямую, либо в результате агентских проблем и других второстепенных факторов. Гхош и Раджан обсуждают, как три закона США

– Sarbanes-Oxley, Gramm-Leach-Bliley и HIPAA – ложатся непропорционально тяжелым бременем на малый и средний бизнес, в основном из-за универсального подхода к соблюдению со стороны крупных бухгалтерских фирм [81]. Они показывают, как обязательные инвестиции в обеспечение соответствия требованиям безопасности могут привести к непредвиденным последствиям — от искажения рынков безопасности до снижения конкуренции.

Учитывая высокую стоимость и сомнительную эффективность регулирования, попытки саморегулирования предпринимались в ряде случаев, но некоторые попытки потерпели крах. Например, ряд организаций создали службы сертификации, чтобы гарантировать качество программных продуктов или веб-сайтов. Их цель была двоякой: преодолеть настороженность общества в отношении электронной коммерции и предотвратить более дорогое регулирование со стороны правительства. Но (как и в случае с Common Criteria) рынки сертификации могут быть легко разрушены гонкой на выживание; сомнительные компании чаще покупают сертификаты, чем уважаемые, и даже обычные компании могут искать самую легкую сделку. В отсутствие способного мотивированного регулятора крах может наступить быстро.

Эдельман проанализировал этот «неблагоприятный отбор» в случае одобрения веб-сайтов и онлайн- рекламы [82]: в то время как около 3% веб-сайтов являются вредоносными, около 8% веб-сайтов, сертифицированных одним крупным поставщиком, являются вредоносными. Он также сравнил результаты обычного веб-поиска и платной рекламы и обнаружил, что, хотя 2,73% компаний, занимающих первые места в веб-поиске, были плохими, 4,44% компаний, купивших рекламу в поисковой системе, были плохими. Его вывод – «Не нажимайте на рекламу» – может стать плохой новостью для поисковой индустрии.

Саморегулирование оказалось несколько лучше для управления исправлениями. Анализ Arora et al. показывает, что конкуренция на рынках программного обеспечения ускоряет выпуск исправлений даже больше, чем угроза раскрытия уязвимости в двух из трех исследованных стратегий [84]. Битти и др. обнаружили, что первопроходцы, применяющие исправления, быстро обнаруживают проблемы, ломающие их системы, а отстающие более уязвимы для атак [83].

Правительства также способствуют обмену информацией о безопасности между частными компаниями. В двух документах анализируются стимулы, по которым фирмы должны делиться информацией о нарушениях безопасности в Центрах обмена и анализа информации (ISAC), созданных после 11 сентября.

правительством США [85, 86]. Теоретические инструменты, разработанные для моделирования торговых ассоциаций и исследовательских совместных предприятий, могут применяться для определения оптимальных членских взносов и других стимулов.

* 1. Варианты практической политики

В отчете, подготовленном по заказу Европейского агентства по сетевой и информационной безопасности (среди авторов которого мы являемся), исследованы практические политические действия по согласованию стимулов для повышения информационной безопасности на уровне ЕС [87]. В течение долгого времени ощущалась нехватка достоверных данных о сбоях в области информационной безопасности, поскольку многие из доступных статистических данных не только неполноценны, но и собираются такими сторонами, как поставщики средств защиты или правоохранительные органы, которые кровно заинтересованы в занижении или завышении данных. Банки и интернет-провайдеры — это две особенно проблематичные «черные дыры», где данные фрагментарны или просто недоступны. Несколько рекомендаций направлены на сбор и публикацию надежных статистических данных, начиная с принятия всесторонних законов о раскрытии информации о нарушениях безопасности и сбора последовательной общеевропейской статистики мошенничества.

Широко известно, что хорошо работающие интернет-провайдеры тщательно выявляют зараженные машины и помещают их в карантин, а плохо работающие интернет-провайдеры — нет. Первым шагом в решении этой проблемы является сбор более качественных данных о количестве спама и другого нежелательного трафика, испускаемого интернет-провайдерами. Однако одной прозрачности недостаточно, так как зараженные машины часто не наносят вреда своим владельцам, а вместо этого загрязняют цифровую среду, рассылая спам, размещая фишинговые веб-сайты и распространяя нелегальный контент.

Эти внешние эффекты должны быть интернализованы, и в отчете рекомендуется довольно радикальный подход: введение установленной законом шкалы убытков для интернет-провайдеров, которые не реагируют оперативно на запросы об удалении скомпрометированных машин. Фиксированные штрафы полезны, потому что они позволяют избежать проблемы количественной оценки убытков после каждого нарушения. Они эффективно использовались в авиационной отрасли, где ЕС ввел штрафы для авиакомпаний, которые отказывают пассажирам в посадке из-за овербукинга, отмены или чрезмерных задержек. Цель фиксированных штрафов — обеспечить эффективное сдерживание, упрощая при этом ответственность в случае совершения нарушений.

Еще одним важным моментом отчета являются его рекомендации по ответственности за дефектное программное обеспечение. Он придерживается прагматичного взгляда на то, что ответственность за программное обеспечение является слишком серьезной проблемой, чтобы решать ее за один раз, из-за большого и растущего разнообразия товаров и услуг, в которых программное обеспечение играет решающую роль. Также важно не делать различий между различными модальностями обслуживания. Например, навигационная служба может предоставляться в виде устройства GPS, онлайн-службы, программного обеспечения для телефона, КПК или ноутбука или их комбинации; это исказило бы рынок, если бы водитель грузовика, который полагался на некачественную услугу и застрял в узкой полосе, мог подать в суд только в том случае, если услуга была оказана определенным образом.

В отчете рекомендуется поэтапный подход, при котором отдельные продукты и услуги будут регулироваться существующими нормами безопасности, ответственности за качество продукции и прав потребителей. В Европе уже существует множество положений о стандартах для всего, от автомобилей до телевизоров. Новая проблема связана с подключением. Что, если устройства, подключенные к сети, заразятся и начнут распространять спам или фишинг? Поскольку сетевые системы могут причинить вред другим, предлагается, чтобы Европа разработала соответствующие стандарты и потребовала от поставщиков удостоверять, что их продукты безопасны по умолчанию. Если позже выяснится, что сертификация была ошибочной, поставщик будет нести ответственность, и интернет-провайдеры могут взыскать с него штрафные санкции.

1. открытых проблем

Есть много активных областей исследований в области экономики безопасности. Здесь мы выделяем только четыре живые задачи. Каждая из них лежит не только на границе между безопасностью и экономикой, но и на границе между экономикой и какой-то другой дисциплиной — соответственно проектированием алгоритмических механизмов, наукой о сетях, организационной теорией и психологией.

#### Разработка алгоритмического механизма

Учитывая в значительной степени неудовлетворительное влияние регулирования информационной безопасности, появляется дополнительный подход, основанный на структуре механизма. Исследователи начинают разрабатывать сетевые протоколы и интерфейсы, которые «защищены от стратегии», то есть спроектированы так, чтобы никто не мог получить выгоду от мошенничества [88]. Разработка плохого поведения из систем может быть дешевле, чем последующее его контролирование.

Одной из ключевых задач является справедливое распределение пугающих цифровых ресурсов, и теория аукционов может дать ключ к решению этой проблемы. Нисан и Сигал показывают, что, хотя можно решить проблему распределения, используя механизмы защиты от стратегии, количество битов, которые необходимо передать, растет экспоненциально; таким образом, во многих случаях лучшим практическим механизмом будет простой групповой аукцион [89]. Они также предполагают, что, если произвольные оценки разрешены, игроки могут подавать заявки, которые вызовут проблемы со связью для всех аукционов, кроме самых маленьких.

Некоторые многообещающие первоначальные результаты касаются конструкции механизма и протоколов. Фейгенбаум и др. показать, как методы комбинаторных аукционов могут быть использованы для обеспечения распределенных механизмов маршрутизации, защищенных от стратегии [90]. Шнейдман и др. сравните механизмы поощрения в BitTorrent, популярном одноранговом приложении для обмена файлами, с теоретическими гарантиями достоверности [91].

* 1. Топология сети и информационная безопасность

Недавно было интересное сотрудничество между физиками и социологами при анализе топологии сложных сетей и ее влияния на социальные взаимодействия. Компьютерные сети, как и социальные сети, сложны, но возникают в результате случайных взаимодействий многих сущностей, использующих простые базовые правила. Новая дисциплина сетевого анализа берет идеи из социологии, физики конденсированных сред и теории графов и, в свою очередь, предоставляет инструменты для моделирования и исследования таких сетей (см. недавний обзор [92]). Некоторые экономисты также признали влияние сетевой структуры на целый ряд видов деятельности, от преступности [93, 94] до распространения новых технологий [95]. Другие исследователи сосредоточились на том, почему формируются сети, где индивидуальные затраты на установление связи между агентами сопоставляются с общей выгодой от улучшения связи [96]. Экономические модели хорошо подходят для сравнения социальной эффективности различных типов сетей и прогнозирования того, какие структуры могут возникнуть, когда агенты действуют эгоистично. См.

[97] для сбора последних работ.

Топология сети может сильно влиять на динамику конфликта. Часто злоумышленник пытается отключить сеть или увеличить ее диаметр, уничтожая узлы или ребра, в то время как защитник использует различные механизмы устойчивости. Примеры включают попытку органа музыкальной индустрии закрыть одноранговую сеть обмена файлами; полиция пытается обезглавить террористическую организацию; и тоталитарное правительство, преследующее политические

активисты. Полиция уже несколько лет интересуется, может ли сетевая наука иметь практическое применение в тайных конфликтах – будь то повстанцы или силы по борьбе с повстанцами.

Разные топологии имеют разные свойства надежности. Albert, Jeong и Barabási показали, что некоторые реальные сети с безмасштабным распределением степеней сопротивляются случайным атакам гораздо лучше, чем целенаправленным атакам [98]. Это связано с тем, что безмасштабные сети, как и многие реальные сети, получают большую часть своей связности от нескольких узлов с высоким порядком вершин. Эта устойчивость делает их очень устойчивыми к случайным сбоям; но удалите «ключевые» узлы, и связь рухнет.

Это статический случай — например, когда полиции становится известно о преступной или террористической сети, и она намеревается разрушить ее, найдя и арестовав ее ключевых людей. Нагараджа и Андерсон распространяют это на динамический случай. В их модели злоумышленник может удалять определенное количество узлов в каждом раунде, после чего защитники набирают другие узлы для их замены [99]. Они изучили, как взаимодействуют атака и защита, используя многоэтапное моделирование, и обнаружили, что формирование локализованных структур клики в ключевых точках сети работает достаточно хорошо, в то время как защита, основанная на кольцах, вообще не работает. Это помогает объяснить, почему одноранговые системы с кольцевой архитектурой оказались довольно хрупкими и почему революционеры склонны организовываться в ячейки.

Открытая проблема заключается в том, как согласовать различия между сгенерированными сетевыми моделями и компьютерными сетями. Распределение степеней — это только один фактор в структуре сети. Ли и др. внимательно изучил топологию компьютерных сетей [100] и обнаружил, что атаки на степень централизации в Интернете не работают, поскольку граничные маршрутизаторы, которые подключаются к домам, имеют гораздо более высокую степень, чем магистральные маршрутизаторы на основных IPS. Однако для атак на частную жизнь топологический анализ оказался весьма эффективным. Когда Данезис и Виттнебен применили эти идеи сетевого анализа к приватности [101], они обнаружили, что анализ трафика всего нескольких организаторов с хорошими связями может привлечь к сети наблюдения удивительное количество членов диссидентской организации.

* 1. Управление крупными проектами

Наряду с распространением на проектирование систем, преступность и скрытые конфликты, экономика безопасности может помочь изучающим управление информационными системами. Возможно, самой большой проблемой здесь является риск провала крупных программных проектов, которые могут стоить миллиарды и угрожать выживанию организаций.

Выше мы отмечали, что, возможно, 30% крупных проектов разработки терпят неудачу [24], и эта цифра кажется невосприимчивой к техническому прогрессу: более совершенные инструменты помогают инженерам создавать более крупные системы, доля которых по-прежнему терпит неудачу, как и прежде. Это говорит о том, что неудача проекта связана не с техническими причинами, а с социально-экономическими факторами, такими как способ принятия решений в фирмах. Таким образом, возникает искушение сопоставить то, что мы сейчас знаем об экономике надежности, с институциональной экономикой и провести анализ пробелов.

Один интересный вопрос заключается в том, особенно ли организации государственного сектора подвержены провалу крупных программных проектов. Директор по информационным технологиям Министерства труда и пенсий Великобритании недавно признал, что только 30% государственных ИТ-проектов достигают успеха [102]. Есть много возможных причин. В литературе по надежности говорится, что неудачи крупных программных проектов в основном связаны с чрезмерно амбициозными, расплывчатыми или меняющимися спецификациями в сочетании с

плохая коммуникация и неспособность распознать признаки сбоя достаточно рано, чтобы предпринять корректирующие действия. Хорошие менеджеры промышленных проектов стараются быстро закрыть варианты и заставить клиента заранее принять трудные решения. Избранные политики, с другой стороны, занимаются посредничеством в конфликтах между различными интересами и группами в обществе, и, поскольку многие из этих конфликтов преходящи, избегание или отсрочка трудного выбора является добродетелью. Кроме того, в равновесии системы имеют слишком много функций, потому что предельная выгода от типичной функции достается небольшой группе голосов, в то время как затраты распределяются между большой пользовательской базой в виде слегка повышенного риска отказа. Это равновесие может быть еще дальше от оптимума, когда проектные решения принимаются выборными должностными лицами: хорошо известные стимулы к снятию ответственности, чтобы не принимать во внимание последствия, которые наступят после следующих выборов или перетасовок, и чтобы никогда не признавать ошибки, обязательно добавляйте их долю. Таким образом, экономика надежности может быть интересной темой для исследователей в школах государственного управления.

* 1. Психология и безопасность

Последняя точка, в которой экономика безопасности дает начало другой дисциплине, связана с психологией — областью, с которой инженеры по безопасности уже имели по крайней мере три точки соприкосновения. Во-первых, три известных эксперимента в области социальной психологии показали, с какой легкостью над людьми могут запугивать авторитетные лица или убеждать сверстников вести себя неподобающим образом. В 1951 году Соломон Аш показал, что большинство людей можно убедить отрицать свидетельство своих собственных глаз, чтобы соответствовать группе [103]; В 1961 году Милграм показал, что большинство людей подвергают сильному удару током актера, играющего роль «ученика», по указанию экспериментатора, играющего роль

«учителя», даже если «ученик» находится в тяжелом состоянии. боль и умолял субъекта остановиться [104]; а в 1971 г. Стэнфордский эксперимент с заключенными показал, что нормальные люди могут подстрекать друг друга к дурным поступкам даже при отсутствии приказа. Там студенты, играющие роль надзирателей, так жестоко издевались над студентами, играющими роль заключенных, что эксперимент пришлось прекратить [105].

Неуместное подчинение — актуальная проблема: воры карт звонят держателям карт, выдают себя за сотрудников банка и требуют ПИН-код [2, 75]. Хуже того, в 1995-2005 годах мошенник, называвший себя

«офицером Скоттом», приказал менеджерам десятков магазинов и ресторанов США задержать какую-то молодую сотрудницу по подозрению в краже и обыскать ее или его с раздеванием. Были заказаны различные другие унижения, включая избиения и сексуальные посягательства. Не менее 13 человек, подчинившихся звонившему и производивших обыски, были привлечены к уголовной ответственности, а семеро осуждены[106]. В октябре 2007 года присяжные обязали McDonalds выплатить 6,1 миллиона долларов одной из жертв, подвергшейся обыску с раздеванием и непристойному насилию в 18-летнем возрасте [107].

Второй точкой соприкосновения было удобство использования безопасности, которое в последнее время стало областью роста; первые результаты собраны в [108]. Третьим было изучение обмана

- несколько менее четко определенная область, но которая простирается от колдовства до маскировки и изучения мошенничества, и которая больше интересует сообщество пользователей, занимающихся безопасностью, поскольку фишинг становится серьезной проблемой.

Здесь также есть потенциально ценный интерфейс с экономикой. Экономический анализ традиционно предполагал, что руководители рациональны и действуют исключительно в личных интересах. Реальные люди по-разному отходят от этого идеала, и в последнее время возникла

лет энергичная школа экономической психологии или поведенческой экономики, изучающая влияние социальных и когнитивных предубеждений человека на принятие экономических решений. Нобелевская премия 2002 года была присуждена Даниэлю Канеманну за его основополагающую роль в создании этой области, особенно в принятии решений в условиях риска и неопределенности. Мы уже упоминали поведенческую экономику в контексте конфиденциальности, и ее обширные исследования эвристики и предубеждений, которые мы используем в нашей повседневной жизни, могут научить инженера по безопасности гораздо большему [109]. В дополнение к неприятию потерь, учету времени и неопределенности предпочтений существуют проблемы *обрамление*–действие как выгода, а не как потеря, повышает вероятность того, что люди его предпримут; в *эвристика доступности*при этом легко запоминаемые данные имеют больший вес при умственной обработке; в *закрепляющий эффект*посредством чего мы основываем суждение на первоначальном предположении или сравнении, а затем при необходимости корректируем его; предубеждения канала (мы более склонны скептически относиться к тому, что мы слышали, чем к тому, что мы видели) и предубеждения в том, как мы имеем дело с мысленным отчетом, начиная от нежелания списывать деньги, которые мы потратили впустую, до склонности слишком сильно беспокоиться о маловероятных событиях.

Шнайер рассматривал когнитивные искажения как основную причину уязвимости нашего общества перед терроризмом [110]. Психолог Дэниел Гилберт в статье с провокационным названием «Если бы только однополый секс вызвал глобальное потепление» также обсуждает, почему мы боимся терроризма гораздо больше, чем изменения климата [111]. У нас есть много встроенных предубеждений, которые имели прекрасный эволюционный смысл, когда мы жили небольшими социальными группами на равнинах Африки полмиллиона лет назад, но теперь могут быть неадекватными. Например, мы более чувствительны к рискам, связанным с преднамеренностью, будь то человека или животного, поскольку распространенными причинами насильственной смерти в то время были голодные львы и враги с острыми палками. Мы также больше боимся неопределенности; редких или незнакомых рисков; рисков, контролируемых другими, особенно «посторонних» или других людей, которым мы не доверяем или считаем морально оскорбительными. Некоторые из этих предубеждений связаны с дефектами нашего мысленного учета.

Изучение когнитивных искажений также может помочь выявить случаи мошенничества и фишинга. *Основная ошибка атрибуции*–что люди часто ошибаются, пытаясь объяснить вещи преднамеренно, когда их причины на самом деле безличны, — подрывает усилия по обузданию фишинга, рассказывая пользователям о кровавых деталях дизайна Интернета — например, предлагая им анализировать URL- адреса в электронных письмах, которые кажутся приходят из банка. Как только пользователи запутаются, они перестанут судить о веб-сайте по его «внешнему виду».

Одной из потенциальных областей исследования является гендер. Недавно люди осознали, что программное обеспечение может создавать барьеры для женщин, и это привело к исследовательской работе по «гендерному человеко-компьютерному взаимодействию» — тому, как следует разрабатывать программное обеспечение, чтобы женщины и мужчины могли его эффективно использовать. Психолог Саймон Барон-Коэн классифицирует человеческий мозг на тип S (систематизаторы) и тип E (эмпатизаторы) [112]. Люди типа S лучше разбираются в геометрии и некоторых видах символического мышления, в то время как люди типа E лучше разбираются в языке и многопроцессорности. Большинство мужчин относятся к типу S, в то время как большинство женщин относятся к типу E. Конечно, врожденные способности могут модулироваться многими факторами развития и социальными факторами. Однако даже при беглом прочтении этот материал вызывает подозрение, что многие механизмы безопасности далеко не гендерно-нейтральны.

Еще одна группа вопросов касается того, как мы развили наше восприятие самих себя, и

– критически – других. Еще одно интересное открытие из работы Барона-Коэна заключается в том, что люди больше всего отличаются от других приматов тем, что у нас есть теория разума; наш

мозг устроен так, что мы можем представить других такими же, как мы, чтобы лучше сопереживать им. Действительно, в психологии и приматологии существует направление исследований, уходящих корнями в 1970-е годы, в которых утверждается, что мы развили свой интеллект в социальном контексте: положительный способ выразить это состоит в том, что совладание со сложными социальными группами стало адаптивным, в то время как более циничная версия что люди, которые были хороши в обмане или в обнаружении обмана в других, имели больше выживших потомков. Без сомнения, наши способности совместно развивались на протяжении многих поколений лжи, социальных манипуляций, сексуальных измен и мести. Эта гипотеза «макиавеллистского мозга», разработанная Хамфри, Бирном, Уайтеном и другими [113], должна быть смягчена наблюдением, что, поскольку более социальными (тип Е) индивидуумами, как правило, являются женщины, социальный мозг мог быть, по крайней мере, в такой же степени связан с воспитанием молодежи. С другой стороны, археологи, такие как Стивен Леблан, показали, что большинство людей большую часть времени жили в состоянии хронической межплеменной войны

— как, впрочем, и группы шимпанзе по сей день [114]. Возникшее в результате эволюционное давление научило нас сотрудничать с членами нашей собственной группы, а также рассматривать членов конкурирующих групп как хищников, добычу или даже паразитов и жестоко обращаться с ними [115]. Такое исследование, безусловно, важно для инженера по безопасности, а также увлекательно: наша профессия на протяжении тысяч, а может быть, и миллионов лет была связана с интеллектуальным и культурным развитием человека. археологи, такие как Стивен ЛеБлан, показали, что большинство людей большую часть времени жили в состоянии хронической межплеменной войны – как, впрочем, и по сей день живут группы шимпанзе [114]. Возникшее в результате эволюционное давление научило нас сотрудничать с членами нашей собственной группы, а также рассматривать членов конкурирующих групп как хищников, добычу или даже паразитов и жестоко обращаться с ними [115]. Такое исследование, безусловно, важно для инженера по безопасности, а также увлекательно: наша профессия на протяжении тысяч, а может быть, и миллионов лет была связана с интеллектуальным и культурным развитием человека. археологи, такие как Стивен ЛеБлан, показали, что большинство людей большую часть времени жили в состоянии хронической межплеменной войны – как, впрочем, и по сей день живут группы шимпанзе [114]. Возникшее в результате эволюционное давление научило нас сотрудничать с членами нашей собственной группы, а также рассматривать членов конкурирующих групп как хищников, добычу или даже паразитов и жестоко обращаться с ними [115]. Такое исследование, безусловно, важно для инженера по безопасности, а также увлекательно: наша профессия на протяжении тысяч, а может быть, и миллионов лет была связана с интеллектуальным и культурным развитием человека.

# Выводы

За последние несколько лет исследовательская программа по экономике безопасности установила много междисциплинарных связей и принесла много полезных (и действительно восхитительных) идей из неожиданных мест. Многие извращенные вещи, давно известные специалистам по безопасности, но просто отвергнутые как «плохая погода», оказываются вполне объяснимыми с точки зрения стимулов, стоящих перед отдельными лицами и организациями, а также с точки зрения различных видов провалов рынка.

Что касается будущего, то работа примерно сотни исследователей, активно работающих в этой области, начала распространяться как минимум на четыре новые области. Во-первых, это технический вопрос о том, как мы можем разработать более совершенные системы, сделав протоколы устойчивыми к стратегии, чтобы априори устранить стимулы для стратегического или злонамеренного поведения.

Второй - это экономика безопасности в целом, где есть сходство с экономистами, изучающими такие темы, как преступность и война. Причины повстанческого движения и инструменты для понимания и борьбы с повстанческими сетями являются очевидным аттрактором.

В-третьих, экономика надежности. Крупные системные сбои обходятся отрасли в миллиарды долларов, а в государственном секторе проблемы кажутся еще более неразрешимыми. Нам нужно лучше понять, какие институты могут лучше всего развиваться и управлять большими сложными взаимосвязанными системами.

Наконец, граница между экономикой и психологией кажется особенно плодотворной как в качестве источника практических идей для разработки более удобных в использовании безопасных систем, так и в качестве источника более глубокого понимания фундаментальных вопросов.

БлагодарностиЭто развивающийся обзорный документ быстро развивающейся области. Его ранняя версия была представлена на SoftInt 2007, а более поздняя — на Crypto 2007. Авторы также выступили с рядом приглашенных докладов на эту тему и выражают благодарность

много отзывов от зрителей и от коллег. Тайлер Мур поддерживается Британской комиссией памяти Маршалла и Национальным научным фондом США.

# Ссылки

* 1. Майкл Мастандуно, «Экономика и безопасность в государственном управлении и науке»,

*Международная организация*т. 52 № 4 (осень 1998 г.)

* 1. Росс Андерсон, «Почему криптосистемы терпят неудачу», *Коммуникации ACM*т. 37, № 11 (ноябрь 94 г.), стр. 32–40.
	2. Ян Эйрес, Стивен Левитт, «Измерение положительных внешних эффектов от ненаблюдаемых мер предосторожности для жертв: эмпирический анализ Lojack», рабочий документ NBER № W5928; Также *Ежеквартальный журнал экономики*т. 113 стр. 43–77
	3. Джин Кэмп, Кэтрин Вольфрам, «Безопасность ценообразования», *Материалы семинара CERT по информационной живучести*(24–26 октября 2000 г.), стр. 31–39.
	4. Хэл Вариан, Управление рисками безопасности в Интернете, Колонка экономических наук, The New York Times, 1 июня 2000 г.
	5. Ник Бом, Ян Браун и Брайан Гладман, «Электронная коммерция: кто несет риск мошенничества?» *Журнал информации, права и технологий*v 3 York Times, 1 июня 2000 г.
	6. Росс Андерсон, «Закрытие фишинговой дыры — мошенничество, риск и небанковские учреждения», *Небанковские организации в платежной системе*, Санта-Фе, май 2007 г.
	7. Тайлер Мур, «Противодействие скрытым атакам на сетевые системы», *Четвертый семинар по экономике информационной безопасности*, июнь 2005 г., Гарвард.
	8. Росс Андерсон, «Служба вечности», *Прагокрипт 96*
	9. Джордж Данезис и Росс Андерсон, «Экономика сопротивления цензуре», в *Безопасность и конфиденциальность IEEE*т. 3 № 1 (2005), стр. 45–50.
	10. Дэвид Гудхарт, «Слишком разнообразно?», *Проспект*(февраль 2004 г.) и вhttp:// [www.](http://www/) guardian.co.uk/race/story/0,11374,1154684,00.html
	11. Росс Дж. Андерсон, «Почему информационная безопасность сложна — экономическая перспектива», в*17-я ежегодная конференция по приложениям компьютерной безопасности*( декабрь 2001 г.) и вhttp: //[www.cl.cam.ac.uk/users/rja14/Papers/econ.pdf](http://www.cl.cam.ac.uk/users/rja14/Papers/econ.pdf)
	12. Джек Хиршлейфер, «От самого слабого звена к лучшему: добровольное предоставление общественных благ», *Общественный выбор*т. 41, (1983), стр. 371–386.
	13. Хэл Вэриан, «Надежность системы и бесплатная поездка», *Экономика информационной безопасности*

, Клювер, 2004 г., стр. 1–15.

* 1. Ховард Кунройтер и Джеффри Хил, «Взаимозависимая безопасность», *Журнал риска и неопределенности*т. 26, № 2–3 (март – май 2003 г.), стр. 231–249.
	2. Майкл Кац и Карл Шапиро, «Внешние эффекты сети, конкуренция и совместимость», в

*Американский экономический обзор*v 75 № 3 (июнь 1985 г.), стр. 424–440.

* 1. Энди Озмент и Стюарт Шехтер, «Начало внедрения протоколов безопасности в Интернете», Пятый семинар по экономике информационной безопасности (26–28 июня, Кембридж, Великобритания)
	2. Росс Андерсон, «Открытые и закрытые системы эквивалентны (то есть в идеальном мире)», в*Перспективы бесплатного программного обеспечения и программного обеспечения с открытым исходным кодом*, MIT Press, 2005, стр. 127–142.
	3. Эрик Рескорла, «Является ли поиск дыр в безопасности хорошей идеей?», Третий семинар по экономике информационной безопасности (2004 г.)
	4. Энди Озмент, «Вероятность повторного обнаружения уязвимостей и социальная полезность поиска уязвимостей», Четвертый семинар по экономике информационной безопасности (2005 г.)
	5. Энди Озмент и Стюарт Шехтер, «Молоко или вино: улучшается ли безопасность программного обеспечения с возрастом?» в*15-й симпозиум по безопасности Usenix*(2006)
	6. Ашиш Арора, Рахул Теланг и Хао Сюй, «Оптимальная политика раскрытия уязвимостей программного обеспечения», Третий семинар по экономике информационной безопасности (май 2004 г., Миннеаполис, Миннесота)

###### Ашиш Арора, Рамайя Кришнан, Ананд Нандкумар, Рахул Теланг и Юбао Ян, Влияние раскрытия уязвимостей и доступности исправлений — эмпирический анализ, Третий семинар по экономике информационной безопасности (2004 г.)

* 1. Билл Кертис, Херб Краснер, Нил Иско, «Полевые исследования процесса проектирования программного обеспечения для больших систем», *Коммуникации ACM*т. 31, № 11 (ноябрь 88), стр. 1268–1287.
	2. Карл Шапиро, Хэл Вариан,*'Информационные правила*, издательство Гарвардской школы бизнеса (1998)
	3. Джордж Акерлоф, «Рынок лимонов: неопределенность качества и рыночный механизм», *Ежеквартальный журнал экономики*т. 84, № 3 (1970), стр. 488–500.
	4. Росс Андерсон, «Криптография и конкурентная политика — проблемы с «доверенными вычислениями», второй семинар по экономике и информационной безопасности (2003 г.)
	5. ВИЗА,*Требования к управлению PIN-кодом: Руководство по требованиям к безопасности устройства для ввода PIN-кода*(2004)
	6. Стюарт Шехтер, «Надежность и риск компьютерной безопасности: количественный подход», Гарвардский университет, май 2004 г.
	7. Картик Каннан и Рахул Теланг, «Экономический анализ рынка уязвимостей программного обеспечения», Третий семинар по экономике информационной безопасности (2004 г.)
	8. Райнер Бёме, «Сравнение рыночных подходов к раскрытию уязвимостей программного обеспечения», *ЭТРИКС 2006*Springer LNCS v 2995, стр. 298–311.
	9. Энди Озмент, «Аукционы ошибок: пересмотр рынков уязвимостей», Третий семинар по экономике информационной безопасности (2004 г.)

###### Райнер Бёме и Гаурав Катариа, «Модели и меры для корреляции в киберстраховании», Пятый семинар по экономике информационной безопасности (2006 г.)

* 1. Хулиси Огут, Нируп Менон и Шринивасан Рагунатан, «Киберстрахование и инвестиции в ИТ-безопасность: влияние взаимозависимых рисков», Четвертый семинар по экономике информационной безопасности (2005 г.)
	2. Ричард Познер, «Экономическая теория конфиденциальности», в*Регулирование*(1978), стр. 19–26.
	3. Ричард Познер, «Конфиденциальность, секретность и репутация» в*Обзор закона Буффало*т. 28 № 1 (1979)
	4. Джек Хиршлейфер, «Конфиденциальность: ее происхождение, функции и будущее», *Журнал юридических исследований*т. 9 (декабрь 1980 г.), стр. 649–664.
	5. Хэл Вариан, «Экономические аспекты личной конфиденциальности», *Конфиденциальность и саморегулирование в век информации*, отчет Национального управления по телекоммуникациям и информации, 1996 г.
	6. Эндрю Одлызко, «Конфиденциальность, экономика и ценовая дискриминация в Интернете», в

*ICEC '03: Материалы 5-й международной конференции по электронной коммерции* стр. 355–366

###### Алессандро Аккисти и Хэл Вариан, «Кондиционирование цен в истории покупок» в

*Маркетинговая наука*в 24 № 3 (2005)

* 1. Алессандро Аккисти и Йенс Гроссклагс, «Конфиденциальность и рациональность: предварительные данные экспериментальных данных», Третий семинар по экономике информационной безопасности (2004 г., Миннеаполис, Миннесота)
	2. Г. Левенштейн, «В поисках конфиденциальности во всех неправильных местах: взгляд поведенческой экономики на индивидуальную заботу о конфиденциальности», на семинаре по экономике информационной безопасности, 2007 г.
	3. Тони Вила, Рэйчел Гринштадт и Дэвид Молнар, «Почему нам нельзя читать политику конфиденциальности», в*Экономика информационной безопасности*(Клувер, 2004), стр. 143–154.
	4. P Swire, «Эффективная конфиденциальность для конфиденциальности, безопасности и конфиденциальной деловой информации», Brookings-Wharton Papers on Financial Services (Brookings, 2003)
	5. Кэтрин Кэмпбелл, Лоуренс Гордон, Мартин Леб и Лей Чжоу, «Экономическая стоимость публично объявленных нарушений информационной безопасности: эмпирические данные фондового рынка», в*Журнал компьютерной безопасности*т. 11 № 3 (2003), стр. 431–448.
	6. Алессандро Аккисти, Аллан Фридман и Рахул Теланг, «Стоит ли нарушение конфиденциальности в цене?», Пятый семинар по экономике информационной безопасности (2006 г.)
	7. Ян Букерт и Ханс Дегриз, «Выбор в сравнении с отказом: бесплатный анализ политик конфиденциальности», Пятый семинар по экономике информационной безопасности (2006 г.)

###### Хэл Вэриан, Фредрик Валленберг и Гленн Ворох, «Демография списка «не звонить», в

*Безопасность и конфиденциальность IEEE*т. 3 № 1 (2005), стр. 34–39.

* 1. Роджер Динглдайн и Ник Мэтьюсон, «Анонимность любит компанию: удобство использования и сетевой эффект», Workshop on Usable Privacy and Security Software (2004)
	2. [http://tor.eff.org](http://tor.eff.org/)
	3. Хэл Вэриан, «Новые чипы и держите потребителей в ежовых рукавицах, даже после того, как они купят продукт», New York Times, 4 июля 2002 г.
	4. Пэм Самуэльсон и Сюзанна Скотчмер, «Право и экономика обратного инжиниринга» (2002 г.), Йельский юридический журнал.
	5. Эрик фон Хиппель, «Проекты программного обеспечения с открытым исходным кодом как пользовательские инновационные сети», Экономика программного обеспечения с открытым исходным кодом, 2002 г. (Тулуза)
	6. Том Лукабо и Дуг Сикер, «Безопасность и блокировка: пример кабельной индустрии США», Семинар по экономике информационной безопасности, 2003 г.; Также *Экономика информационной безопасности*, т. 12 из *Достижения в области информационной безопасности* (Клувер, 2004), стр. 225–246.
	7. Феликс Оберхольцер и Колеман Струмпф, «Влияние совместного использования файлов на продажи пластинок».

- Эмпирический анализ», Кембридж, Массачусетс, июнь 2004 г.

* 1. Хэл Вэриан, Основной доклад на Третьей конференции по управлению цифровыми правами, Берлин, Германия, 13 января 2005 г.

### Стивен Кобб, «Экономика спама», ePrivacy Group,http://www.spamhelp. org/ articles/economics of spam.pdf,2003 г.

* 1. Райнер Бёме и Торстен Хольц, Влияние биржевого спама на финансовые рынки, Семинар по экономике информационной безопасности, 2006 г.
	2. Лаура Фридер и Джонатан Зиттрейн, «Спам работает: данные по рекламе акций и соответствующей рыночной активности», исследовательская публикация Berkman Center № 2006-11, 2006 г.
	3. Адитья Акелла, Шринивасан Сешан, Ричард Карп, Скотт Шенкер и Христос Пападимитриу, «Эгоистичное поведение и стабильность Интернета: теоретико- игровой анализ TCP», ACM SIGCOMM, стр. 117–130.
	4. Элиас Куцупиас и Христос Пападимитриу, «Наихудшее равновесие»,*16-й СТОЦ*, Springer LNCS v 1563, стр. 387–396.
	5. Тим Рафгарден и Эва Тардос, «Насколько плоха эгоистичная маршрутизация?», Журнал ACM 49(2), стр. 236–259, 2002 г.

##### Алекс Фабрикант, Анкур Лутра, Элица Манева, Христос Пападимитриу, Скотт Шенкер, «Об игре по созданию сети»,*22-й ПОДК*(2003), стр. 347–351.

* 1. Эллиот Аншелевич, Анирбан Дасгупта, Эва Тардос и Том Векслер, «Близкий к оптимальному дизайн сети с эгоистичными агентами»,*35-й СТОЦ*стр. 511–520, 2003 г.
	2. Эллиот Аншелевич, Анирбан Дасгупта, Джон Клейнберг, Эва Тардос, Том Векслер, Тим Рафгарден,

«Цена стабильности проектирования сети при справедливом распределении затрат», *45-й ФОКС*(2004), стр. 295–304.

* 1. Магнус М. Халлдорссон, Джозеф Халперн, Ли Ли, Вахаб Миррокни. «Об играх с разделением спектра»,*23-й ПОДК*(2004), стр. 107–114.
	2. Джеймс Аспнес, Кевин Чанг, Александр Ямпольский, «Стратегии прививки для жертв вирусов и проблема разделения суммы квадратов», 16-й симпозиум ACM-SIAM по дискретным алгоритмам (2005), стр. 43–52.
	3. Синтия Дворк и Мони Наор, «Ценообразование посредством обработки или борьбы с нежелательной почтой», *Крипто 92*стр. 139–147
	4. Бен Лори и Ричард Клейтон, «Доказательство выполнения работы доказывает, что оно не работает», Третий семинар по экономике информационной безопасности (2004 г.)
	5. Андрей Сержантов и Ричард Клейтон, «Моделирование стимулов для стратегий блокировки электронной почты», Четвертый семинар по экономике информационной безопасности (2005 г.)
	6. Михал Фельдман, Кевин Лай, Ион Стойка и Джон Чуанг, «Надежные методы стимулирования для одноранговых сетей», Пятая конференция ACM по электронной коммерции, 2004 г.
	7. Крисантос Делларокас, «Анализ экономической эффективности механизмов онлайн-репутации, подобных eBay», Третья конференция ACM по электронной коммерции, 2001 г.
	8. Андрей Сержантов и Росс Андерсон, «О справедливом обращении с противниками», Третий семинар по экономике информационной безопасности (2004 г.)
	9. Карл Ландвер, «Улучшение потока информации на рынке информационной безопасности», в

*Экономика информационной безопасности*(Клювер, 2004), стр. 155–164.

* 1. Росс Андерсон,*'Инженерия безопасности'*, Уайли 2001
	2. *Предложение Европейской комиссии о рамочном решении Совета об атаках на информационные системы*, апрель 2002 г.
	3. *Комментарии федерального правительства Германии о TCG и NGSCB в области доверенных вычислений*(2004), в<http://www.bsi.bund.de/sichere>plattformen/ index.htm
	4. Дуглас Барнс, «Дегельминтизация Интернета», в*Техасский юридический журнал*т. 83, № 279 (2004), стр. 279–329.
	5. Альфредо Гарсия, Барри Горовиц, «Потенциал недостаточного инвестирования в интернет- безопасность: последствия для регуляторной политики», Пятый семинар по экономике информационной безопасности (2006 г.)
	6. Тайлер Мур, «Экономика цифровой криминалистики», Пятый семинар по экономике информационной безопасности (2006 г.)
	7. Аниндья Гхош и Удай Раджан, «Экономическое влияние раскрытия нормативной информации на инвестиции в информационную безопасность, конкуренцию и социальное обеспечение», Пятый семинар по экономике информационной безопасности (2006 г.)
	8. Бенджамин Эдельман, «Неблагоприятный отбор в онлайн-сертификатах доверия», Пятый семинар по экономике информационной безопасности (2006 г.)
	9. Стив Битти, Сет Арнольд, Криспин Коуэн, Перри Уэгл, Крис Райт, Адам Шостак, «Сроки применения исправлений безопасности для оптимального времени безотказной работы», в *ЛИЗА 2002*стр. 233–242

###### Ашиш Арора, Кристофер Форман, Ананд Нандкумар и Рахул Теланг, «Конкурентные и стратегические эффекты в сроках выпуска исправлений», Пятый семинар по экономике информационной безопасности (2006 г.)

* 1. Эстер Гал-Ор и Аниндия Гхош, «Экономические последствия обмена информацией о безопасности»,*Исследование информационных систем*(2005), стр. 186–208.
	2. Ларри Гордон, Мартин Лоэб и Уильям Люцишин, «Экономический взгляд на обмен информацией, связанной с нарушениями безопасности», Первый семинар по экономике информационной безопасности (16-17 мая 2002 г., Беркли, Калифорния)

##### Росс Андерсон, Райнер Бёме, Ричард Клейтон и Тайлер Мур, «Экономика безопасности и внутренний рынок», ENISA, 2008 г.

* 1. Ноам Нисан и Амир Ронен, «Алгоритмический дизайн механизма (расширенный реферат)» в*СТОК '99*(1999), стр. 129–140.
	2. Ноам Нисан и Илья Сигал, «Коммуникационная сложность задач эффективного распределения»*Черновик. Вторая версия 5 марта 2002 г.*
	3. Джоан Фейгенбаум, Христос Пападимитриу, Рахул Сами и Скотт Шенкер, «Механизм BGP для маршрутизации с наименьшими затратами» в*ПОДК '02*стр. 173–182
	4. Джеффри Шнейдман, Дэвид С. Паркс и Лоран Массули, «Верность в интернет- алгоритмах», в*PINS '04: Материалы семинара ACM SIGCOMM по практике и теории стимулов в сетевых системах.*

### Марк Ньюман, «Структура и функция сложных сетей», в*Обзор СИАМ* т. 45 стр. 167–256

* 1. Раадж Сах, «Социальный осмос и модели преступности», в*Журнал политической экономии*т. 99,

№ 6 (1991), стр. 1272–95.

* 1. Коралио Баллестер, Антони Кальво-Арменгол и Ив Зеноу «Кто есть кто в преступных сетях? Разыскивается – ключевой игрок», № 617, серия рабочих материалов НИИ экономики промышленности
	2. Ян Брамуль и Рэйчел Крэнтон «Стратегические эксперименты в сетях», Рабочий документ NajEcon №. 784828000000000417 с сайта [www.najecon.org](http://www.najecon.org/)
	3. Мэтью Джексон, «Экономика социальных сетей», Рабочий документ отдела гуманитарных и социальных наук Калифорнийского технологического института 1237; Также в*Материалы 9-го Всемирного конгресса эконометрического общества*КУБОК 2006
	4. Габриэль Деманж, Мирна Вудерс*'Группообразование в экономике: сети, клубы и коалиции.*

Издательство Кембриджского университета, 2005 г.

###### Река Альберт, Хавун Чжон и Альберт-ласло Барабаси, «Допускаемость сложных сетей к ошибкам и атакам», в*Природа*т. 406 № 1 (2000), стр. 387–482.

* 1. Шишир Нагараджа и Росс Андерсон, «Топология скрытого конфликта», Пятый семинар по экономике информационной безопасности (2006 г.) Великобритания)
	2. Лун Ли, Дэвид Олдерсон, Уолтер Виллинджер, Джон Дойл, «Основной подход к пониманию топологии Интернета на уровне маршрутизатора», в*СИГКОММ 2004*стр. 3–14
	3. Джордж Данезис, Беттина Виттнебен, «Экономика массового наблюдения», Пятый семинар по экономике информационной безопасности (2006 г.)
	4. Дж. Харли,*основной доклад*, Саммит правительства Великобритании по информационным технологиям, май 2007 г.
	5. С. Э. Аш,*'Социальная психология'*, ОУП 1952 г.
	6. С. Милграм,*'Повиновение авторитету: экспериментальный взгляд»*, HarperCollins (1974, переиздано в 2004 г.)
	7. П. Зимбардо,*'Эффект Люцифера».*, Случайный дом (2007)
	8. Вольфсон, «Самая жестокая мистификация», в*Курьер-Журнал*, 9 октября 2005 г.
	9. KPHO, «Содомированный бывший сотрудник McDonald's выиграл 6,1 млн долларов», KPHO, 6 октября 2007 г.; в<http://www.kpho.com/news/14277937/detail.html>
	10. Л. Кранор,*'Безопасность Юзабилити*, О'Рейли, 2005 г., ISBN 0-596-80827-9
	11. Т. Гилович, Д. Гриффин, Д. Канеман,*'Эвристика и предубеждения — психология интуитивного суждения».*, Издательство Кембриджского университета, 2002 г.
	12. Б. Шнайер, «Психология безопасности»,*ЮАР 2007*, в[www.schneier.com](http://www.schneier.com/)
	13. Д. Гилберт, «Если бы только однополый секс вызвал глобальное потепление», LA Times, 2 июля 2006 г.
	14. С. Барон-Коэн,Существенная разница: мужчины, женщины и экстремальный мужской мозг

, Пингвин, 2003 ISBN 0-141011017

* 1. Р. В. Бирн, А. Убелен,*'Макиавеллистский интеллект - социальная экспертиза и эволюция интеллекта у обезьян, человекообразных обезьян и людей.*, Оксфорд, 1988; и А. Уайтэн, Р. В. Бирн,*'Макиавеллистский интеллект II - Расширения и оценки »*, Кембридж, 1997 г.
	2. S LeBlanc, KE Register,*'Постоянные битвы: почему мы сражаемся»*, Святого Мартина. 2003 г.
	3. Д.Л. Смит, «Почему война?», 5 января 2007 г., стр. http://realhumannature.com/?page id= 26