Лекция 7. Правовое обеспечение безопасности использования информационной инфраструктуры

дтн, дюн, проф.
Стрельцов Анатолий Александрович

Института проблем информационной безопасности
МГУ им. М.В.Ломоносова

Основные вопросы

- 1. Национальная информационная инфраструктура
- 2. Угрозы безопасности функционирования и использования национальной информационной инфраструктуры
- 3. Правовые средства обеспечения безопасности национальной информационной инфраструктуры

1. Национальная информационная инфраструктура

- Информационная инфраструктура — система технических средств и организационных структур, обеспечивающих возможность выполнения задач обработки и передачи информации
- Техническую основу информационной инфраструктуры общества составляет совокупность сетей связи, а также средств создания, хранения и обработки информации, объединенных в компьютерные и коммуникационные сети.

Составляющие информационной инфраструктуры

- сети связи,
- средства доступа к информационным системам, сетям связи и услугам сети Интернет по поиску, обработке, хранению и представлению информации потребителям;
- информационные системы;
- организации, занимающиеся созданием и развитием и эксплуатацией сетей связи, средств доступа и информационных систем.

Единая сеть электросвязи России

- ЕСЭ состоит из расположенных на территории РФ сетей электросвязи следующих категорий:
- сеть связи общего пользования;
- выделенные сети связи;
- технологические сети связи, присоединенные к сети связи общего пользования;
- сети связи специального назначения и другие сети связи для передачи информации при помощи электромагнитных систем
- 126-ФЗ «О связи»

Сеть связи общего пользования

- **Сеть связи общего пользования** предназначена для возмездного оказания услуг электросвязи любому пользователю услугами связи на территории РФ и включает в себя сети электросвязи, определяемые географически в пределах обслуживаемой территории и ресурса нумерации и неопределяемые географически в пределах территории РФ и ресурса нумерации, а также сети связи, определяемые по технологии реализации оказания услуг связи.
- Сеть связи общего пользования представляет собой комплекс взаимодействующих сетей электросвязи, в том числе сети связи для трансляции телеканалов и (или) радиоканалов

Выделенные сети связи

- **Выделенными сетями связи** являются сети электросвязи, предназначенные для возмездного оказания услуг электросвязи ограниченному кругу пользователей или группам таких пользователей. Выделенные сети связи могут взаимодействовать между собой. Выделенные сети связи не имеют присоединения к сети связи общего пользования, а также к сетям связи общего пользования иностранных государств.

Технологические сети связи

- *Технологические сети связи* предназначены для обеспечения производственной деятельности организаций, управления технологическими процессами в производстве.
- Технологии и средства связи, применяемые для создания технологических сетей связи, а также принципы их построения устанавливаются собственниками или иными владельцами этих сетей.

Сети связи специального назначения

- Сети связи специального назначения предназначены для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка. Эти сети не могут использоваться для возмездного оказания услуг связи, если иное не предусмотрено законодательством Российской Федерации.

Сеть Интернет

- **Сеть Интернет** может рассматриваться как многоаспектная система, включающая несколько уровней коммуникационной инфраструктуры: национальный и межнациональный; межрегиональный и межконтинентальный, каждый из которых функционирует на основе унифицированных протоколов взаимодействия устройств сети Интернет и в едином адресном пространстве данной сети.
- Интернет является объединением на единых правилах множества коммуникационных сетей, поддерживаемых индивидуальными провайдерами. Развитие сетей провайдеров является необходимым этапом становления любого сегмента глобального Интернета.

Управление и использование сети Интернет

- Провайдеры:
- коммуникационных сетей;
- узлов межсетевого обмена;
- опорных сетей
- национальных, региональных и корпоративных узлов доступа
- информационных и коммуникационных услуг

Объекты критической информационной инфраструктуры

- Критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;
- Объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

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, используемые в наиболее важных составляющих инфраструктуры общества
- российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

2. Угрозы безопасности

- компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

- компьютерный инцидент - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

3. Правовые средства обеспечения безопасности ИИ

- Юридические обязывания в области безопасности сетей связи:
- лицензирование деятельности юридических лиц и индивидуальных предпринимателей по возмездному оказанию услуг связи
- обязательное подтверждение соответствия установленным требованиям средств связи для обеспечения целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации

Тайна связи

- На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Правовые средства обеспечения безопасности КИИ

- дозволения участия в противодействии угрозам безопасности некоторым физическим и юридическим лицам
- Юридические обязывания лиц, участвующих в системе противодействия угрозам
- Запреты злонамеренного и враждебного использования ИКТ против объектов КИИ
- 187-ФЗ «О безопасности критически важной информационной инфраструктуры РФ» от 26.07.2017

Принципы обеспечения безопасности ОКИИ

- законность;
- непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;
- приоритет предотвращения компьютерных атак.

Полномочия Президента Российской Федерации

- Определяет:
- основные направления государственной политики;
- федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной СОПКА;
- порядок создания и задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Правительство Российской Федерации

- Устанавливает:
- показатели критериев значимости объектов критической информационной инфраструктуры и их значения, а также порядок и сроки осуществления их категорирования;
- порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- порядок подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры.

ФО, уполномоченный в области безопасности КИИ

- утверждает порядок ведения реестра значимых объектов критической информационной инфраструктуры и ведет данный реестр;
- утверждает форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости
- устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, а также требования к созданию систем безопасности таких объектов и обеспечению их функционирования
- осуществляет государственный контроль

ФО, уполномоченный в области функционирования СОПКА

- создает национальный координационный центр по компьютерным инцидентам
- координирует деятельность субъектов критической информационной инфраструктуры
- организует и проводит оценку безопасности критической информационной инфраструктуры
- утверждает порядок информирования федерального органа исполнительной властио компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак

Силы обнаружения, предупреждения и ликвидации последствий компьютерных атак

- подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы
- организация для обеспечения координации деятельности субъектов критической информационной инфраструктуры
- подразделения и должностные лица субъектов критической информационной инфраструктуры,

Субъекты критической информационной инфраструктуры имеют право:

- получать информацию, необходимую для обеспечения безопасности принадлежащих им значимых ОКИИ
- получать информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;
- за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак
- разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры обязаны:

- незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной
- оказывать содействие в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;
- обеспечивать выполнение порядка, технических условий установки и эксплуатации средств СОПКА, их сохранность.

Категорирование объектов КИИ

- Категорирование *(первая, вторая, третья категория) осуществляется исходя из:
- социальной значимости, выражающейся в оценке возможного ущерба,
- политической значимости,;
- экономической значимости,
- экологической значимости,
- значимости ОКИИ для обеспечения обороны страны, безопасности государства и правопорядка.

Реестр значимых ОКИИ

- В целях учета значимых объектов критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, ведет реестр значимых объектов критической информационной инфраструктуры в установленном им порядке.

Система безопасности ОКИИ

- В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создает систему безопасности такого объекта и обеспечивает ее функционирование.

Система обнаружения атак

- Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

- Информационные ресурсы Российской Федерации - информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.

Выводы

- 1. Безопасность функционирования информационной инфраструктуры является важным условием обеспечения безопасности информационной деятельности субъектов информационной сферы, реализации национальных интересов в данной сфере
- 2. Правовое обеспечение информационной безопасности информационной инфраструктуры направлено на противодействие угрозам безопасности сетей связи, национального сегмента сети Интернет, а также объектов инфраструктуры общества и государства, использующих информационную инфраструктуру.

- Спасибо за внимание