Санкт-Петербургский государственный университет

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Игнатьева Ольга Анатольевна, к.соц.н.,
доцент кафедры политического управления СПбГУ

Санкт-Петербургский государственный университет

ЦЕЛЬ ИССЛЕДОВАНИЯ

Анализ особенностей и направлений обеспечения информационной безопасности в Российской Федерации.

ИНФОРМАЦИОННЫЕ ВОЙНЫ

Для ведения информационных войн используются:

1.Кибероружие (программный код);

2.Фейки в СМИ и социальных сетях.

N.B! Впервые опробованы в ходе цветных революций в 2000-ые годы.

ТЕХНОГЕННЫЕ УГРОЗЫ

Внешние факторы:

1.Кибератаки на информационную инфраструктуру США могут стать причиной для использования реального вооружения (Дж.Байден).

2.Использование реального вооружения (химического, биологического, ядерного) ведет к экологическим катастрофам.

Внутренние факторы:

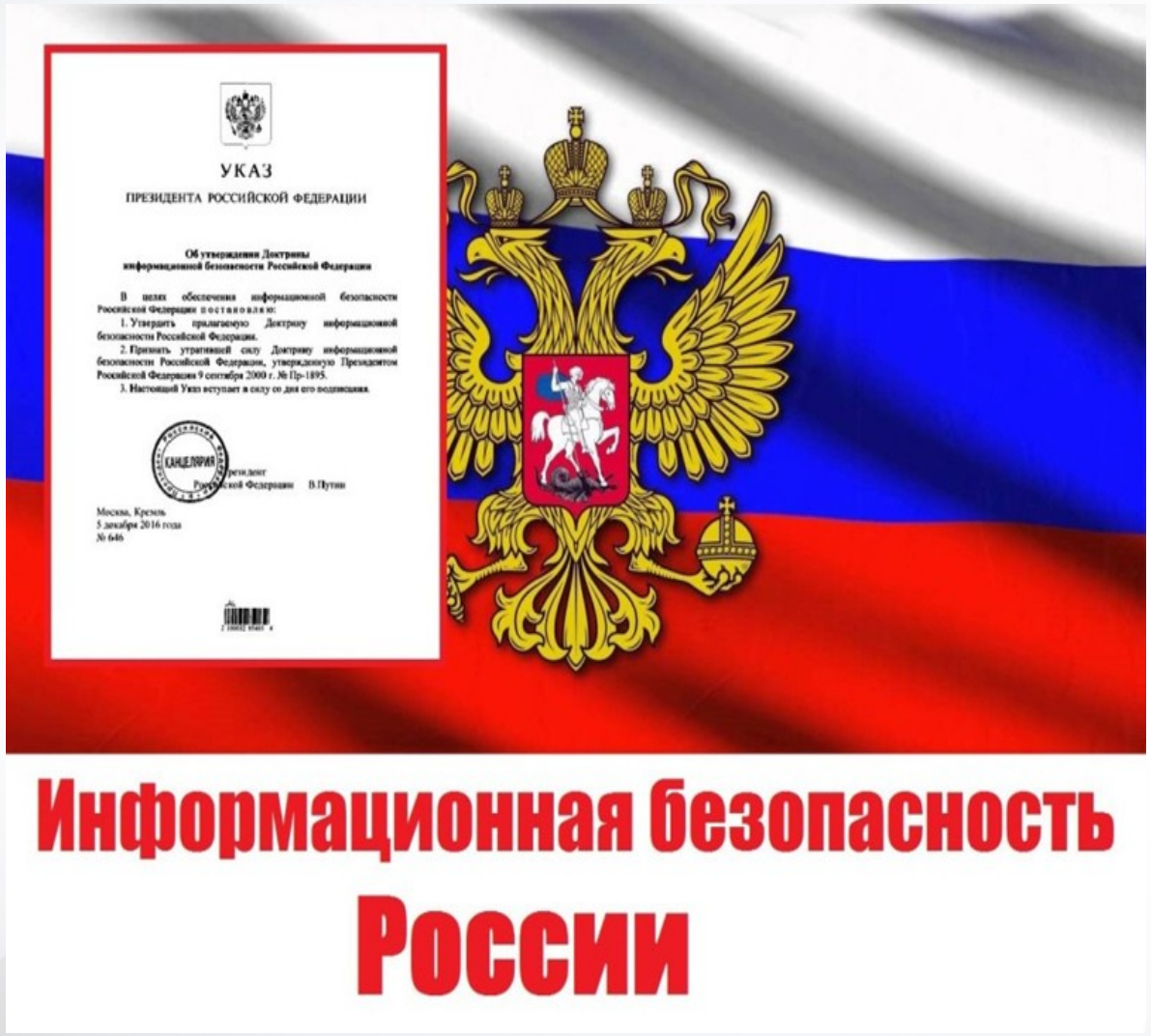
1.Пропагандистские войны ведут к дестабилизации общественно-политической ситуации внутри страны;

2.Протестная активность неуправляемой толпы ставите под угрозу нормальное функционирование промышленных объектов и повышает риск терактов на них.

ДОМИНИРОВАНИЕ ИНТЕРНЕТА

1. Цифровой империализм как новый тип глобальной власти;
2. Фиджитэл реальность поколения Z;
3. Место российских цифровых платформ в рейтинге Ranking Digital Rights (2020)

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ (2016)



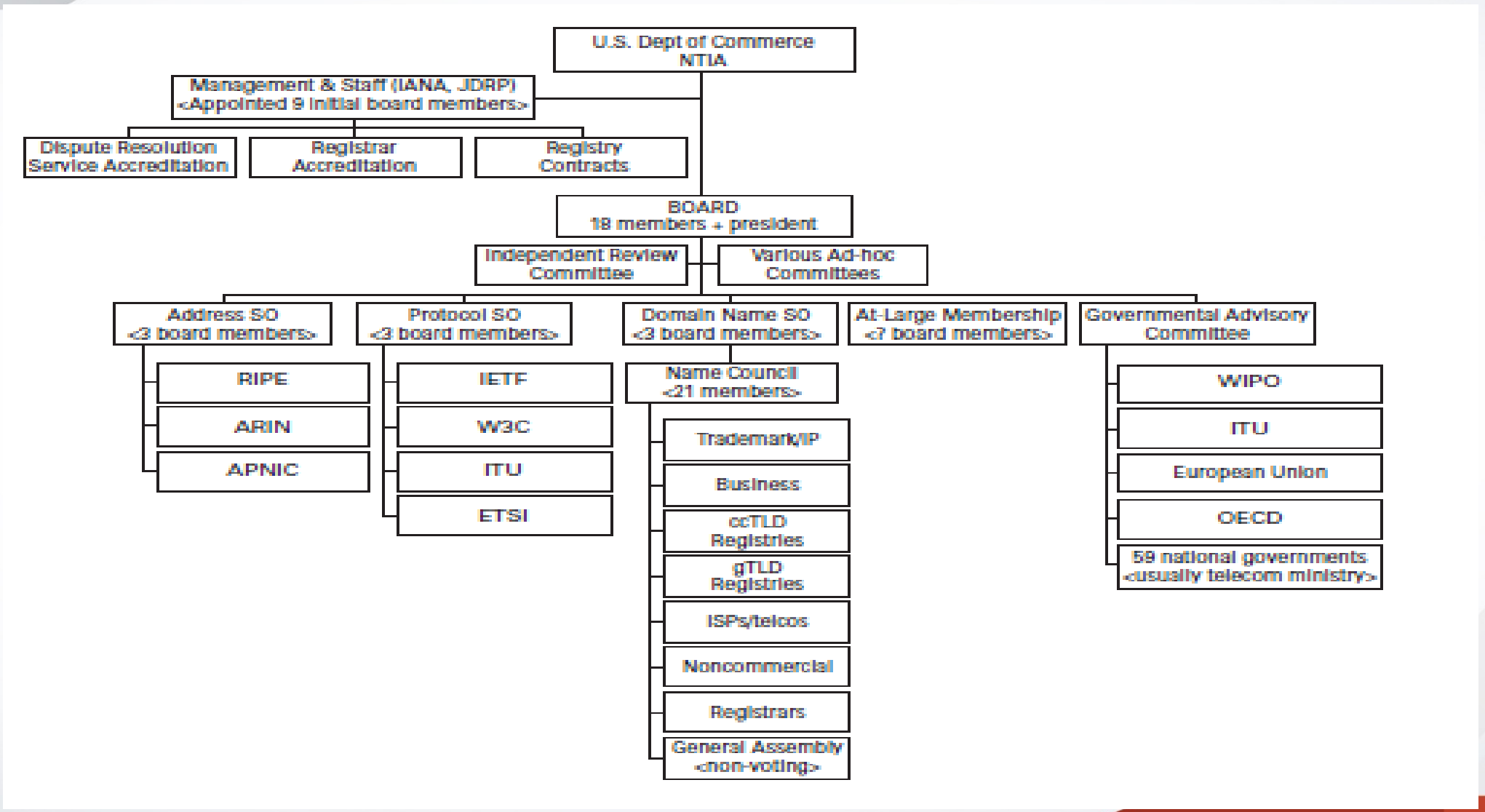
<u>Основные направления обеспечения информационной безопасности:</u>

1.Защита критической инфраструктуры;
2.Защита личных данных;
3.Противодействие кибератакам;
4.Противодействие распространению экстремистских идей;
5.Противодействие идеям, призывающим к самоубийству;
6.Противодействие распространению идей, призывающих к протесту и дестабилизации общества

КИБЕРАТАКИ СО СТОРОНЫ УКРАИНЫ И КОЛЛЕКТИВНОГО ЗАПАДА

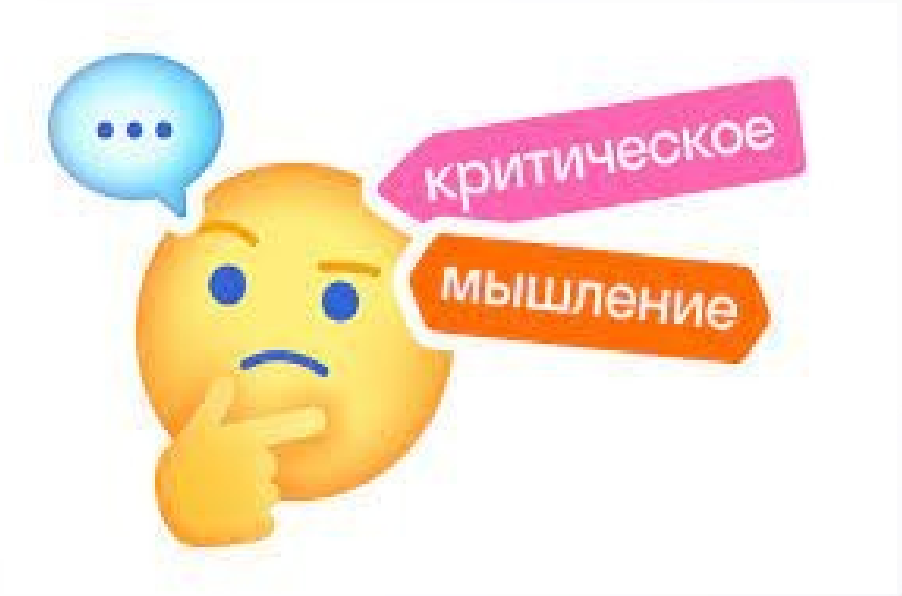
1. Кибератаки на объекты критической инфраструктуры РФ;
2. Призыв Зеленского В.А. к созданию киберлегиона;
3. Кибератака на сайт МЧС путем размещения информации о планирующемся ядерном ударе со стороны РФ.

МЕЖДУНАРОДНЫЙ РЕЖИМ РЕГУЛИРОВАНИЯ ИНТЕРНЕТА
ICANN



ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

1. Необходимо проверить источник информации;
2. Проверить, повторяется ли эта информация в других источниках (особенно в официальных);
3. Поставить перед собой вопрос, с какой целью создан данный материал?
4. Сохранять способность критического и трезвого мышления



СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЦИФРОВЫМ УГРОЗАМ

1. Совершенствование законодательной базы;
2. Диалог в рамках WSIS и на других международных площадках;
3. Привлечение к сотрудничеству передовых специалистов в области информационно-коммуникационных технологий;
4. Контроль контента интернета;
5. Цифровая гигиена

РЕКОМЕНДАЦИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Необходимо создать независимый национальный Интернет по аналогии с КНР.
2. Необходимо развивать собственные социальные сети в существующем глобальном Интернете.
3. Необходимо совершенствовать канал передачи видеоконтента rutube для достижения характеристик youtube.
4. Необходимо объединить усилия национальных государств для изменения режима глобального управления Интернетом.
5. Необходимо способствовать созданию и продвижению цифровых платформ в глобальном Интернете, популяризирующих ценности и культуру русского мира за пределы РФ.
6. Необходимо создать все необходимые условия для наших ведущих IT специалистов для работы в России, в том числе в рамках кибербезопасности.

Контакты

spbu.ru

Игнатьева Ольга Анатольевна, к.соц.н.,
доцент кафедры политического управления СПбГУ
olga7919@mail.ru