Безопасность критической информационной инфраструктуры РФ

Что такое критическая информационная инфраструктура?

Понятие «критическая информационная инфраструктура» закреплено в «Стратегии развития информационного общества РФ на 2017 – 2030 годы» (утв. Указом Президента РФ от 09 мая 2017 г. № 203) и в Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Критическая информационная инфраструктура Российской Федерации (далее – критическая информационная инфраструктура, КИИ) – совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой.

Объекты КИИ – информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Субъекты КИИ – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Таким образом, все информационные системы и информационно-телекоммуникационные сети, функционирующие в организациях и на предприятиях большинства значимых отраслей промышленности, а также в государственных органах, относятся к критической информационной инфраструктуре и подлежат защите.

Для обеспечения безопасности КИИ в России создается особый режим.

В создании и развитии единой государственной системы обеспечения безопасности КИИ в РФ задействованы следующие участники:

- Президент Российской Федерации;
- Правительство Российской Федерации;
- Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации – назначается Указом Президента Российской Федерации;
- Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – в соответствии с Указом Президента Российской Федерации от 15 января 2013 г. № 31с г. Москва «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» назначена ФСБ России;
- Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи (Минкомсвязь России).

Каким образом обеспечивается безопасность КИИ?

Безопасность КИИ обеспечивается за счёт выполнения следующих мероприятий:

1. Категорирование объектов КИИ, которое осуществляется исходя из социальной, политической, экономической, экологической значимости, а также значимости объекта КИИ для обеспечения обороноспособности, безопасности государства и правопорядка. Закон определяет три категории значимости: первую, вторую и третью. Значимость может вообще не присваиваться. Критерии значимости объектов КИИ устанавливаются Правительством РФ;
2. Информирование уполномоченных органов о выполнении мероприятий по обеспечению безопасности КИИ;
3. Подключение к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (Национальному координационному центру по компьютерным инцидентам) с целью передачи сведений обо всех компьютерных инцидентах, возникающих на объектах КИИ и получения информации;
4. Разработка и осуществление мероприятий по обеспечению безопасности значимого объекта КИИ. Субъект создает Систему безопасности значимого объекта КИИ. Требования определяет орган, уполномоченный в области обеспечения безопасности КИИ.

Каков международный опыт обеспечения безопасности КИИ?

В Соединенных Штатах Америки критическая инфраструктура характеризуется как инфраструктура, обеспечивающая основополагающие сервисы для американского общества, определяющие экономику, безопасность и здоровье страны. Государственным органом, уполномоченным в области безопасности критической информационной инфраструктуры США, является Department of Homeland Security. Вопросы безопасности критической инфраструктуры регулируются президентской директивой PPD-21, принятой 12 февраля 2013 года.

В рамках критической инфраструктуры США выделяется 16 секторов:

- Сектор химической промышленности (Chemical Sector);
- Сектор коммерческих предприятий (Commercial Facilities Sector);
- Сектор связи (Communications Sector);
- Сектор критического производства (Critical Manufacturing Sector);
- Сектор плотин (Dams Sector);
- Сектор оборонной промышленности (Defense Industrial Base Sector);
- Сектор помощи в чрезвычайных ситуациях (Emergency Services Sector);
- Энергетический сектор (Energy Sector);
- Сектор финансовых сервисов (Financial Services Sector);
- Сектор пищевой и агро- промышленности (Financial Services Sector);
- Сектор государственных предприятий (Financial Services Sector);
- Сектор здравоохранения (Healthcare and Public Health Sector);
- Сектор информационных технологий (Information Technology Sector);
- Сектор ядерных реакторов, материалов и отходов (Nuclear Reactors, Materials, and Waste Sector);
- Сектор транспортных систем (Transportation Systems Sector);
- Сектор водоснабжения и канализации (Water and Wastewater Systems Sector).

Для каждого сектора назначен свой орган, отвечающий за формирование специфических требований и мероприятий.

В Евросоюзе работа по безопасности критической инфраструктуры действует программа по защите критических инфраструктур (European Programme for Critical Infrastructure Protection, EPCIP), в рамках которой создана сеть по обмену информацией об инцидентах и предупреждениях, касающихся критической инфраструктуры (Critical Infrastructure Warning Information Network, CIWIN), сеть информации по защите критической инфраструктуры (European Reference Network for Critical Infrastructure Protection, ERNCIP). Мероприятия по идентификации объектов ключевой инфраструктуры во исполнение консульской директивы 2008/114/EC от 08 декабря 2008 г. Открытые исследования на тему безопасности КИИ выполняет Агентство Евросоюза по сетевой и информационной безопасности (European Union Agency for Network and Information Security, ENISA), ОБСЕ.

В Китайской Народной Республике 07 ноября 2016 года опубликован Закон о кибербезопасности, в рамках которого безопасности критической информационной инфраструктуры посвящен раздел.

Выводы

Мировые державы развивают законодательную и техническую базу для защиты КИИ как части критической инфраструктуры.

В современных реалиях, когда геополитическое противостояние перемещается в цифровую плоскость, обеспечение безопасности КИИ является необходимостью для защиты государственных интересов.

Следует отметить, что на текущий момент законодательная и нормативная база Российской Федерации находится в стадии развития и наполнения. Критике подвергается вводимый ею и используемый понятийный аппарат. Основная содержательная часть мероприятий по обеспечению безопасности КИИ ещё не выпущена в виде готовых документов.

Залогом адекватного и предсказуемого регулирования порядка обеспечения безопасности КИИ является широкое обсуждение как понятийной, так и содержательной часть законодательных требований в рамках экспертных сообществ, и при этом требуется учитывать существующий мировой опыт. Данный меры будут способствовать выстраиванию эффективной и управляемой системы обеспечения безопасности КИИ в Российской Федерации.

безопасность критической информационной инфраструктуры, аналитика

From:
http://sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://sps-ib.ru/analitika:bezopasnost_kii

Last update: **2017/08/14 16:27**