Секция «Государственная политика и государственное управление: проблемы и практики»

Сравнение политики правового противодействия кибертерроризму в современной России и странах Запада

Научный руководитель – Аветисян Карен Рафаэлович

Смольянинов Владислав Александрович
Студент (специалист)
Московский университет Министерства внутренних дел Российской Федерации, Факультет подготовки специалистов в области информационной безопасности, Москва, Россия
E-mail: vlad48088@gmail.com

Сравнение политики правового противодействия кибертерроризму в современной России и странах Запада

Смольянинов Владислав Александрович
Курсант
Московский университет МВД России имени В.Я.Кикотя,
Фокультет подготовки специалистов в области информационной безопасности, Москва, Россия
E-mail: vlad48088@gmail.com

Политика противодействия кибертерроризму: зарубежный и отечественный опыт Цифровая эволюция поспособствовала рождению новой транснациональной угрозы - кибертерроризма. Так как оснащение общества компьютерными сетями и информационными технологиями происходит быстро, то велика вероятность использования их злоумышленниками. В научной и юридической литературе понятие кибертерроризма трактуется вариативно. Одним из первых ввёл это понятие в 1997 г. М. Поллитт, говоривший о политизированных насильственных атаках информационно-компьютерных данных субнациональными группами[1].

Д. Деннинг определил кибертерроризм как противоправную атаку компьютеров для принуждения власти к содействию[2]; В.А. Васенин - как совокупность деструктивных политико-социально-экономически мотивированных противоправных деяний; Л.В. Смирнов - информационную атаку электронных данных критических и частных сегментов, с признаками и целями «классического» терроризма[3]; А.В. Федоров - информационно-манипуляционный компонент более масштабного теракта[4].

Неправомерное использование данных представляет повышенную опасность. Электронные медиа, потеснившие традиционные СМИ, прополитизируют, исходя из их детерминантов: анонимности, доступности, оперативности. Податливость контентному воздействию коррелирует с возрастным фактором и отсутствием у поляризованного населения аналитического мышления и доверия институту власти.

Позиции Европы и США отлична от российской, они базируются на разработке мер информационной безопасности применительно к террористическим и криминальным угрозам. Европа сконцентрировала свою деятельность на разработке конвенции по борьбе с киберпреступностью, а Соединенные Штаты, пусть и стараются уделять внимание всем аспектам ведения борьбы с кибертерроризмом, но, практически, не стремятся к достижению международных договоренностей по этому вопросу.

Не найдя поддержки своей позиции на мировом политическом пространстве, Российская Федерация перенесла центр своей активности на региональный уровень.

На сегодняшний день в Российской Федерации нормативным документом, определяющим наиболее полные подходы к обеспечению кибербезопасности, является Концепция стратегии кибербезопасности Российской Федерации[5]. В документе представлено определение киберпространства, в котором оно обозначается как сфера деятельности в информационном пространстве, произошедшая от совокупности коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование. Определение кибербезопасности, в свою очередь, состоит из совокупности условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

В 2013 году Президент РФ Владимир Владимирович Путин поручил Указом от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[6] ФСБ РФ разработку и внедрение государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на всевозможные технические устройства РФ.

В структуре МВД также существует структура, занимающаяся противодействием преступлениям в сфере компьютерной информации. Так, одними из основных направлений работы МВД России является:

1) Выявление и пресечение фактов противоправного доступа к компьютерной информации.

2) Ведение борьбы с изготовлением, распространением и использованием вредоносных программ для ЭВМ.

3) Противодействие действиям преступников с использованием возможностей электронных платежных систем.

4) Пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет.

5) Выявление, пресечение и устранение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи.

6) Противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

7) Противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

8) Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

9) Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий.

Обеспечение безопасности от кибертеррористической угрозы становится одной из самых приоритетных для национальной безопасности нашей страны. Основой обеспечения борьбы с киберпреступностью является осуществление эффективной системы взаимосвязанных мер по выявлению, предупреждению и пресечению таких действий. Российская Федерация реализует политику противодействия кибертерроризму в рамках реализации основных принципов построения информационного общества. Это обусловлено необходимостью создания общенациональных систем безопасности информационнокоммуникационной инфраструктуры, обеспечивающих ее защиту от возможных угроз.

В Российской Федерации можно выделить конкретные проблемы противодействия и выявления кибертерроризма:

1.Отсутствие соответствующих законодательных актов, которые будут отражать современное состояние дел в сфере защиты компьютерной информации и регулировать отношения в сети Интернет.

2.Неимение обязательных технических средств у следственных и оперативных органов, из-за которого не оказывается своевременное запечатление фактов совершения актов кибертерроризма.

3.Недостаточное количество специально подготовленных кадров, которые специализируются на выявлении и раскрытии компьютерных преступлений, а также специализированных подразделений ПО.

4.Система защиты интернет-сервисов не успевает совершенствоваться вслед за все более совершенными способами и методами совершения актов кибертерроризма.

С другой стороны, правительства большинства зарубежных стран предпринимают меры для предотвращения роста и минимализации актов кибертерроризма.

Так, в Великобритании был принят закон о терроризме, который призван ужесточить борьбу с различными группировками, использующими территорию Соединенного Королевства в своих корыстных целях. В нём говорится, что «в случае взлома хакерами компьютерной системы, обеспечивающей национальную безопасность страны, а также попыток с их стороны каким-либо образом оказать воздействие на государственные структуры или угрожать обществу, они могут быть обвинены в терроризме со всеми вытекающими последствиями».

Одним из подтверждений важности рассматриваемой проблемы и решительности государства в борьбе кибертерроризмом служит вступление в действие в Великобритании Закона о терроризме 2000 года. В данном законе определение терроризма впервые за все время расширяется и затрагивает область киберпространства. Английские правоохранительные органы теперь могут считать террористическими те действия, которые "серьезно вмешиваются или серьезно нарушают работу какой-либо электронной системы" и принимать к компьютерным преступникам, изобличенным в таких действиях, меры государственного принуждения.

Примерно в тоже время в США После ужасных событий 11 сентября 2001 года был утвержден закон «Об объединении и укреплении Америки путем задействования полномочий и инструментов, необходимых для борьбы с терроризмом», в соответствии с которым любое действие, ведущее к нарушению работы персонального компьютера и противоправного проникновения в компьютер классифицируется как терроризм, а провайдер обязуется по требованию ФБР предоставить всю известную ему информацию об интересующем их пользователе

Соединённые Штаты Америки предусматривают санкции за киберпреступления, учитывающие денежные штрафы и тюремное заключение. Наказание за киберпреступления зависит от многих факторов: тяжести совершенного преступления, размера экономического ущерба, который был причинен данным деянием, криминального прошлого подсудимого и многих других.

Вывод.

Исходя из положений второй главы, можно сделать вывод, что на кибертерроризм нельзя закрывать глаза. В Российской Федерации не уделяется соответствующего внимания данной проблеме. Сам термин легально не закреплен ни в одном нормативно-правовом акте. А уголовная ответственность, наступающая за совершение террористического акта предусмотрена ст. 205 УК РФ, при этом квалифицированного признака, связанного с осуществлением кибератак российский Уголовный кодекс не предусматривает Пользуясь зарубежным опытом, нужно составить не только структурированный план борьбы с кибертерроризмом, но и подготовить обширную правовую основу для этого. Так, первым делом, нужно дать чёткое определение кибертерроризму и выделить его в отдельную статью в Уголовном Кодексе Российской Федерации. Это поможет правильно квалифицировать состав преступления, и назначать за его совершение справедливое наказание.

Также следует вести некий контроль за деятельностью в сети Интернет, вводя цензуру на сайты и форумы, которые представляют опасность безопасности Российской Федерации и её населения, при этом цензура не должна ограничивать права и свободы человека и гражданина, а всего лишь предупреждать попадание пользователей на сайты с сомнительным содержанием.

Источники и литература

1) 1. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013 № Пр-153).
2) 2. Архипова, Т. Г. Современная российская государственность и перспективы ее модернизации / Т. Г. Архипова // Вестник РГГУ. Серия: История. Филология. Культурология. Востоковедение. – 2017. – № 8 (29).
3) 3. Бошно, С. В. Государство / С. В. Бошно // Право и современные государства. – 2013. – № 6.
4) 4. Бошно, С. В. Трудности формирования правовой культуры / С. В. Бошно // Право и современные государства. – 2016. – № 2.