Национальный центр цифровой экономики

Доверие и безопасность в цифровой экономике

Ершова Татьяна Викторовна
Директор НЦЦЭ
(МГУ имени М.В. Ломоносова)

Цифровизация и национальная безопасность

Абалкинские чтения – форум Вольного экономического общества России

Москва, 6 марта 2018

Ключевые факторы, влияющие на развитие цифровой экономики

Нецифровые факторы	Цифровые факторы

• Государственная политика и стратегическое планирование
• Лидерство и институты
• Законодательство, регулирование и стандарты
• Человеческий капитал
• НИОКР и инновации в сфере цифровой экономики
• Бизнес-среда
• Доверие и безопасность в цифровой экономике
	• Цифровая инфраструктура
	• Совместно используемые цифровые платформы и сервисы
	• Новые / нарождающиеся цифровые технологии
	• Цифровой сектор экономики
	  ○ ИКТ-сектор
	  ○ Сектор контента и СМИ
	• Цифровая трансформация государственного сектора
	  ○ Цифровое правительство
	  ○ Цифровое здравоохранение
	  ○ Цифровое образование
	  ○ Цифровая культура
	• Цифровая трансформация бизнеса
	• Цифровые граждане / потребители

Доверие и безопасность в цифровой экономике – содержание понятия

- Безопасная информационная инфраструктура
  - сетевая безопасность
  - управление безопасностью данных (доступность, целостность, конфиденциальность), в том числе в аспектах
    - доверия облачным сервисам
    - критическим ошибкам пользователей
    - подлинности онлайн-транзакций
- Повышение доверия граждан и бизнеса к цифровым технологиям
  - обеспечение неприкосновенности частной жизни при работе в онлайновом режиме и освоение способов ее защиты
  - преодоление препятствий для эффективного использования документов и осуществления сделок в электронной форме
  - защита пользовательских данных и прав потребителей
  - защита от спама
  - развитие безопасных и надежных приложений

Меры, принимаемые на глобальном уровне (1)

- Женевская декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии» (принята на Всемирной встрече на высшем уровне по вопросам информационного общества 12 декабря 2003), раздел Б, п. 35:
  - необходимо формировать, развивать и внедрять глобальную культуру кибербезопасности в сотрудничестве со всеми заинтересованными сторонами и компетентными международными организациями
  - необходимо опираться на расширяющееся международное сотрудничество
- Женевский план действий, направление С5, п. 12:
  - доверие и безопасность относятся к главным опорам информационного общества
- Глобальная программа кибербезопасности (Международный союз электросвязи), 2007
  - правовые, технические и процедурные меры, организационные структуры, создание потенциала, международное сотрудничество

Меры, принимаемые на глобальном уровне (2)

- Европейская Конвенция по киберпреступлениям, Будапешт, 23 ноября 2001 – подписали более 50 государств (Россия как член ЕС не присоединилась)
- Концепция сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности (утверждена решением Совета глав государств СНГ от 10 октября 2008)
- Государства-члены ШОС внесли в качестве официального документа ООН «Правила поведения в области обеспечения международной информационной безопасности» (январь 2015)
- Россия подготовила проект конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности» (2016)
  - исключает возможность вмешательства спецслужб третьих стран в чужие компьютерные системы и отдельной статьей описывает механизм защиты суверенитета

Место России в международном рейтинге

Глобальный индекс кибербезопасности МСЭ
2017
165 стран

№	Страна	Баллы
1	Сингапур	0.925
2	США	0.919
3	Малайзия	0.893
…		
9	Канада	0.818
10	Россия	0.788
11	Япония	0.786

Ситуация на национальном уровне (1)

- Национальная политика в сфере обеспечения информационной безопасности
  - государственная политика в сфере информационной безопасности определена в Доктрине информационной безопасности, утвержденной указом Президента РФ в 2016 г.
  - политика информационной безопасности постоянно актуализируется и выполняется в полном объеме

- Решение правовых вопросов в области кибербезопасности
  - защита персональных данных, ведение «черных списков» и контроль провайдеров осуществляется Роскомнадзором (ФЗ 152, ФЗ 139)
  - обеспечение безопасности информации (некриптографическими методами) в системах информационной и телекоммуникационной инфраструктуры контролируется ФСТЭК России
  - обеспечение информационной безопасности (в том числе с использованием инженерно-технических и криптографических средств) осуществляется ФСБ России
  - расследование киберпреступлений находится в ведении МВД России
  - каждое ведомство имеет свою собственную сертификацию и требования к решениям по обеспечению безопасности и защите данных
    - процесс сертификации различен
    - но они тесно увязаны и взаимно согласованы

Ситуация на национальном уровне (2)

- Технические меры по обеспечению информационной безопасности
  - созданы и функционируют государственные и отраслевые центры реагирования на компьютерные инциденты (CERT)
  - центры реагирования на компьютерные инциденты для населения НЕ создавались
    - население может быть подвержено компьютерным атакам, в том числе через социальные сети и мессенджеры, не находящиеся в юрисдикции РФ

- Безопасность критической информационной инфраструктуры
  - осуществляется в соответствии с законодательством (ФЗ «О безопасности критической информационной инфраструктуры РФ» № 187 от 12.07.2017) и требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды
  - деятельность по защите критической инфраструктуры осуществляется с использованием механизмов государственно-частного партнерства
    - но соответствующих механизмов мало и координация вопросов обеспечения информационной безопасности недостаточна

- Повышение осведомленности граждан и организаций об обеспечении информационной безопасности при использовании цифровых технологий
  - отдельных программ такого рода в России нет
  - соответствующие мероприятия осуществляются, в основном, путем популяризации защищенных цифровых продуктов и услуг – интернет-банкинга, предоставления государственных или муниципальных услуг в электронной форме

Оценка России по фактору «Доверие и безопасность» в рамках оценки развития цифровой экономики (Digital Economy Country Assessment, DECA Russia, Всемирный банк, 2017)

Общая оценка текущего состояния и выводы

- Россия активно занимается вопросами обеспечения информационной безопасности
- При этом недостаточно внимания уделяется вовлечению в этот процесс населения: оно является «отстраненным» от этих проблем, что создает угрозы информационной безопасности из-за отсутствия элементарной осведомленности населения
  - следствием данной проблемы является недоверие населения к онлайн-бизнесу, электронной торговле и другим важным составляющим цифровой экономики
- Общая оценка – ***хорошо***

Мероприятия по направлению «Информационная безопасность» программы «Цифровая экономика РФ: (утв. 18 декабря 2017) (1)

Поставлена задача обеспечения технической, организационной и правовой защиты личности, бизнеса и государственных интересов при взаимодействии в условиях цифровой экономики, в том числе:

- в части обработки персональных данных, больших пользовательских данных (включая социальные сети и прочие средства социальной коммуникации)
  - законодательное определение прав и обязанностей участников информационного взаимодействия
  - обеспечение контроля обработки таких данных и доступа к ним
  - установление ответственности за надлежащую обработку и безопасность таких данных
- законодательное обеспечение предустановки отечественных антивирусных программ на все персональные компьютеры, ввозимые и создаваемые на территории РФ
- создание системы получения знаний в области информационной безопасности на основе национальной электронной библиотеки

Мероприятия по направлению «Информационная безопасность» программы «Цифровая экономика РФ (2)

- В части создания технических инструментов, обеспечивающих безопасное информационное взаимодействие граждан в условиях цифровой экономики
  - специализированный ресурс, обеспечивающий гражданам России доступ к информации о случаях использования их персональных данных, а также возможность отказа от такого использования
  - национальная база знаний индикаторов вредоносной активности
  - ресурс антивирусного мультисканера и проверки на наличие признаков вредоносной активности
  - национальная система фильтрации трафика при использовании информационных ресурсов детьми
  - специализированный ресурс, предназначенный для взаимодействия с уполномоченными органами в части оперативной передачи данных о признаках противоправных действий в области информационных технологий (компьютерного мошенничества, навязанных услуг операторов связи, фишинговых схем)
- В части создания организационных условий и институтов
  - национальный и региональные центры реагирования на компьютерные инциденты
  - механизмы государственного содействия росту рынка услуг по страхованию информационных рисков
  - система экспертных организаций в области компьютерной криминалистики

Возможные дополнительные меры на уровне политики (1)

- Целенаправленные усилия правительства по повышению уровня осведомленности и понимания киберугроз обществом
  - поддержка деятельности по защите от угроз и смягчению последствий для населения и организаций, пострадавших от кибератак и кибермошенничества
    - предоставление населению и компаниям актуальных и легких для исполнения рекомендаций
    - создание собственного ПО
    - обмен информацией об актуальных криминальных угрозах
    - широкое распространение этой информации
    - оценка стоимости киберрисков
    - формулирование очевидных преимуществ обеспечения кибербезопасности для бизнеса и населения
    - убеждение организаций и граждан принять необходимые меры

Возможные меры на уровне политики (2)

- Организация сотрудничества по защите от угроз и смягчению последствий кибератак и кибермошенничества для граждан и организаций
  - привлечение авторитетных личностей для расширения охвата рекомендациями общества, повышения их значимости и доверия ним
  - создание / использование волонтерских организаций / групп
  - создание тематических блогов, групп в социальных сетях, научно-популярных программ на телевидении
  - организация сотрудничества вендоров, правоохранительных органов, представителей отраслей и компаний в целях предотвращения появления групп «обманутых юзеров»
  - использование таких организаций, как страховые компании, регулирующие организации, органы отраслевой стандартизации и инвесторы, которые могут оказать влияние на бизнес и население с тем, чтобы обеспечить управление киберрисками с их стороны
  - разработка и принятие стандартов кибербезопасности и защиты компаний и граждан

Контактная информация

Ершова Татьяна Викторовна

Директор Национального центра цифровой экономики
МГУ имени М.В. Ломоносова

Главный редактор научно-аналитического журнала «Информационное общество»

tatiana.ershova@digital.msu.ru

https://digital.msu.ru/
http://www.infosoc.iis.ru/