



Совместный семинар
ПИР-Центра политических исследований
и Фонда гражданских инициатив в политике Интернет
**«ТРАНСФОРМАЦИЯ ПОНЯТИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ
В ИНФОРМАЦИОННУЮ ЭПОХУ»**

25 февраля 2004 г., Отель «Марриотт Ройал Аврора», Зал «Петровский 2»

Тезисы выступления Президента Фонда аналитических программ «Экспертиза»
Урнова М.Ю.

**Возможный подход к пониманию информационной безопасности страны в
современных условиях.**

1. Рабочие определения.

Безопасность системы

«Негативная» формулировка: Защищенность системы от воздействий, делающих невозможным достижение ею своих целей или, как минимум, затрудняющих достижение этих целей (то есть снижающих эффективность функционирования системы).

«Позитивная» формулировка: Создание условий, обеспечивающих возможность достижения системой своих целей.

Национальная безопасность

Когда говорят о «национальной безопасности», под системой обычно понимается страна.

Информационная безопасность

Когда говорят об «информационной безопасности», речь идет о защите информационной подсистемы страны (процессы обмена информацией, поиска, обработки хранения информации и пр.)

2. Целевые функции (цели) и безопасность системы.

Как следует из определения, представления о безопасности существенно зависят от представлений о целях системы.

Долгосрочной целью любой страны является:

- как минимум, неухудшение ключевых характеристик жизнедеятельности страны по сравнению с другими странами («выживание»)

- как максимум, улучшение ключевых характеристик жизнедеятельности страны по сравнению с другими странами («развитие»).

Иная (более технологичная) формулировка цели: обеспечение конкурентоспособности страны в экономике, технологии, политике, культуре, науке, образовании, здравоохранении и других ключевых подсистемах.

3. Уточненные определения национальной и информационной безопасности.

«Позитивное» определение *национальной безопасности*: Создание условий, обеспечивающих конкурентоспособность страны.

«Позитивное» определение *информационной безопасности страны*: Создание условий функционирования информационной подсистемы страны, необходимых для обеспечения конкурентоспособности страны.

4. Условия функционирования информационной подсистемы, необходимые для обеспечения конкурентоспособности страны.

а) Максимизация скорости обмена информацией (во внутренних и международных коммуникациях), минимизация сложностей поиска информации (максимальное облегчение доступа к информации), минимизация стоимости поиска, получения, анализа, хранения и пересылки информации), минимизация «закрытости» информации.

б) Минимизация возможностей нарушения режима «закрытости» информации (минимизация возможностей подрыва конкурентоспособности страны путем промышленного, военного и иного шпионажа и пр.)

в) Оптимизация режима защиты интеллектуальной собственности (нахождение баланса между защитой авторских прав и доступом к инновациям со стороны «пользователей»)

Совершенно очевидно, что условия (а) и (б) конфликтуют и нуждаются в нахождении точки оптимума. В условии (в) проблема нахождения точки оптимума также присутствует в явном виде.

5. Общая формулировка задачи обеспечения информационной безопасности страны.

В самой общей форме задача обеспечения информационной безопасности страны может быть сформулирована как задача нахождения оптимального соотношения между информационной открытостью и информационной закрытостью, где в качестве критерия оптимальности выступает конкурентоспособность страны.

Вообще говоря, эта задача поддается формализации и квантификации. Ее решения могут быть представлены в виде сценарных прогнозов ситуации, в которых необходимые количественные параметры и переменные могут быть получены из имеющейся статистики и на базе экспертных оценок.

В долгосрочном плане (временной горизонт 25-30 лет) критерий конкурентоспособности сводится к сугубо экономическим показателям.

В среднесрочной перспективе (до 10-15 лет) задача выглядит сложнее, однако тоже поддается количественным оценкам.

Одной из самых очевидных задач, требующих экспертного анализа и квантификации, является сопоставление экономической «цены открытости» (уязвимости для промышленного и военного шпионажа) и экономической «цены закрытости» (потерь, связанных со снижением эффективности научных и технологических разработок, качества подготовки кадров и пр.)