RIW 2017

Международно-правовое измерение обеспечения международной информационной безопасности.

Более 75% компаний в мире взламываются каждый год;

К 2020 г. экономические потери могут достигнуть $3 трлн;

90% всех взломов начинается с электронной почты

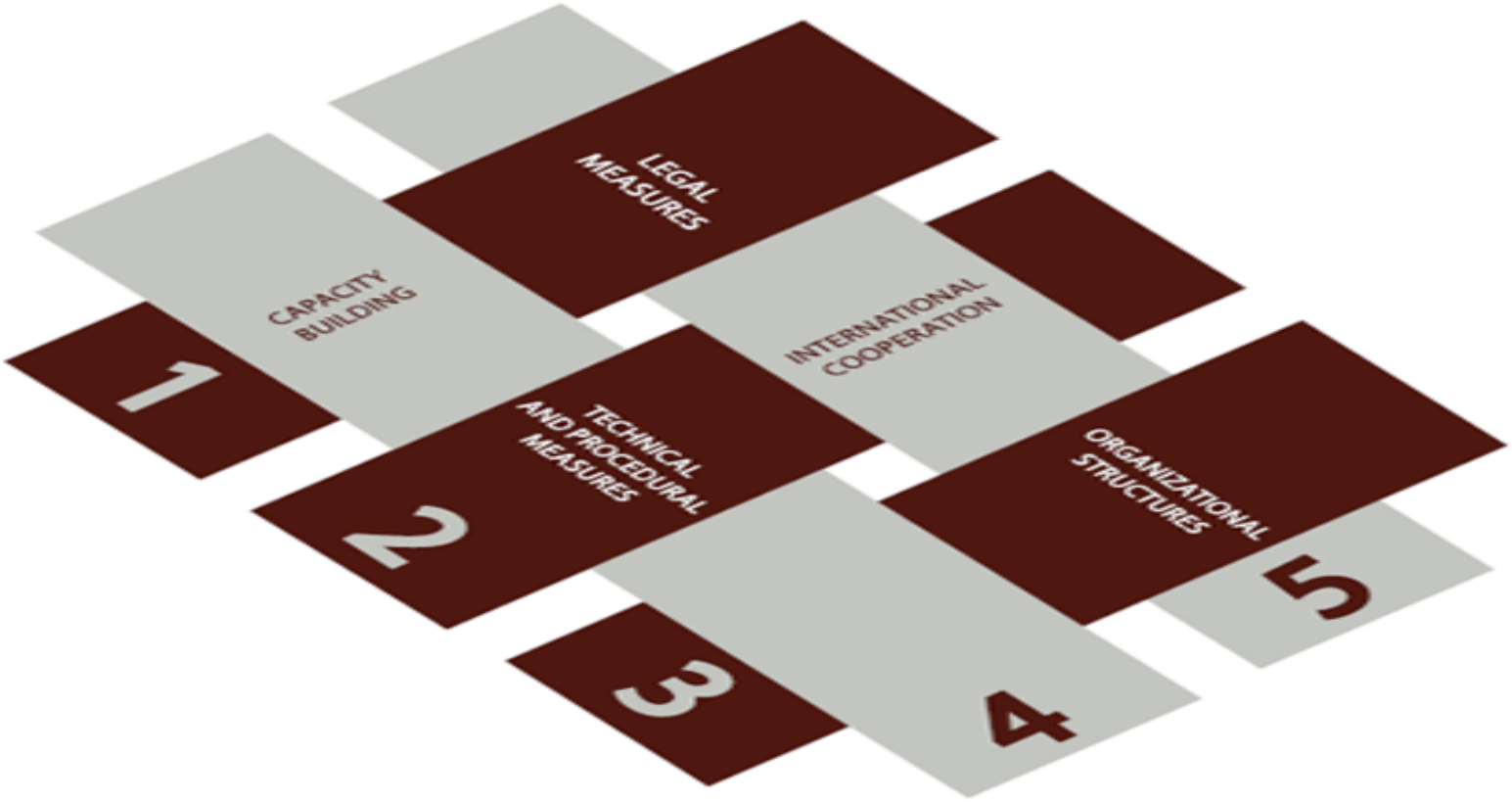
- информационная безопасность
- безопасность информационно-коммуникационных технологий (ИКТ)
- кибербезопасность

Международный союз электросвязи

Актуальная повестка глобальной кибербезопасности
(*ITU Global Cybersecurity Agenda*, *GCA*)

Глобальный индекс безопасности 2017 г.
(*Global Cybersecurity Index*, *GCI*).

A five-part platform



- правовая основа **(*Legal Framework*)**; оценивается исходя из существования соответствующих институциональных структур и нормативно-правовой базы, в сфере кибербезопасностьи и киберпреступностьи;
- технологические мероприятия (***Technical Measures*)** оценивается исходя из существования технических институциональных структур и технической базы связанных с кибербезопасностью;
- организационные структуры (***Organizational Structures***) оценивается на основе координации институциональных структур по политико-стратегическому развитии кибербезопасности на национальном уровне;
- расширение возможностей/наращивание потенциала (***Capacity-Building***) оценивается исходя из наличия программ исследований и разработок, образования и обучения; сертификации специалистов и учреждений государственного сектора, стимулирующие расширение возможностей развития кибербезопасности;
- международное сотрудничество (***International Cooperation*)** оценивается исходя из наличия отношений сотрудничества, включая функционирование совместных структур и сетей обмена информацией.

- «Двустороннее измерение».

Российской Федерацией подписано ряд межправительственных билатеральных международных договоров:

- о сотрудничестве в сфере обеспечения международной информационной безопасности (Белоруссия, Китай, Куба);
- о безопасности информационно-коммуникационных технологий (Малайзия, Индия).

Индия

Основные угрозы в области обеспечения безопасности в сфере ИКТ:

- вредоносное использование информационно-коммуникационных технологий, направленное на подрыв суверенитета, нарушение территориальной целостности государств Сторон и создание угрозы международному миру, правам человека, свободе выражения мнений, безопасности и стратегической стабильности;
- вредоносные атаки на критическую информационную инфраструктуру, которые могут подорвать безопасное и стабильное функционирование глобальных и национальных сетей, в том числе действия, способные нанести экономический вред;
- террористические акты, в том числе пропаганда терроризма и вербовка для осуществления террористической деятельности, совершаемой с использованием информационно-коммуникационных технологий;
- преступные деяния, совершаемые с использованием информационно-коммуникационных технологий;
- распространение информации с использованием информационно-коммуникационных технологий с целью нарушить общественный порядок, общинное и социальное согласие и подорвать осуществление государственного управления;
- угрозы безопасному и стабильному функционированию глобальной и национальной информационной инфраструктуры, имеющие природный и (или) техногенный характер.

Китайская Народная Республика.

Обеспечение международной информационной безопасности:
Перечень основных понятий:

- «информационная безопасность»;
- «информационная инфраструктура»;
- «информационное пространство»
- «информационные ресурсы»;
- «защита информации»;
- **«объекты критической информационной инфраструктуры»;**
- **«компьютерная атака»;**
- «неправомерное использование информационных ресурсов»;
- «несанкционированное вмешательство в информационные ресурсы»;
- «угроза информационной безопасности».

Республика Куба.

Обеспечение международной информационной безопасности

Перечень основных понятий:

- «информационная безопасность»;
- **«информационная война»**
- «информационная инфраструктура»
- **«информационное оружие»**
- «информационное пространство»
- «информационные ресурсы»
- «защита информации»
- **«критически важные объекты»**
- **«международная информационная безопасность»**
- «неправомерное использование информационных ресурсов»
- «несанкционированное вмешательство в информационные ресурсы»
- «угроза информационной безопасности»

Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности 2009 г.

- **Перечень основных понятий**
- **Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков:**

1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.
2. Информационный терроризм.
3. Информационная преступность.
4. Использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других стран.
5. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.
6. Угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Государства – основные субъекты международного права, но интернет не целостный объект регулирования, технологическая инфраструктура интернета: физические объекты коммуникации, серверы, ноутбуки, смартфоны, программное обеспечение и т.д. – преимущественно являются частной собственностью.

DIGITAL GENEVA CONVENTION TO PROTECT CYBERSPACE
(*Fourth Geneva Convention*)

- не атаковать технологические компании, частный сектор, критическую инфраструктуру;
- содействовать усилиям частного сектора по выявлению, реагированию и восстановлению после инцидентов;
- сообщать об уязвимостях поставщикам/разработчикам, а не накапливать, продавать или использовать такие уязвимости;
- сдерживать разработку кибер-оружия, обеспечить меры ограничения его использования и обращения;
- принять меры к нераспространению кибер оружия;
- ограничить наступательные операции, с тем, чтобы избежать массовых инцидентов.

DIGITAL GENEVA CONVENTION TO PROTECT CYBERSPACE
(Fourth Geneva Convention)

Создать международную организацию, подобную Международному Комитету Красного Креста (Женева, Швейцария) с участием субъектов публичного и частного права.

Поддержание «цифрового нейтралитета».

Спасибо за внимание