VI Международная научно-практическая конференция "Право в цифровую эпоху“
НИУ ВШЭ, 24-25 октября 2016 г.

International Laboratory for IT & IP Law

ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ РЕАЛИЗАЦИИ КОНЦЕПЦИИ УПРАВЛЕНИЯ РИСКАМИ ЦИФРОВОЙ БЕЗОПАСНОСТИ В РОССИЙСКОМ ЗАКОНОДАТЕЛЬСТВЕ

Ефремов Алексей Александрович

*к.ю.н, доцент Воронежского государственного университета,
член Экспертного совета Института развития Интернета*

Ключевые вопросы

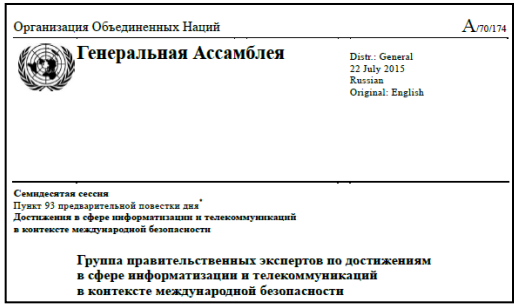
- Зачем нам Рекомендация ОЭСР ? (актуальность)
- Традиционный подход – концепция международной информационной безопасности
- Управление рисками цифровой безопасности – в чем отличия?
- Проблемы реализации в российском законодательстве
- «Мы не одни такие» - вызовы для ЕС
- Встретится ли «Запад» и «Восток»? – потенциал гармонизации концепций и Цифровая декларация ЕАЭС

Зачем нам Рекомендация ОЭСР?

- Общемировой тренд цифровизации (диджитализации) – цифровой трансформации традиционных отраслей экономики
- Формирование и развитие конкурирующих концепций информационной (цифровой) безопасности в документах международных организаций
- Работа ЕЭК по формированию Единого цифрового пространства ЕАЭС
- Ориентация на документы и подходы ОЭСР в Договоре о ЕАЭС 2014 г., а также партнеров РФ по ЕАЭС (Армения, Казахстан)
- Ориентация на документы ОЭСР документов стратегического планирования РФ и реализация Плана законодательной работы по приведению российской нормативно-правовой базы в соответствие с нормами ОЭСР

Концепция международной информационной безопасности

- Отражена в Докладе Группы правительственных экспертов ООН 2015 г., документах ШОС, ОДКБ, соглашениях РФ с Кубой 2014 г., Китаем 2015 г.
- Мультилатеризм (multi-lateral) – многостороннее регулирование государствами
- Принцип суверенитета государств над ИКТ-инфраструктурой на их территории
- Защита от угроз информационной безопасности


Организация Объединенных Наций A/70/174

Генеральная Ассамблея

Distr.: General
22 July 2015
Russian
Original: English

Семидесятая сессия
Пункт 93 предварительной повестки дня
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Управление рисками цифровой безопасности

- Рекомендация ОЭСР по управлению рисками цифровой безопасности для экономического и социального процветания 17.09.2015 (Digital security risk management for economic and social prosperity. C (2015) 115)
- Канкунская Декларация ОЭСР о цифровой экономике 2016 г.
- Принцип суверенного равенства или суверенитета государств не упоминается
- Вовлечение всех заинтересованных субъектов (all stakeholders) - мультистейкхолдеризм

Управление рисками цифровой безопасности

- Риски цифровой безопасности – это не технические проблемы (угрозы), а экономические риски
- Управление рисками цифровой безопасности - составная часть общего процесса управления рисками и принятия решений в каждой организации
- Новые координационные механизмы правительства с неправительственными заинтересованными субъектами и повышение эффективности государственно-частного сотрудничества на национальном, региональном и международном уровнях

Проблемы реализации в российском законодательстве

- ФЗ «Об информации, …», Доктрина ИБ РФ 2000 г., проект Доктрины ИБ 2016 г. вообще не содержат терминов «риск» и «управление рисками»
- Российская доктрина ИБ ориентирована на технократический подход определения угроз («модели угроз» ФСТЭК/ФСБ)
- Потребуется изменение понятийного аппарата и механизмов обеспечения информационной безопасности на законодательном и стратегическом уровнях
- Потребуется разработка методик оценки рисков вместо существующих моделей угроз информационной безопасности
- С другой стороны, переход на риск-ориентированный контроль (надзор) в сфере ИБ (РКН/ФСТЭК/ФСБ) потребует и «риск-ориентированные» нормы (обязательные требования)

Вызовы для ЕС

enisa European Union Agency for Network and Information Security

- Национальные стратегии кибер-безопасности (National Cyber Security Strategies (NCSSs)
- Приняты с 2011 г. (Великобритания, Румыния, ФРГ, Чехия) по 2016 г. (Словения) – всего 24 страны
- Ориентированы на технократический подход отражения угроз

www.enisa.europa.eu

Встретится ли «Запад» и «Восток»?

- Возможности гармонизации обусловлены:
  - Необходимостью обеспечения информационного (цифрового) суверенитета
  - Расширения применения экономической оценки рисков цифровой безопасности вместо технократической модели угроз информационной безопасности
  - Внедрение механизмов государственно-частного партнерства в обеспечении информационной безопасности
- Цифровая декларация ЕАЭС 27.10.2016
  - Принцип укрепления цифрового суверенитета
  - Обеспечение безопасности граждан, бизнеса и их данных в цифровом пространстве, сохраняя при этом гибкость, необходимую для эффективного использования цифровых процессов, данных и технологий

Благодарю за внимание!
Вопросы?

Ефремов Алексей Александрович

yefremov@law.vsu.ru