Данная работа будет посвящена хактивизму.

Хактивизм - использование компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации. Зарождение политически идейных хакеров в восьмидесятых годах и их рост до наших дней значительно изменил ход ведения любой войны, фактически создав сетевые войны между хактивистами, хактвистскими группировками и крупными компаниями, политическими деятелями, другими хакерами и т.д.
На данный момент данная тема имеет особенную актуальность, ведь именно сейчас хактивистские группировки приобрели свою огромную аудиторию, своих спонсоров, обозначили общественности свои основные цели. Особенно после вступления на пост президента Соединенных Штатов Дональда Трампа, хактивисты особенно активны (так как основа, база одной из крупнейших хактивистских группировок нашего времени, "Anonymous", находится именно в США и активно действует на данной территории).
 В своем реферате я собираюсь доступно изложить историю хактивизма для любого читателя, объяснить, чем же является хактивизм, кем были его основополагатели и куда ведут его пути развития.
Сам реферат будет состоять из двух глав. В первой я опишу историю хактивизма до нашего времени, покажу виды и способы осуществления кибертеррористических актов. Во второй части я покажу хактивизм настоящего времени, крупнейшие группировки современности и их цели, а также основные кибератаки этого года. В заключении я хотел бы сделать прогноз на дальнейшие действия хактивистских группировок, а именно:
- наиболее предсказуемые цели последующих атак
- развитие дальнейших взаимоотношений между хактивистскими группировками
- возможная пропаганда/продвижение собственных интересов хактивистов в массы
ориентируясь на их противников, их сообщения в медиа и другие, более реалистичные прогнозы.

Часть первая

Первой интернет-войной считается конфликт в Косово 1998 года. Вооруженный конфликт вспыхнул между албанскими повстанцами, ополченцами и Союзной Республикой Югославией. Интернет тогда использовался всеми сторонами и в абсолютно разных интересах: хакеры использовали сети для осуждения военных действий как Югославии, так и НАТО, путем нарушения работы правительственных компьютеров и получения контроля над сайтами, индивидуумы рассказывали в Интернете истории об опасностях и ужасах войны, а политики и общественные деятели использовали всемирную паутину для того, чтобы их призывы достигли как можно более широкой аудитории. Люди всего мира обсуждали в сети спорные вопросы и обменивались текстами, изображениями и видео, которых нельзя было найти в иных средствах массовой информации. В апреле 1999 года газета *Los Angeles Times* написала, что Косовский конфликт превратил киберпространство в нематериальную военную зону, где сражение за умы и сердца ведется с помощью электронных изображений, групповых почтовых рассылок и хакерских нападений.

Уже в этом конфликте можно увидеть несколько видов использования сети интернет для проведения террористических актов. Но со временем интернет-борьба только приобретала новое, а сетевые воители - самосовершенствовались. На данный момент существует множество способов проведения кибертеррористических актов.

Термин “Кибертерроризм” был введен исследователем Института Безопасности и Разведки в Калифорнии , Барри Колином, в 1980-м году, чтобы определить терроризм в киберпространстве. Специальный агент ФБР Марк Поллитт определяет кибертерроризм как “преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов”. Политически мотивированные атаки, причиняющие серьезный вред, типа серьезных экономических затруднений или длительных остановок энергоснабжения, водоснабжения, можно также охарактеризовать как кибертерроризм. Виды кибертерроризма представлены ниже.

**Виртуальные “сидячие забастовки” и блокады.**

Виртуальная сидячая забастовка (демонстрация) или виртуальная блокада – это “виртуальное” исполнение физической забастовки или блокады, чрезмерная нагрузка сервера информацией. Цель состоит в том, чтобы привлечь внимание к действиям протестующих и причинам этих действий, с помощью нарушения нормального функционирования сети и блокирования доступа к услугам.

При сидячей забастовке в сети активисты пытаются создать настолько забитый трафик, что другие пользователи не могут данный сайт посетить. Подобная атака может быть проведена за счет большого количества протестующих, и для нее не требуется взлом сайта или сервера, поэтому этот способ является гражданским, нежели хактивистским. Первый протест такого рода был осуществлен 21 декабря 1995 года, группой, называющей себя “Strano Network”. Она протестовала против политики французского правительства в вопросах ядерных программ и социальной сфере. Сам акт хактивизма этой группировки заключался в том, что они в течение часа атаковали различные сайты правительственных агентств. Участники группы с разных континентов были проинструктированы следующим образом: им полагалось с помощью браузера зайти на правительственные сайты. По сообщениям, некоторые сайты действительно были выведены из строя на некоторое время.
В 1998 году группа под названием “Electronic Disturbance Theater” (EDT) сделала следующий шаг в развитии концепции электронного гражданского неповиновения. Ею был организован ряд забастовок в сети, сначала против сайта мексиканского Президента Зедильо, позже – против веб-сайта администрации Президента США Клинтона, сайтов Пентагона, Франкфуртской фондовой биржи, Мексиканской фондовой биржи.В этой забастовке, проведенной EDT 9 сентября 1998 года участвовало около 10000 человек со всех континентов, что составило 600000 попаданий в минуту на каждый сайт. Цель данных демонстраций состояла в выражении солидарности мексиканцу Сапатитасу. По словам одного из деятелей EDT, Пентагон в качестве мишени был выбран потому, что “США воспитывает солдат для последующего нарушения прав человека”. Фондовые биржи были атакованы, поскольку, по мнению EDT, они выражают роль капитализма и глобализации, использующих методы геноцида и этнических “зачисток”, но народ должен выбирать свою судьбу сам, а не принудительно, под прицелом западного государства и западного финансирования.

Для проведения подобных атак создаются специальные сайты, с которых скачивается автоматизированное программное обеспечение. Каждый участник должен посетить сайт, с которого загружается это программное обеспечение, которое запрашивает доступ к сайту-мишени каждые несколько секунд. Кроме того, это ПО позволяет протестующим производить иные операции – например, связанные с ошибками сервера.

Но когда на сервер Пентагона началась атака, одновременно было предпринято контрнаступление на браузеры пользователей, переориентировавшее их к странице с программой Applet (прикладная программа, запускаемая при каждом обращении к Web-странице, в исходный текст которой она встроена). Эта программа называлась “HostileApplet” (“Вражеская программа”). Программа загружалась в браузеры пользователей, что вызывало бесконечные требования перезагрузить документы, в результате чего перезагружались сами машины. Сайт Президента Зедильо не наносил ответного удара, но зато в качестве защиты было использовано программное обеспечение, заставившее браузеры протестующих открывать одно окно за другим, пока не “рухнет” компьютер. Франкфуртская фондовая биржа сообщила о том, что им было известно об атаке, но они полагают, что это никак не отразилось на их деятельности. По их словам, нормальная посещаемость сайта составляет 6 миллионов попаданий в день. Но несмотря на оказанное сопротивление, EDT считали свою атаку успешной.

**Бомбардировка электронной почты.**

Бомбардировка тысячами сообщений в день может привести к полной блокировке переполненного почтового ящика, делая невозможным получение электронной почты. Таким образом, бомбардировка электронной почты тоже является формой виртуальной блокады. Хотя бомбардировка электронной почты часто используется как средство мести или преследования, нередко использование этого инструмента для противодействия правительственной политике.

Первым известным нападением на почтовые ящики считается бомбардировка организацией “Тигры освобождения Тамила” электронных почтовых ящиков посольств Шри-Ланки, которые были завалены тысячами сообщений следующего содержания: “Мы Черные Тигры Интернет и мы делаем это, чтобы разрушить ваши коммуникации”. Одной из ветвей LTTE – Тамил Илам - приписывается бомбардировка электронной почты, произошедшая в 1998 году.

Эта бомбардировка состояла из приблизительно 800 писем в день в течение двух недель. Уильям Чурч, редактор центра CIWARS, отметил, что “Тигры освобождения Тамила отчаянно нуждаются в огласке, и они получили в точности то, что они хотели. Учитывая то, что террористическая деятельность этой организации заключается в кровавых терактах, этот тип деятельности гораздо более предпочтителен… CIWARS хотел бы поощрить их, от имени мира, отдавать большее предпочтение именно этому виду “террористических” действий”. Однако считается, что эта бомбардировка электронной почты была удачной, т. к. посеяла панику в посольствах.

Бомбардировке электронной почты в также подвергся в 1997 году основной поставщик Интернет – услуг в Сан-Франциско – Institute for Global Communications (IGC) за размещение на сайте *Euskal Herria Journal,* сомнительного издания Нью-Йоркской группы, поддерживающей независимость басков в Северной Испании и на Юго-западе Франции. Протестующие посчитали, что IGC “поддерживает терроризм”, поскольку на страницах сайта были материалы террористической группы “Родина и Свобода”, или ETA, ответственной за убийства более 800 человек за время тридцатилетней войны за независимость басков. Нападение против IGC началось после того, как члены ETA убили в Северной Испании популярного городского советника.

Целью протестующих была цензура. Они засыпали IGC тысячами подложных сообщений через сотни почтовых служб. В результате работа почты была парализована, и почту получить было невозможно, а линии поддержки были забиты людьми, которые не могли получить свою почту. Нападавшие также наводнили бесполезной информацией счета персонала и членов IGC, забивая их страницы поддельными заказами и номерами кредитных карт, и угрожали применить ту же тактику против организаций, пользующихся услугами IGC. Единственный способ, которым IGC мог остановить нападение – это блокировка доступа ко всем почтовым службам.

Сайт IGC закрылся 18 июля, однако перед закрытием зеркала этого сайта были размещены на нескольких сайтах на трех континентах. Крис Эллисон, представитель Кампании за свободу Интернет – английской группы, разместившей одно из зеркал сайта, сказал, что “сеть должна предоставлять возможность для обсуждения спорных идей”. Нью-Йоркский журнал настаивал на том, что его целью было “опубликование информации, часто игнорируемой международными СМИ, с целью лучшего понимания сути конфликта”. Французская газета Monde написала, что бомбардировка электронной почты IGC представляет собой “беспрецедентный конфликт”, открывший “новую эру цензуры, наложенной прямыми действиями анонимных хакеров”.

Через месяц после удаления IGC со своего сервера сайта журнала *Euskal Herria Journal* Антитеррористическое подразделение Скотланд-Ярда закрыло сайт английской Кампании за свободу Интернет, разместившей на сайте сомнительный журнал. Согласно официальному заявлению, эти действия были направлены на борьбу с терроризмом. Кампания за свободу Интернет заявила, что переместит журнал в свой Американский участок.

Случай с сайтом *Euskal Herria Journal* иллюстрирует мощь хактивистов в Интернете. Несмотря на свое желание, IGC не смог оставить сайт на своем хостинге, поскольку мог не выдержать нападения. Можно было бы проигнорировать несколько сообщений электронной почты, требующих закрыть сайт, но нельзя игнорировать бомбежку электронной почты. Случай также иллюстрирует мощь Интернет как средства свободы слова.