Лекция 13. Правовое обеспечение безопасности общества в ИКТ-среде

дтн, дюн, проф.
Стрельцов Анатолий Александрович

Основные вопросы лекции

- 1. Общество и общественная безопасность
- 2. Угрозы общественной безопасности в ИКТ-среде
- 3. Правовые механизмы обеспечения общественной безопасности в ИКТ-среде

1. Понятие «Общество»

- Население страны, ее граждане, рассматриваемые в совокупности с их историей, интересами, потребностями, желаниями, убеждениями, поведением, психологией
- Общность людей, наделенных волей и сознанием, проживающих на определенной территории, обладающая определенной степенью экономического и духовного единства и целостностью организации жизни
- Особая система, и самостоятельный социальный организм, действующий на данной территории и охватывающий все население

Основные интересы общества в ИКТ-среде

- Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
- Создание и использование ИКТ-среды – действия, направленные на создание информационно-коммуникационных технологий, сетей связи, информационных систем, сайтов сети Интернет, локальных вычислительных систем и иных средств и систем поиска, обработки, передачи, хранения и распространения информации

Обеспечение общественной безопасности

- Реализация определяемой государством системы политических, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие преступным и иным противоправным посягательствам, а также на предупреждение, ликвидацию и (или) минимизацию последствий чрезвычайных ситуаций природного и техногенного характера

Правовое обеспечение общественной безопасности

- Система правовых принципов и норм, регулирующих отношения в области противодействия угрозам общественной безопасности

2. Основные угрозы безопасности общества в ИКТ-среде

- 1. Угроза экстремистской деятельности
- Экстремистская деятельность – насильственное изменение основ конституционного строя и нарушение целостности РФ; публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности человека по признаку национальной принадлежности; воспрепятствование законной деятельности государственных органов, общественных и религиозных объединений, соединенное с насилием

Основные угрозы безопасности общества в ИКТ-среде

- 2. Угроза террористической деятельности
- Терроризм - идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий:
- Информационное воздействие на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, пропаганды терроризма
- Информационные деструктивные воздействия на объекты критической информационной инфраструктуры.

3. Правовое обеспечение безопасности общества в ИКТ-среде

- Основные источники права:
- № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»
- №114-ФЗ от 25.07.2002 «О противодействии экстремистской деятельности»
- № 35-ФЗ от 6.03.2006 «О противодействии терроризму»
- Закон РФ от 27.12.1991 № 2124-1 «О средствах массовой информации»
- Уголовный кодекс РФ1
- Уголовно-процессуальный кодекс РФ

3.1. Правовое противодействие экстремизму в ИКТ-среде

- Принципы:
- признание, соблюдение, и защита прав и свобод человека и гражданина
- законность
- приоритет обеспечения безопасности РФ
- приоритет мер предупреждения
- сотрудничество государства с общественными и религиозными объединениями
- неотвратимость наказания

Правовое обеспечение противодействия экстремистской деятельности

- Правовые средства:
- Запрет распространения информации экстремистского характера
- Позитивные обязывания субъектов, осуществляющих деятельность по распространению информации в ИКТ-среде
- Предостережение о недопустимости осуществления экстремистской деятельности
- Юридическая ответственность за нарушение запрета и невыполнение обязываний

Запреты распространения определенных видов информации

- №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»
- Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность

Позитивные обязывания (№149-ФЗ от 27.07.2006)

- **Организатор распространения информации в сети "Интернет"** обязан: обеспечивать реализацию требований к оборудованию, используемому для осуществления ОСМ; при использовании кодирования ЭС представлять в ФОИВ в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

- **Владелец сайта и (или) страницы сайта в сети "Интернет» (блогер) обязан** не допускать использование сайта или страницы сайта в сети "Интернет" в целях распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов.

- Владелец программы для ЭВМ, владелец сайта и (или) страницы сайта в сети "Интернет", которые используются для обработки и распространения новостной информации в сети "Интернет" (новостной агрегатор), обязан не допускать их использование в целях распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов,

Предостережение о недопустимости осуществления экстремистской деятельности

- № 114-ФЗ от 25.07.2002 «О противодействии экстремистской деятельности»
- Общественному или религиозному объединению либо иной организации в случае выявления фактов, свидетельствующих о наличии в их деятельности, признаков экстремизма, выносится предупреждение в письменной форме о недопустимости такой деятельности с указанием конкретных оснований вынесения предупреждения, в том числе допущенных нарушений. В случае, если возможно принять меры по устранению допущенных нарушений, в предупреждении также устанавливается срок для устранения указанных нарушений, составляющий не менее двух месяцев со дня вынесения предупреждения.
- Предупреждение общественному или религиозному объединению либо иной организации выносится Генеральным прокурором Российской Федерации или подчиненным ему соответствующим прокурором, либо федеральным органом исполнительной власти, осуществляющим функции в сфере государственной регистрации некоммерческих организаций, общественных объединений и религиозных организаций.

Юридическая ответственность

- №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»
- Злоупотребление блогером правом на распространение общедоступной информации, выразившееся в нарушении требований законодательства, влечет за собой уголовную, административную или иную ответственность в соответствии с законодательством Российской Федерации.
- Нарушение владельцем новостного агрегатора требований законодательства влечет за собой уголовную, административную или иную ответственность в соответствии с законодательством Российской Федерации.

3.2. Правовое обеспечение противодействия терроризму в ИКТ-среде

- Правовую основу противодействия терроризму составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные законы, нормативные правовые акты Президента Российской Федерации, нормативные правовые акты Правительства Российской Федерации, а также принимаемые в соответствии с ними нормативные правовые акты других федеральных органов государственной власти.

Позитивное обязывание

- Обладатель информации, оператор информационной системы обязаны обеспечить:
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации; своевременное обнаружение фактов несанкционированного доступа;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, нарушающего их функционирование; возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- нахождение на территории РФ баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ

Позитивные обязывания

- Физические лица, осуществляющие предпринимательскую деятельность без образования юридического лица либо использующие принадлежащее им имущество в социальных, благотворительных, культурных, образовательных или иных общественно полезных целях, не связанных с извлечением прибыли,

- выполняют требования к антитеррористической защищенности объектов (территорий), используемых для осуществления указанных видов деятельности и находящихся в их собственности или принадлежащих им на ином законном основании.

- Юридические лица обеспечивают выполнение указанных требований в отношении объектов, находящихся в их собственности или принадлежащих им на ином законном основании.

Позитивные обязывания

- Владелец сайта и (или) страницы сайта в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет" (далее - блогер), при размещении и использовании указанной информации, в том числе при размещении указанной информации на данных сайте или странице сайта иными пользователями сети "Интернет", обязан

- не допускать использование сайта или страницы сайта в сети "Интернет" в целях совершения уголовно наказуемых деяний, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов

Надзор

- В случае обнаружения на новостном агрегаторе фактов фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений, а также распространения новостной информации с нарушением законодательства РФ
- уполномоченные государственные органы вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, посредством заполнения электронной формы на официальном сайте данного органа с приложением решения суда или решения указанного государственного органа с требованием принять меры по прекращению распространения такой информации.
-

Организация противодействия терроризму

- В целях обеспечения координации деятельности территориальных органов федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления по профилактике терроризма, а также по минимизации и ликвидации последствий его проявлений по решению Президента РФ могут формироваться специальные органы.

- Для реализации решений указанных органов могут издаваться акты. Решения указанных органов, принятые в пределах их компетенции, обязательны для исполнения органами государственной власти субъектов РФ, органами местного самоуправления, организациями, должностными лицами и гражданами в соответствующем субъекте РФ.

- Неисполнение или нарушение указанных решений влечет ответственность, предусмотренную федеральными законами или законами субъектов Российской Федерации.

Правовой режим контртеррористической операции

- На территории (объектах), в пределах которой (на которых) введен правовой режим контртеррористической операции, в порядке, предусмотренном законодательством РФ, на период проведения контртеррористической операции допускается применение следующих мер и временных ограничений:

- ведение контроля телефонных переговоров и иной информации, передаваемой по каналам телекоммуникационных систем, а также осуществление поиска на каналах электрической связи и в почтовых отправлениях в целях выявления информации об обстоятельствах совершения террористического акта, о лицах, его подготовивших и совершивших, и в целях предупреждения совершения других террористических актов;

- приостановление оказания услуг связи юридическим и физическим лицам или ограничение использования сетей связи и средств связи;

Запрет злоупотребления свободой массовой информации

- Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань.

Запрет в области распространения информации о контртеррористической операции

- При освещении контртеррористической операции запрещается
- распространение в средствах массовой информации сведений о специальных средствах, технических приемах и тактике проведения такой операции, если их распространение может препятствовать проведению контртеррористической операции или поставить под угрозу жизнь и здоровье людей.

Реализация запрета в ИКТ-среде

- Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено
- В целях ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено".

Техническое регулирование

- Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

3.3. Преступления в сфере компьютерной информации

- Основной источник права:
- Уголовный кодекс Российской Федерации.
- Уголовно-процессуальный кодекс Российской Федерации
- Основное правовое средство – запрет.

Статья 272. Неправомерный доступ к компьютерной информации

- Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, — наказывается штрафом в размере до двухсот тысяч рублей;
- То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, — наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей;
- Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой — наказываются штрафом в размере до пятисот тысяч рублей.
-

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

- Создание, распространение или использование компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, —

- наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Статья 274. Нарушение правил эксплуатации средств передачи компьютерной информации и информационно-телекоммуникационных сетей

- Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо ИКС и оконечного оборудования, а также правил доступа к ИКС, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб,

- — наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет.