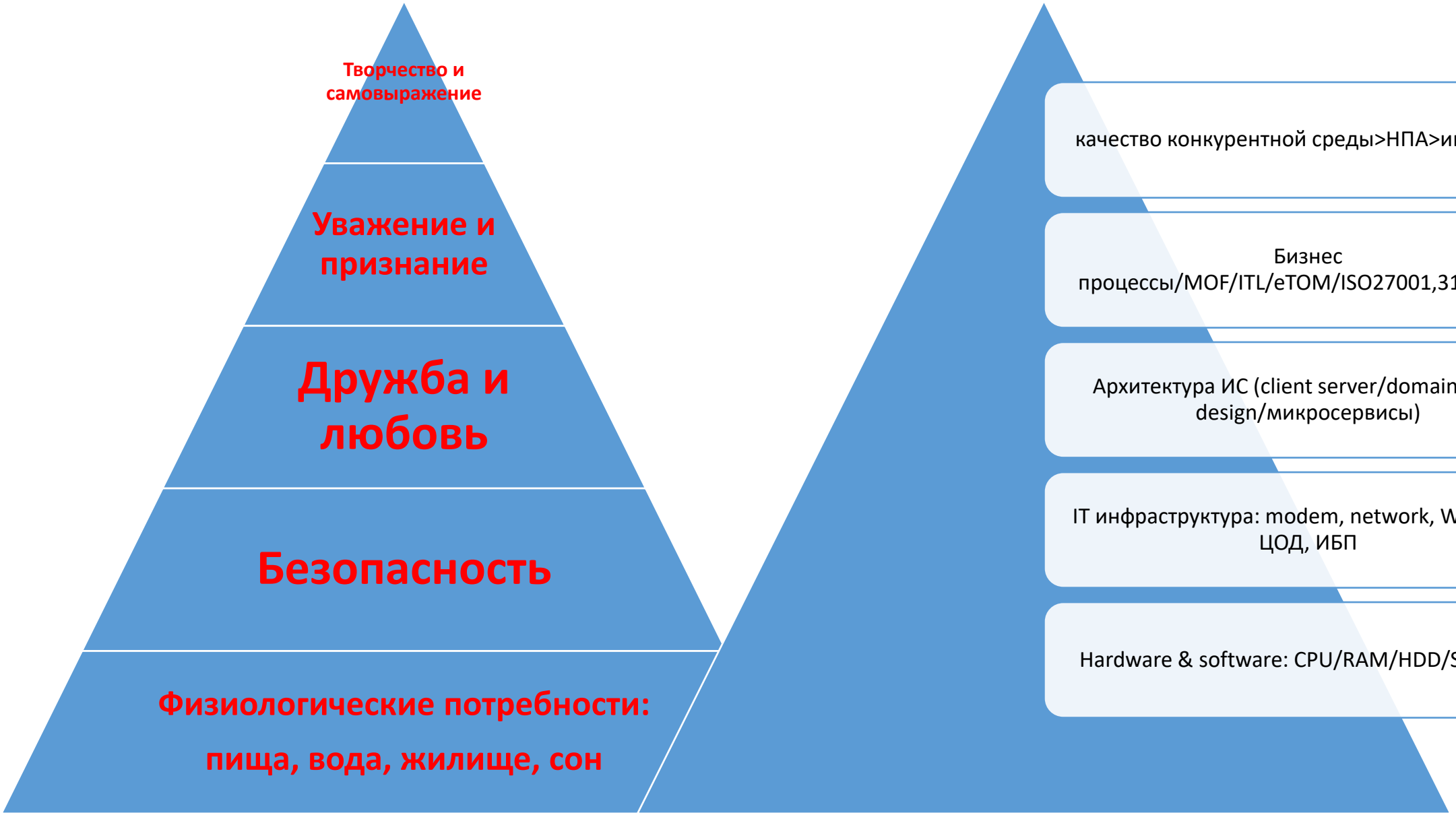

Творчество и самовыражение
Уважение и признание
Дружба и любовь
Безопасность
Физиологические потребности:
пища, вода, жилище, сон
качество конкурентной среды>НПА>институты
Бизнес процессы/MOF/ITL/eTOM/ISO27001,3100,9000
Архитектура ИС (client server/domain driven design/микросервисы)
IT инфраструктура: modem, network, Wi-Fi, СКС, ЦОД, ИБП
Hardware & software: CPU/RAM/HDD/SSD/GPU

новый риск ответственности перед регулятором

- пункт 10 «Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных» №909 в редакции от 18.01.2021 содержит следующее требование:
  - *«Хранение и передача персональных данных ограниченного доступа осуществляются с использованием средств криптографической защиты информации, имеющих параметры не ниже третьего уровня безопасности согласно стандарту Республики Казахстан **СТ РК 1073**-2007 "Средства криптографической защиты информации. Общие технические требования»*

что означает необходимость юридически значимо подтвердить соответствие используемого средства криптографической защиты информации стандарту СТ РК 1073-2007, то есть сертифицировать.

- ЗРК «Об аккредитации в области оценки соответствия» устанавливает лица аккредитованные проводить такую оценку соответствия - их немного, но именно они оказываются единственными выгодоприобретателями такого положения дел
- пункт 2 статьи 3 «Сфера применения настоящего Закона» ЗРК О техническом регулировании исключает из числа объектов технического регулирования продукцию, используемую в целях защиты сведений, относящихся к охраняемой в соответствии с законами РК, информации ограниченного доступа, а значит и Персональные Данные ограниченного доступа, **а ещё продукцию, бывшую в употреблении**
- В совокупности эти обстоятельства, формально истолкованные, образуют нормативную ловушку – капкан для пользователей СКЗИ

СТРК 1073 -2007

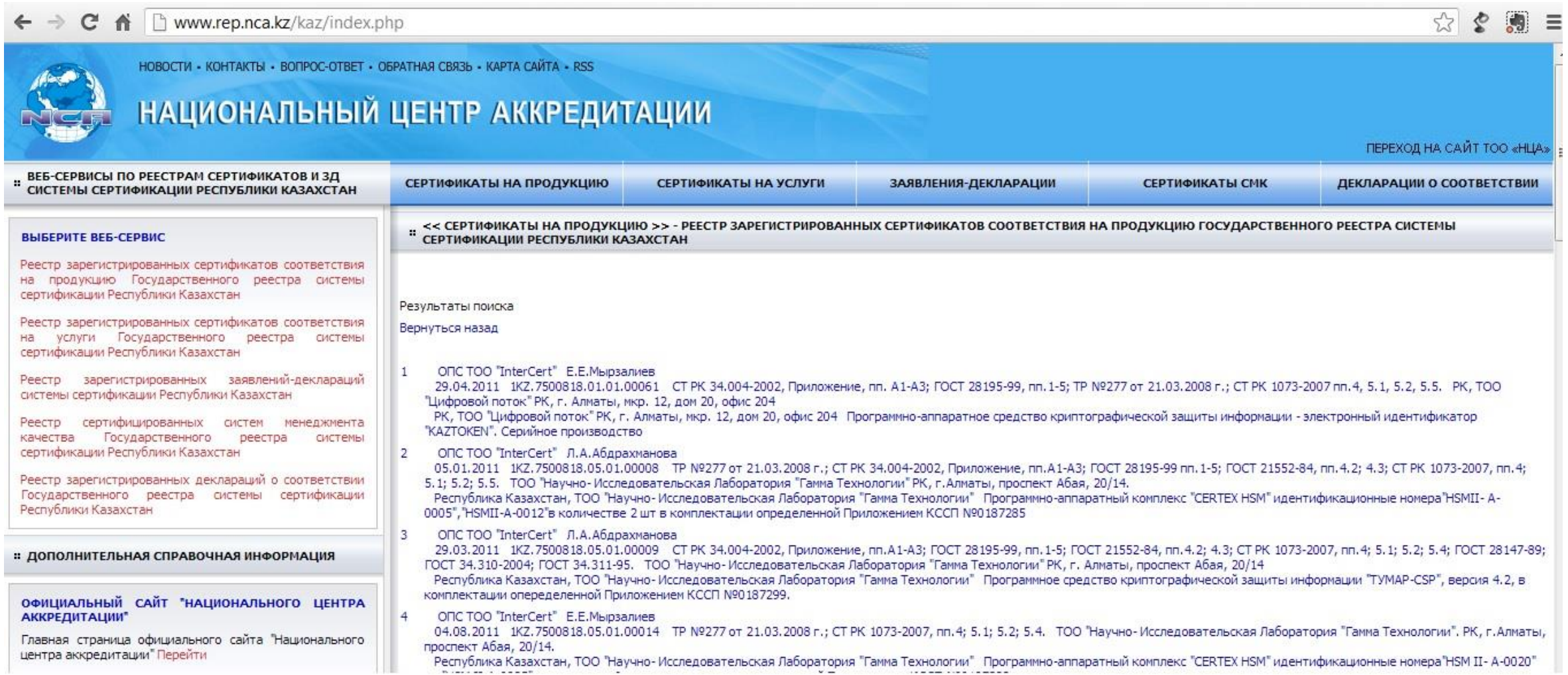
- Разработчик – КНБ Республики Казахстан
- Впервые принят в 2002 году
- Настоящая редакция 2007 года
  - Определить 4 уровня безопасности, увязанные с возможным ущербом от разглашения
  - Определить основные параметры криптографических алгоритмов и допустимые диапазоны их значений
  - Отказаться от определения конкретных криптографических алгоритмов

Требования	I уровень	II уровень	III уровень	IV уровень
Ущерб, МРП	100	10 000	1 000 000	100 000 000
Вычислит-ная сложность	2^{50}	2^{80}	2^{120}	2^{160}
Генератор ключей	случайные события	случайные события	физический шум	физический шум
Длина ключа симм. алгор.	60	100	200	250
Длина ключа асимм. алгор.	500	1500	4000	8000
Длина ключа элл. кривые	120	160	250	400
Длина хэш-кода	120	160	250	400
Длина ЭЦП	120	200	300	400

ECRYPT II(http://ecrypt.eu.org)

длина ключа	защита
32	защита от атак «реального времени» отдельных лиц
64	краткосрочная защита от атак малой организации (бюджет — 10 тыс. $)
72	краткосрочная защита от атак средней организации (бюджет — 300 тыс. $)
80	краткосрочная защита от атак государственного агенства (бюджет — 300 млн. $)
112	среднесрочная защита (на 20 лет) от атак государственных агентств
128	долгосрочная защита (на 30 лет) от атак государственных агентств
256	защита на все обозримое будущее (даже с учетом создания квантовых компьютеров)

Сертифицированные продукты



Сертификация

- Заявление
- Один или несколько экземпляров СКЗИ
- Нормативная и техническая документация
- Эксплуатационная документация
  - Для программных СКЗИ
  - спецификация программного обеспечения
  - архитектура ПО
  - описание логики модулей ПО
  - исходный код ПО
- ЗРК «О техническом регулировании» ограничивает срок сертификации тремя, годами, и позволяет сертифицировать только продукцию не бывшую в употреблении
- Стоимость сертификации превышает 8 млн. тенге

Конфликт интересов

Качественные недорогие СКЗИ	Требуется сертификация, требующая дополнительных расходов – **это рост транзакционных издержек**
Качественная сертификация аккредитованным органом	Предоставление исходных кодов производителями – нереалистичное требование к зарубежным поставщикам СКЗИ, например CheckPoint

Истоки

- Сам по себе СТ РК 1073-2007, принятый в 2007 году, не содержит каких-либо требований специфичных для РК или Таможенного Союза, утратил актуальность, хотя должен пересматриваться каждые 5 лет. Авторы уже не пенсии.
- 15.09.2014 г. Центр Специальной информационной службы КНБ уведомил о разработке проекта изменений в стандарт СТ РК 1073-2007, но тогда, и в 2017 году он был оставлен без изменений.
- В 2020 году, эксперты по криптографии Академии КНБ РК обосновали необходимость обновления стандарта публикацией в журнале «ИЗВЕСТИЯ НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК РЕСПУБЛИКИ КАЗАХСТАН».
- В текущем году наступил срок очередного пересмотра стандарта, а КНБ уже не несёт ответственности за СТ РК 1073-2007.
- Связка устаревшего до бесполезности стандарта, и избыточного регулирования в Правилах№909 оказывает угнетающее воздействие на рынок потребления СКЗИ
- Это положение усугубляет проект внесения изменений в законодательные акты РК по вопросам защиты персональных данных: в том числе в Предпринимательский и Гражданский кодексы, наделяющие уполномоченный орган в сфере защите персональных данных избыточной функцией регулирования - произвольного проведения проверок и профилактического контроля по отношению ко всем субъектам, вовлеченным в процесс сбора и обработки персональных данных.

Solution

- решением описанной проблемы может стать изменение в Правилах№909, исключающее ссылку на СТ РК 1073, и признание стандарта СТ РК 1073-2007 утратившим силу. Такими полномочиями располагает технический комитет по стандартизации № 34 «Информационные технологии», функционирующий на базе АО «Национальный инфокоммуникационный Холдинг «Зерде», и курируемый комитетом технического регулирования и метрологии Министерства по Инвестициям и развитию РК.

Привлечь потенциально заинтересованные организации:

АФР	ЦАРКА
АФК	Кредитные бюро
НБ РК	Ассоциация Телеком операторов
КЦМР	Ассоциация Интернет провайдеров
Казтелепорт	Ассоциация микрофинансовых организаций Казахстана
Астел	Ассоциация страховщиков Казахстана
Казтранском	Казахстанская Ассоциация Информационной Безопасности
Казтелерадио	Служба реагирования на компьютерные инциденты
АО «Зерде»	Ассоциация блокчейн и индустрии дата-центров в Казахстане
АО НИТ	Казахстанская Ассоциация Блокчейн-Технологий
НУЦ	Ассоциация "BLOCKCHAINKZ”
Казсат	Ассоциация Казахстанского Интернет Бизнеса и Мобильной Коммерции
KASE	
KCell	
Билайн	
АО "Казахтелеком"	
Транстелеком	

Обходное решение

- Уведомление прокуратуры и уполномоченного органа о нарушениях – отсутствии сертификатов соответствия СТ РК 1073 на СКЗИ используемые в госучреждениях и предприятиях квазигоссектора, и других. Волна таких заявлений с целью создания прецедентов, с которыми регулятор не сможет не считаться – своего рода «итальянская забастовка»

Вопреки запрета президента на создание национальных операторов

- Планируется организация государственного головного SOC национального масштаба, во главе иерархии отраслевых государственных SOC.
- Вместо этого следует выработать меры регулирования – профилирования рынка услуг SOC. Определить компоненты уровня ядра инфраструктуры InfoSec, и лишь их минимальный набор оставить в составе платформы под присмотром регулятора. Всё остальное отдать в конкурентную среду.

Назарларыңызға рахмет!