Регулирование «критической инфраструктуры», «критической информационной инфраструктуры» в праве зарубежных государств и в Европейском Союзе.

Критическая инфраструктура. Защита и устойчивость Европы

(*Critical Infrastructure. Protection and Resilience Europe*) 9-11 мая 2017 Гаага.

Регулирование в Российской Федерации

«Доктрина информационной безопасности РФ» утверждена Указом №646 2016 г.

- **«информационная инфраструктура РФ» –** совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Регулирование в Российской Федерации

«О безопасности критической информационная инфраструктура РФ» (Проект ФЗ №47571-7)

«критическая информационная инфраструктура РФ» – совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой.

(Использование интернета – основной вопрос регулирования «критической информационной инфраструктуры»)

Понятийно-категориальный аппарат права зарубежных государств и в Европейского Союза.

«Critical», *«Essential»*:

- ключевой;
- критический;
- критически важный;
- жизненно важный.

Понятийно-категориальный аппарат права зарубежных государств и Европейского Союза.

(*Internet*) – интернет как способ и средство оказания и получения различных услуг;

(*Internet Access*) - доступ к интернету.

Интернет обладает «собственной» критической инфраструктурой.

Безопасность и устойчивость критической инфраструктуры (США)

(*Critical Infrastructure Security and Resilience*)
Директива Президента США 12.02.2013)

- Критическая инфраструктура США обеспечивает основные услуги, которые лежат в основе американского общества. Критическая инфраструктура страны разнообразна и сложна и включает в себя распределенные сети, различные организационные структуры и операционные модели, основанные на разных формах собственности (государственная, частная), взаимозависимые функции и системы как в физическом пространстве, так и в киберпространстве, а также структуры управления, обладающие различным уровнем компетенций и обязанностей.

Критическая инфраструктура США

«Критическая инфраструктура» (*critical infrastructure*) – системы и активы, как физические, так и виртуальные, настолько жизненно важные для США, что нарушение функционирования или уничтожение таких систем и активов окажет деструктивное влияние на безопасность, национальную экономическую безопасность, национальное здравоохранение и охрану здоровья, или их любое сочетание.
(Свод законов США 42 U. S. C. 5195c(e))

Критическая инфраструктура США

16 секторов критической инфраструктуры: химический сектор; сектор коммерческой деятельности; связь; коммуникации; сектор важнейших производств; гидроэлектростанции; сектор военно-промышленных баз; аварийно-технических служб; энергетика; финансы; сектор продовольствия и сельского хозяйства; сектор государственных учреждений; медицина и здравоохранение; сектор информационных технологий; сектор ядерных реакторов и ядерных отходов; транспортные системы; сектор водоснабжения, сбора и отведения сточных вод.

Критическая инфраструктура США

Три стратегических императива укрепления безопасности и устойчивости критической инфраструктуры (федеральный уровень):

1)определение функциональных взаимоотношений между федеральным правительством и штатами в целях объединения усилий по укреплению критической инфраструктуры безопасности и устойчивости;

2)обеспечение эффективного обмена информацией путем определения ключевых показателей и системных требований для федерального правительства;

3)внедрение интегративного анализа для планирования и принятия оперативных решений, касающихся критической инфраструктуры.

Критическая инфраструктура США

- владельцы критически важной инфраструктуры (*owners of critical infrastructure*);
- операторы критически важной инфраструктуры (*operators of critical infrastructure*)

Управляют рисками при осуществлении своей деятельности и использовании активов, и определяют эффективность, безопасность и устойчивость стратегий функционирования критической инфраструктуры.

Право Европейского Союза

- Директива Европарламента и Совета ЕС «Об общих мерах высокого уровня безопасности сетевых и информационных систем в рамках Союза»
от 6 июля 2016. «**Директива NIS».**

(*Directive (EU) 2016/1148 of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information systems Security of Network and Information Systems Across the Union*) -

- Директива Европарламента и Совета ЕС о сетевой и информационной безопасности от 18 декабря 2015 г.

«Директива NIS».

Три уровня обеспечения безопасности сетей и информационных систем в рамках ЕС:

- Уровень Союза;
- Национальный уровень;
- Уровень управления рисками и информирования об инцидентах, который возложен на
- **«операторов критически важных услуг»** (*operators of essential services*);
- **«провайдеров цифровых услуг»** (*digital service providers*)

«Директива NIS»

Дата	Вступление в силу + …	Этап реализации
Август 2016 г.	-	Вступление в силу
Февраль 2017 г.	6 месяцев	Формирование задач Группой сотрудничества
Август 2017 г.	12 месяцев	**Введение в действие требований безопасности и отчетности для провайдеров цифровых услуг**
Февраль 2018 г.	18 месяцев	Разработка Группой сотрудничества программы работы
Май 2018	21 месяц	Перенос нормативных положений Директивы в национальное право государств-членов
Ноябрь 2018 г.	27 месяцев	**Государство-члены определяют круг операторов ключевых услуг**
Май 2019 г.	33 месяца (т.е. через год после переноса нормативных положений Директивы в национальное право государств-членов)	**Доклад Комиссии по оценке соответствия определения государствами-членами операторов ключевых услуг**
Май 2021 г.	57 месяцев (т.е. через 3 года после переноса нормативных положений Директивы в национальное право государств-членов)	Комиссия проведет обзор действия Директивы с акцентом на стратегическое и оперативное сотрудничество, а также **на деятельность операторов ключевых услуг и провайдеров цифровых услуг**

«Директива NIS»

фундаментальные различия между

«операторам критически важных услуг» (*operators of essential services*);

«провайдерами цифровых услуг» (*digital service providers*) -

обусловливают различия в правовом регулировании согласно «**Директиве NIS»**

Сети и информационные системы в большинстве являются частными поэтому сотрудничество между государством и частным сектором – важная задача обеспечения безопасности сетей и информационных систем в рамках ЕС

«Директива NIS»

«Оператор критически важных услуг» - частные/государственные организации предоставляющие услуги.

Критерии отнесения организаций к числу **«операторов критически важных услуг»:**

-организация оказывает услуги необходимые для поддержания критически важной общественной и / или экономической деятельности (*critical societal and/or economic activities*);

-оказание таких услуг связано с использованием сетей и информационных систем;

-инциденты могут оказать значительное разрушительное воздействие на предоставление таких услуг (Ст. 5)

«Директива NIS»

Секторы критически важных услуг:

- энергетика;
- транспорт;
- банковская сфера;
- инфраструктура финансовых рынков;
- здравоохранение;
- водоснабжение (обеспечение и распределение);
- цифровая инфраструктура

«Директива NIS»

«Провайдер цифровых услуг»
(*digital service providers*)

-онлайн торговые площадки (*online marketplace*);

-онлайн поисковики (*online search engine*);

-сервисы облачных вычислений (*cloud computing service*)

«Директива NIS»

«Провайдер цифровых услуг»:

- Любое юридическое лицо, предоставляющее «цифровые услуги», если оно предоставляет такие услуги в пределах страны-члена ЕС;
- находится под юрисдикцией страны-члена, где лицо имеет свое головное учреждение (головной офис).

Государства-члены ЕС *не* определяют круг организаций провайдеров цифровых услуг

Директива NIS применяется для всех провайдеров цифровых услуг в рамках определенного сектора

Регулирование в Российской Федерации

«объекты критической информационной инфраструктуры» – информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горно-добывающей промышленности, металлургической промышленности и химической промышленности.

(Проект ФЗ №47571-7).

Право зарубежных государств и Европейского Союза.

Секторы/объекты критической инфраструктуры экономики, управления и отраслей практически совпадают (нормативное закрепление в праве США, ЕС, странах ЕС, Китай, Индия, Япония, Нидерланды и др.).

Разграничены сектор телекоммуникаций и сектор информационных технологий.

Информационные технологии рассматриваются в качестве самостоятельного сектора критической инфраструктуры.

Регулирование в Российской Федерации

- **субъекты критической информационной инфраструктуры** – государственные органы, юридические лица, владеющие на праве собственности или ином законном основании объектами критической информационной инфраструктуры, операторы связи, обеспечивающие взаимодействие объектов критической информационной инфраструктуры между собой.

(Проект ФЗ №47571-7).

Закон КНР «Закон о кибербезоасности»
(*Cyber Security Law*)
1 июня 2017 г.

Понятие **«критической информационной инфраструктуры»** (*critical information infrastructure*) закреплено.

Суверенитет государства – основа регулирования.

Предусмотрена многоуровневая государственная защита (*tiered protection system*) «критической информационной инфраструктуры»

Закон КНР «Закон о кибербезоасности»

Меры обеспечения безопасности **критической информационной инфраструктуры (***Operations Security for Critical Information Infrastructure*) возложены на государство.

Критическая информационная инфраструктура - общественные коммуникации и информационные услуги, управление, трафик, водоснабжение, финансы, общественные услуги, электронное управление и иная критическая информационная инфраструктура, которая в случае ее уничтожения, нарушения функциональности или потери данных может действительно угрожать национальной безопасности, национальному благосостоянию, источникам существования людей или общественным интересам.

Закон КНР «Закон о кибербезоасности»

«Операторы критической информационной инфраструктуры» (*critical information infrastructure operators*) обязаны, в частности:

1) создавать специализированные органы по управлению безопасностью и назначать лиц, ответственных за управление безопасностью;
2) периодически проводить обучение по безопасности сетей для сотрудников;
3) 3) осуществлять резервное копирование для аварийного восстановления систем имеющих важное значение и баз данных;
4) 4) разрабатывать планы реагирования на чрезвычайные ситуации для инцидентов сетевой безопасности и периодически организовывать тренировки

Закон КНР «Закон о кибербезоасности»

Операторы критической информационной инфраструктуры, покупающие сетевые продукты и услуги, которые могут повлиять на национальную безопасность, обязаны проходить проверку безопасности, организованную соответствующими государственными органами департаментами Государственного Совета КНР.

Закон КНР «Закон о кибербезоасности»

Операторы критической информационной инфраструктуры один раз в год должны провести проверку и оценку безопасности своих сетей и рисков, и представить отчет о сетевой безопасности, результатах проверки, а также о мерах по усилению безопасности.

Закон КНР «Закон о кибербезоасности»

«Сетевые операторы» (*Network operators*) собственники сетей, администраторы и поставщики сетевых услуг.

Обязаны защищать свои сети от сбоев, повреждений или несанкционированного доступа и предотвращать утечки данных, кражи или подделки. Деятельность «сетевых операторов» регулируется в зависимости от их классификации в рамках многоуровневой системы защиты сетей.

Закон КНР «Закон о кибербезоасности»

Поставщики сетевых продуктов и услуг (*providers of network products and services*) обязаны обеспечить :

- соответствие китайским «национальным стандартам»;
- безопасность продукции.

Продукты и услуги, относящиеся к **«критическому сетевому оборудованию и продукции сетевой безопасности»** (*Critical Network Equipment and Network Security Products*) должны предварительно пройти тестирование аккредитованными центрами.

«Закон об информационных технологиях» Индии (*Information Technology Act 2008*)

«Критическая информационная инфраструктура» (*Critical Information Infrastructure*) компьютерные ресурсы выведение из строя или разрушение которых окажет катастрофическое влияние на национальную безопасность, экономику и социальное благосостояние нации (ст.70).

«Закон об информационных технологиях»

Секторы критической информационной инфраструктуры: энергетика, банки и финансы, телекоммуникации, транспорт (воздушный, наземный, водный, железнодорожный), космос, оборона, правоприменительная деятельность, безопасность и разведка, государственные стратегические организации, здравоохранение, водоснабжение, предприятия стратегической сферы производства, электронная организация управления (E-Governance)

«Закон об информационных технологиях»

Разграничены сектор телекоммуникаций и сектор информационных технологий. Информационные технологии рассматриваются в качестве самостоятельного критического инфраструктурного сектора.

«Доступ в интернет» относится к критической инфраструктуре наряду с информационными технологиями.

«Закон об информационных технологиях»

Индийский Национальный центр защиты критической информационной инфраструктуры (*National Critical Information Infrastructure Protection Centre, NCIIPC*) - «Центр NCIIPC»

Создан в 2014 г. в соответствии с Законом об информационных технологиях.

«Центр NCIIPC»

Миссия «Центра NCIIPC»: принятие всех необходимых мер для содействия защите критической информационной инфраструктуры, от несанкционированного доступа, воздействия , использования, обнародования, разрушения, нарушения функциональности через согласованную координацию, синергию и повышение защищенности безопасности информации на основе согласованной координации, взаимодействия и повышения информационности всех заинтересованных сторон.

Функции «Центра NCIIPC»

- Осуществление деятельности в качестве государственной головной организации, ответственной за все меры по защите критической информационной инфраструктуры страны;
- Разработка рекомендаций, направленных на снижение уязвимости критической информационной инфраструктуры от кибертерроризма, кибервойны и других угроз;
- Выявление всех критических элементов информационной инфраструктуры;
- Стратегическое обеспечение деятельности Правительства по реагированию на кибер-угрозы безопасности в отношении выявленных критической информационной инфраструктуры;
- Координация, обмен данными, мониторинг, сбор, анализ и прогноз угроз на национальном уровне по критической информационной инфраструктуре для раннего предупреждения и оповещения;
- Помощь в разработке соответствующих планов, разработка стандартов, обмен передовым опытом и совершенствование закупок, связанных с защитой критической информационной инфраструктуры;

Функции «Центра NCIIPC»

(продолжение)

- Разработка стратегии защиты, политик, оценок уязвимостей и аудита, методология и планы по их распространению и внедрению для защиты критической информационной инфраструктуры;
- Проведение научных исследований и развития и смежных видов деятельности для защиты критической информационной инфраструктуры;
- Разработка и организация программ обучения и информирования, развитие аудита и органов по сертификации для защиты критической информационной инфраструктуры;
- Разработка и реализация национальных и международных стратегий сотрудничества в целях защиты критической информационной инфраструктуры;
- Разработка рекомендаций в области защиты критической информационной инфраструктуры, предупреждения и ликвидации последствий по согласованию с заинтересованными сторонами и тесной координацией с группой реагирования на чрезвычайные ситуации (CERT - Indian Computer Emergency Response Team);
- Обмен информацией с группой реагирования на чрезвычайные ситуации (CERT) и др.

СПАСИБО ЗА ВНИМАНИЕ, ГОСПОДА!

М.Касенова, 2017