УДК 343.34

ПОЛИТИЧЕСКИЙ АСПЕКТ КИБЕРПРЕСТУПЛЕНИЙ

Козячая А.В., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., доцент,
кандидат экономических наук
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *киберпреступность, внешняя политика, кибертерроризм, кибератака, хакер.*

В XXI веке информационные технологии стали неотъемлемой частью жизни каждого человека. Наравне с технологическим и информационным прогрессом в мире свою масштабность набирает киберпреступность. В данной статье рассматривается влияние действий киберпреступников на деятельность целых государств.

В современном мире под влиянием быстрого развития информационных технологий формируются «виртуальные» измерения политических пространств, которые становятся значимыми для внутренней и международной политики. К числу таких «виртуальных» измерений относится киберпространство [5, с.152].

Киберпространство - это виртуальная информационная среда. Оно имеет физическую составляющую - компьютеры, а также системы и инфраструктуру, обеспечивающие их системное взаимодействие. У него есть и когнитивная составляющая - люди, создающие и использующие информационно-коммуникационные технологии, а также принципы и система взаимодействия между ними [3, с.136].

Почти сразу же после своего возникновения киберпространство превратилось в пятое «поле битвы» различных политических и военных сил и продолжает оставаться таковым. Более того, многие битвы между разведывательными организациями разных стран, их военными структурами, а также экономические и информационные сражения, включая экономический шпионаж и финансовые диверсии, развертываются именно в киберпространстве. Это обстоятельство определяет высокую значимость процессов, протекающих в киберпространстве, для современного политического анализа, теории и практики политической науки [5, с.153].

Динамичность технического и информационного прогресса способствует появлению новых форм и методов преступных деяний, которые наносят серьезный ущерб как отдельным государствам и регионам, так и ставят под угрозу международную безопасность в целом [4].

Уголовный кодекс Российской Федерации выделяет следующие виды преступлений в сфере компьютерной информации: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Киберпространство дает возможность для трансформации традиционных видов преступлений в новые, такие как мошенничество, взлом, клевета, распространение порнографии, ложной информации, кража данных и др. сейчас приобретают совершенно иной смысл. Кроме того, в современном быстроменяющемся мире киберугрозы могут нанести существенный вред не только человеку, но и всему государству. Например, вирусная программа «Stuxnet» была использована для поражения ядерной инфраструктуры Ирана в 2010 году, что сократило производство урана на 20%, и, которая, кроме этого, поразила тысячи компьютеров и систем, управляющих автоматизированными производственными процессами по всему миру [3, с.138].

Еще одним примером модификации «классического» преступления стала «прослушка». По данным, опубликованным в ряде СМИ, Агентство национальной безопасности США установило «прослушку кабинетов представительства Евросоюза в Вашингтоне, штаб-квартиры ООН в Нью-Йорке и Совета ЕС в Брюсселе. Прослушке также подвергались 38 посольств и миссий различных стран в Нью-Йорке и Вашингтоне. Самыми громкими дипломатическими скандалами стали прослушка телефонных переговоров президента Бразилии Дилмы Русеф и канцлера Германии Ангелы Меркель, а также перехват защищенной спутниковой связи с Москвой Д. А. Медведева из Лондона во время саммита G20 в апреле 2009 г. [5, с.155-156].

Политическая система любого государства напрямую связана с информацией, ее производством и распространением. Однако не всегда данный процесс прогрессивно влияет на развитие внутренней политики государства и упрочнение положительной репутации органов государственной власти. На практике встречаются ситуации, когда информация используется против органов государственной власти, то есть специально создается диаметрально противоположное впечатление о политических событиях и процессах в государстве. Данное преднамеренное искажение информации может осуществляться как национальными преступными группировками, так и заинтересованными структурами

из других государств. Преднамеренные кибератаки на информационные системы государственных органов способствуют развитию мнения общественности о несостоятельности данных институтов власти, в связи с чем усложняется их работа, которая в зависимости от масштабов хакерской атаки может быть и парализована полностью. Так, в 2015 году Украина подверглась кибератаке на свою национальную электросеть, в результате чего свыше 600000 жителей остались без электричества [1].

Подобные кибератаки можно назвать кибертерроризмом. Эксперты рассматривают кибертерроризм как преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта [1].

Одним из наиболее масштабных по своим последствиям конфликтов такого рода стало обвинение со стороны руководства Демократической партии США «русских хакеров» во взломе ее информационных ресурсов и вмешательстве в президентскую кампанию Соединенных Штатов в 2016 г. Тем самым было продекларировано заявление о воздействии России на внутриполитическую ситуацию в США и растиражирована версия о поддержке Россией Д. Трампа, что якобы стало основным фактором его избрания президентом. Несмотря на отсутствие серьезных доказательств вмешательства России в американские дела и надуманность самих обвинений во «вмешательстве», эти нападки, связанные с атаками в киберпространстве, стали одним из важнейших факторов как многочисленных внутриполитических конфликтов в США, так и резкого обострения российско-американских отношений. Таким образом, один этот факт говорит об огромном и всевозрастающем влиянии процессов в киберпространстве на внутреннюю и мировую политику, а также о растущем значении кибербезопасности в современных условиях [5, с.154-155].

Кибертерроризм ориентируется на использование различных форм и методов вывода из строя информационной инфраструктуры государства. Одна из таких форм - разработка и использование компьютерных вирусов. При этом основным способом кражи паролей и ведущим инструментом в области промышленного шпионажа является внедрение вирусов-троянов. Ярким примером проявления кибертерроризма является операция кибершпионажа «Красный октябрь», в ходе которой против дипломатических ведомств, государственных структур и научно-исследовательских организаций разных стран мира соби-

ралась информация с мобильных устройств, компьютеров и сетевого оборудования атакованных организаций. Атаке при этом подверглись правительственные структуры, дипломатические ведомства, исследовательские институты, торговые и коммерческие структуры, нефтяные и газовые компании, аэрокосмическая отрасль [1].

Таким образом, нельзя не обратить внимание на политический аспект киберугроз, где киберпреступники или целые группировки хакеров, кракеров и других злоумышленников могут подорвать авторитет государства, уничтожить целую инфраструктуру любого региона мира, а также обратить свои кибервоенные действия в настоящую войну.

На современном этапе нормы международного, в частности российского, права в этой области все еще требуют доработок и усовершенствования. Эксперты и специалисты предлагают способы предотвращения киберугроз и кибератак посредством отказа от цифрового пространства вообще, перехода каждого государства на киберпространство в своей стране, а также создания международных организаций, которые регулировали бы вопрос о киберпреступности на международном уровне.

Библиографический список:

1. Аккаева, Х. А. Международный кибертерроризм как политический феномен / Х. А. Аккаева // Социально-политические науки. – 2018.
2. Буткевич, С. А. Экстремизм и терроризм в киберпространстве: выявление, нейтрализация и предупреждение / С. А. Буткевич // Вестник Краснодарского университета МВД России. – 2018. – № 1 (39). – С. 17-22.
3. Захаров, Т. В. Кибербезопасность и кибервойна: что должен знать каждый / Т. В. Захаров, П. Зингер, А. Фридман // Государство и право в новой информационной реальности. – 2018. – С. 135-142.
4. Канунникова, Н. Г. Современные вызовы и угрозы международной безопасности / Н. Г. Канунникова // Социально-политические науки. – 2018.
5. Кардава, Н. В. Киберпространство как новая политическая реальность: вызовы и ответы / Н. В. Кардава // История и соврменность. – 2018. - № 2. - С. 152-166.

POLITICAL ASPECT OF CYBER CRIMES

Kozyachaya A.V.

Key words: *cybercrime, foreign policy, cyber terrorism, cyber attack, hacker.*

In the 21st century, information technology has become an integral part of every person's life. Along with technological and informational progress in the world, cybercrime is gaining its scale. This article discusses the impact of the actions of cybercriminals on the activities of entire states.