

МЕЖДУНАРОДНЫЕ МЕХАНИЗМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Вопросы противодействия использованию информационных технологий в преступных целях содержатся в таких международных документах, как Окинавская хартия Глобального информационного общества, подписанная главами «восьмерки» от 22 июля 2000 г., Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г., Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г., Декларация принципов построения информационного общества, принятая на Всемирной встрече на высшем уровне в Женеве в декабре 2003 г. и др.

Конвенция Совета Европы о киберпреступности, о борьбе с преступлениями в сфере компьютерной информации, подписанная рядом государств Европейского Союза 23 ноября 2001 г., направлена на повышение эффективности уголовных расследований и процессуальных действий в отношении уголовных преступлений, связанных с компьютерными системами и компьютерными данными. Конвенция вступила в силу 1 июля 2004 г.

В настоящее время Конвенцию подписали более 30 государств, но менее половины из них ее ратифицировало. Следует отметить, что ряд государств, таких как Болгария, Венгрия, Дания, Литва, Румыния, Эстония и др., при ратификации Конвенции приняли оговорки относительно целого ряда статей Конвенции.

Кроме того, 28 января 2003 г. 25 государств подписали Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем. В настоящее время документ ратифицирован Албанией, Данией (с оговорками, связанными с распространением расистских и ксенофобских материалов посредством компьютерных систем (статья 3); расистским и ксенофобским мотивированным оскорблением (статья 5); отрицанием, чрезвычайной минимизацией, одобрением или оправданием геноцида или преступлений против человечества (статья 6); территориальным применением (статья 14)) и Кипром.

В Декларации принципов информационного общества, утвержденной на первом Всемирном саммите, прошедшем в Женеве 10 декабря 2003 г. на

высшем уровне, одним из основополагающих принципов информационного общества определен, как уже отмечалось, принцип укрепления доверия и безопасности при использовании информационно-коммуникационных технологий. Речь идет о формировании, развитии и внедрении глобальной культуры кибербезопасности. Указанные процессы должны основываться на международном сотрудничестве заинтересованных сторон и компетентных международных организаций, а также на уровне социально-экономического развития каждого государства, связанном с ориентацией на развитие аспектов информационного общества.

В октябре 2003 года была принята Резолюция Совета Европы № 1 «О борьбе с терроризмом», принятой на 25-й Конференции европейских министров юстиции в Софии. Комитету министров Совета Европы было рекомендовано приступить к рассмотрению возможности создания европейского регистра национальных и международных правовых актов, начав в качестве приоритетной задачи с правовых актов в области борьбы с терроризмом.

Идея создания Общеввропейского регистра нашла отражение также в Рекомендации ПАСЕ 1677 (2004) от 6 октября 2004 г. Комитета Министров Совета Европы о начале подготовительной работы по составлению общеввропейского регистра национальных и международных нормативных актов, связанной с необходимостью обеспечения создания системы компьютеризированного доступа к нормативным актам государств-членов Совета Европы и других европейских организаций и обменом правовой информацией.

Отрицательное влияние пробелов и различий в законодательстве об обеспечении информационной безопасности государств – членов Европейского Союза отмечается и в подписанном 24 февраля 2005 г. в Брюсселе Рамочном решении Совета Евросоюза об атаках на информационные системы, в котором особенно подчеркнута необходимость защиты информационных систем и банков данных от преступных посягательств террористических групп и иных преступных организаций.

В последнее время в целом ряде государств (Бельгии, Дании, США и др.) национальное законодательство дополнено нормами, направленными на ограничение распространения незапрашиваемых электронных сообщений или запрет этой деятельности.

Вопросы борьбы со «спамом» нашли отражение и в Декларации принципов построения информационного общества. «Спам» представляет для пользователей, сетей и в целом для Интернета серьезную проблему, масштабы которой, как указывается в Декларации, к сожалению, возрастают. Среди разновидностей хакерских атак быстро набирают

популярность так называемые DDoS-атаки, т.е. множество запросов от огромного числа компьютеров со всего мира, зараженных вирусами.

Словосочетание, имеющее аббревиатуру DDoS, на русский язык переводится как «распределенный отказ обслуживания». Цель атаки заключается не в том, чтобы проникнуть в систему, а в том, чтобы парализовать ее работу.

С точки зрения информационной безопасности история появления DDoS-атак, по мнению автора, довольно поучительна. Технология, которая легла в основу этой разновидности хакерских атак, была создана исключительно в мирных целях. Она активно использовалась для изучения пропускной способности каналов передачи данных и для проверки их поведения в условиях пиковых нагрузок. Однако вскоре эта технология и инструменты попали в руки тех, кто нашел им иное применение.

Первые случаи хакерских DDoS-атак были зарегистрированы в 1996 г. В настоящее время DDoS стал гораздо большей проблемой, чем «спам». «Спам», как нежелательные почтовые рассылки, в глобальном масштабе – всего лишь незначительные помехи на уровне 1 %. Объем же DDoS-данных, как считают специалисты, достигает 5 %, и последствия DDoS-атаки гораздо серьезнее.

В большинстве европейских стран и США приняты специальные акты, прямо и недвусмысленно определяющие хакерские атаки и ответственность за их реализацию. В Российском законодательстве эти вопросы должным образом не урегулированы. Наиболее близкие статьи УК: статья 272 «Неправомерный доступ к компьютерной информации» и статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ» с максимальными сроками наказания пять и семь лет соответственно. Однако эти статьи в случае с DDoS практически не работают. В ходе атаки неправомерного доступа не совершается, а факт использования вирусов вообще недоказуем. В дальнейшем, учитывая трансграничность этих угроз, борьба с DDoS неминуемо выйдет на глобальный уровень.

Из представленного анализа следует, что вопросы противодействия вызовам и угрозам следует рассматривать не только на национальном, но и на международном уровнях, в связи с этим в дальнейшем вопрос создания системы международной информационной безопасности.

Также следует отметить, что до сих пор в международных актах и в национальном законодательстве отсутствуют четко сформулированные понятия киберпреступности, кибербезопасности и кибертерроризма. Представляется, что объединение общих усилий международного информационного сообщества необходимо для выработки единого правового механизма регулирования противодействия использованию

информационных технологий в преступных целях. Немаловажную роль также должны сыграть «горячие линии» о противоправном содержании информации в Интернете и создание пространства доверия в целях противодействия анонимности.

Литература

1. Батурин Ю. М. Проблемы компьютерного права / Ю. М. Батурин. - М., 1991.
2. Бачило И. Л. Информационное право: основы практической информатики. Учебное пособие / И. Л. Бачило. - М., 2001.
3. Глушкова Н. Д. Информационные правоотношения. Телекоммуникации: правовые аспекты / Н. Д. Глушкова. - М., 2003.
4. Рассолов И. М. Теоретические проблемы Интернет-права / И. М. Рассолов. - М.: РПА МЮ РФ, 2002.
5. Терещенко Л. К. Правовой режим информации / Л. К. Терещенко. - М., Юриспруденция, 2007.

УДК 393

Климова Е. И., к.ю.н., доцент,
филиал РГСУ в г. Минске, Республика Беларусь,
Климов Д. А., адъюнкт, Академия МВД, Республика Беларусь

О ФУНКЦИЯХ ОПЕРАТИВНО-РОЗЫСКНОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Гарантированные Конституцией Республики Беларусь законность, правопорядок, защита личности, общества и государства от противоправных посягательств обеспечиваются полнотой содержания, обоснованностью направленности и эффективностью реализации уголовного и уголовно-процессуального законодательства. Система принципов и задач уголовного закона предполагает неотвратимость ответственности, личную виновную ответственность и справедливость наказания. Статья 26 Конституции Республики Беларусь провозглашает, что никто не может быть признан виновным в совершении преступления, если его вина не будет в предусмотренном законом порядке доказана вступившим в законную силу приговором суда. Предусмотренный порядок – это производство по материалам, включающее получение, проверку и разрешение заявлений (сообщений) о преступлении, и уголовному делу. Он установлен Уголовно-процессуальным кодексом Республики Беларусь (далее УПК), является единым и обязательным для всех участников уголовного процесса и иных лиц.

Основополагающие функции уголовного закона – охранительная, предупредительная и воспитательного воздействия – дополняются и