РЕФЕРАТ

на тему

IT-Воители - прошлое, настоящее и будущее хактивизма.

Выполнил:

Матвеев Василий Юрьевич

Руководитель:
Коняхин Александр Валерьевич

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись руководителя)

Рецензент:

Мокин Евгений Анатольевич

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись рецензента)

Москва

2016/2017 уч. г

**Оглавление**

1. Введение.
2. Часть первая. Виды кибератак.

2.1 Виртуальные “сидячие забастовки” и DDos-атаки.

2.2 Бомбардировка электронной почты

2.3 Web-хакерство и компьютерные взломы

1. Часть вторая. Мировая обстановка.

3.1 Крупнейшие мировые кибервойска

3.2 Отдельные группировки

1. Заключение.

# Введение

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, отдельными 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. Также я постараюсь ответить на вопрос: есть ли будущее у современного хактивизма и в какой сфере оно будет реализовано?
Сам реферат будет состоять из двух глав. В первой я опишу важные моменты в истории 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**

**Типы кибератак**

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 DDos-атаки**

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. По схожим принципам работают и DDos-атаки (от англ. Distributed Denial of Service — «отказ от обслуживания») - атаки на сайт с целью выведения его из строя путем подачи большого количества различных запросов. В ее результате сервера, обслуживающие данный сайт, обрабатывают данные одновременно отправленные ложные запросы, из-за чего простое пользование сайтом становится невозможным. Чаще всего жертвами DDos-атак становятся рекламные, коммерческие и информационные сайты.

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, 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, отдавая 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”.

Подобные случаи иллюстрируют 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.

**Web-хакерство и компьютерные взломы**

Этот способ является наиболее популярным даже среди неосведомленных в данной теме людей. Тема компьютерных взломов активно освещается и в интернете, и на телевидении. Правда, риск быть взломанным слишком мал для обычных пользователей интернета, но чрезвычайно велик для известных и значимых людей, сайтов крупных компаний или научных подразделений. Средства массовой информации заполнены историями о хакерах, получающих доступ к сайтам, и меняющих содержание страниц. Часто сообщения связаны с политикой – как, например, сообщение о том, что группа португальских хакеров изменила в сентябре 1998 г. содержание 40 индонезийских сайтов, разместив на них большими черными буквами слоган “Свобода Восточному Тимору”. По сообщениям *New York Time*s, хакеры также добавили ссылки на сайты, размещающие информацию о нарушении Индонезией прав человека в бывшей португальской колонии. Тогда, в августе 1999 года, Нобелевский лауреат Хосе Рамон Хорта, представляющий движение за независимость Восточного Тимора от Индонезии, предупредил о существовании плана глобальной сети хакеров на случай, если Джакарта сорвет голосование о будущем Восточного Тимора. В заявлении, сделанном *Sydney Morning Herald*, он сказал, что план готовили более 100 хакеров, в основном подростков, из разных стран.

Другой путь, которым хактивисты изменяют информацию, просматриваемую пользователями – это вмешательство в работу службы доменных имен, так, чтобы название одного сайта, приводило на IP другого. Когда пользователи направляют браузеры на один сайт, их переадресовывают к альтернативному.

Самой большой акцией подобного рода была совместная атака более трехсот сайтов антиядерными хакерами Milw0rm совместно с хакерами группы Ashtray Lumber-jacks в июле 1998 года. По сообщениям, хакеры получили незаконный доступ сайтам Британского провайдера EasySpace. Они изменили базу данных провайдера так, что все пользователи, пытавшиеся получить доступ к сайтам, попадали на сайт с лозунгом протеста против гонки вооружении: “используй свою силу для поддержания МИРА и положи конец этому ядерному абсурду”.

Еще один подобный случай был оглашен Los Angeles Times. Онисообщили, что калифорнийский студент факультета информатики, называющий себя Бронк Бастер, принадлежащий к группировке “LoU” (Legion of the Underground), со своим компаньоном Зайклоном, взломал китайскую сеть и стер управляемый государством сайт по правам человека и цензуре. По словам хакера, они обнаружили примерно 20 серверов firewall, блокирующих все от Playboy.com до Parents.com. Никакие данные не уничтожались, лишь были перемещены.

**Часть вторая**

**Мировая обстановка**

**Крупнейшие мировые кибервойска**

В 2017 году около 100 стран имеют неофициальные кибервойска. Наиболее развитыми считаются кибер-подразделения США, Китая, Великобритании, Северной Кореи и России. Помимо защиты своего государства, данные войска организуют кибершпионаж за предприятиями, властью и обстановкой в других странах, в чем зачастую оказываются замеченными.
 Примером подобного воровства информации являются атаки кибервойск Китая на различные организации, находящиеся в США. Еще в 2013 году фирма Mandiant опубликовала отчет, в котором находились данные о кибератаках на как минимум 141 американскую компанию, выполненных хактивистской группировкой, находящейся в Китае. Также в данном документе было отмечено, что воры интеллектуальной собственности могут находиться невидимыми со своего компьютера в течении года, проводя слежку над определенной компанией. По сводкам Mandiant, киберпреступники имели доступ к данным крупнейших компаний из 20 ведущих отраслей в течение нескольких лет. Хактивисты имели доступ данным через так называемую “вскрытую сеть”, выкрадывая посредством нее технические планы, сведения о технологических процессах, результаты испытаний, бизнес-планы, информацию о ценах, соглашения о партнерстве, сообщения электронной почты и списки контактов руководителей данных организаций. Лишь за 1 месяц китайские хактивисты смогли проникнуть в сети 17 компаний, 87% из которых находились в странах английского языка. Также Mandiant сообщили, что практически вся слежка за иностранными компаниями в Китае производится не его официальными кибервойсками, а отдельной группировкой APT1, спонсируемой, предположительно, китайским правительством. Масштаб инфраструктуры китайского хактвизма достаточно велик: 937 командных серверов, размещенных на 849 отчетливых IP-адресах в 13 странах. Для управления системой APT1 использовали удаленный десктоп за границей. По данным Mandiant, за всеми взломами могут стоять более ста человек.
 В стране с наибольшей киберармией в мире - около 9 тысяч человек - США - ведется активная подготовка “сетевых” войск. По словам директора Агентства национальной безопасности США, Майкла Роджерса, до конца 2018 года Пентагон планирует развернуть 133 подразделения кибервойск, 50% которых будут отвечать за безопасность военных компьютерных сетей, 20% - за проведение боевых операций, 10% будут заниматься вопросами национальных угроз и оставшиеся 20% - в качестве команд поддержки. Выполнено это будет из-за угрозы со стороны Китая и террористической группировки “Исламское Государство”. “Мы находимся в ситуации, немного непривычной для военной арены. Как только будут установлены базовые рамки, подразделения начнут свою работу по противодействию угрозам”, - отметил Роджерс на заседании Национального пресс-клуба, добавив, что в связи с ростом количества кибератак войска США приступят к работе еще до того, как будут полностью сформированы.

 В России же ситуация с кибервойсками обстоит несколько иначе. По данным источника из ФСБ РФ, ежегодно на развитие кибервооружения будет выделяться порядка 250 миллионов долларов из государственного бюджета. Подобный ход является ответом Соединенным Штатам на подготовку их киберармии. В планы России не входит развязка конфликтов в киберпространстве. В сравнении с Китаем и Соединенными Штатами, киберармия нашей страны довольно малочисленна - около 1 тысячи хакеров - поэтому нашим хакерам будет довольно сложно соперничать с чересчур сильными киберармиями соперника, находясь в атакующей стороне.

**Отдельные группировки**

На момент конца 2016 - начала 2017 года мы можем выделить одну крупнейшую хактивисткую группировку, объединяющую в себе многих хакеров со всего мира - “Anonymous”. По информации многих информационных агенств, “Anonymous” - идеология, а не просто группа людей. Активисты данной группировки борются против притеснения свобод, коррупции, за полную свободу информации и “интересы общества”, как выражаются представители “Anonymous” на своем официальном канале в YouTube. У данной группировки нет лидеров, и один не может говорить за всех, в ней все имеют равные права. Изредка в организации могут встречаться пользователи с несколько повышенными правами, но это всего лишь знак отличия технического персонала, который работает над поддержанием коммуникации. Чтобы стать частью “Anonymous” вы не должны быть программистом или работать в IT-сфере. Для этого достаточно распространять информацию, олицетворяющую идеологию данной группировки или использовать софт LOIC, созданный самими “Anonymous” для совершения DDos атак. Основное правило членов организации:

“Оставаться анонимным и защищать анонимность других”.

Сама организация существует с 2007-2008 годов. Официальной даты создания организации не существует, так как сама идея зарождалась на анонимных хакерских форумах, а учитывая практически полную анонимность группировки и отсутствие ее единого командования, точной информации о создании найти невозможно.
Первая операция группировки “Anonymous” в России получила название “Чанология” (operation “Chanology” - оригинальное название). Она была запущена в ответ на попытки церкви саентологии удалить из сети рекламное интервью с Томом Крузом в январе 2008 года. 21 января на официальном канале “Anonymous” на YouTube был выложен видеоролик под названием «Послание к саентологии». В нём действия церкви были названы интернет-цензурой, а также было высказано намерение «изгнать церковь из Интернета». Затем последовали DDos-атаки, отправка факсом листов, закрашенных чёрным цветом. Усилиями группировки были созданы сайты, критикующие церковь Саентологии и координирующие действия тех, кто решил присоединиться к операции. В феврале были организованы мирные демонстрации возле офисов церкви в Великобритании и Соединенных Штатах. Кроме того, “Anonymous” требовали, чтобы Служба внутренних доходов США пересмотрела решение об освобождении Церкви саентологии от уплаты налогов. После этой операции популярность организации возросла в разы. За “Чанологией” последовали крупные операции “Расплата” (оригинальное название - “Payback”), защита сайта “WikiLeaks”, атаки на правительство Египта, сайт Ватикана и сайт Европарламента, операция “Россия” (кодовое название - “OpYoungBustards”) и объявление войны террористической организации “ИГИЛ” в 2015 году.

В 2017 году активисты “Anonymous” активно боролись с кандидатом, а теперь уже президентом Соединенных Штатов Америки Дональдом Трампом. Свою борьбу они не называли войной, как это сделали европейские СМИ, но записали официальное обращение к президенту США:
“Дорогой Дональд Трамп, мы наблюдали за вами на протяжении долгого времени, и то, что мы видим, невероятно раздражает. Ваша непоследовательная и полная ненависти кампания шокировала не только Соединенные Штаты, но и всю планету вашими ужасающими действиями и идеями. Вы говорите то, что ваша аудитория хочет слышать, но в реальном мире вы не боретесь ни за что, кроме вашей собственной жадности и силы.”

По словам источника thenextweb.com, действия хактивистов “Anonymous” не увенчались успехом. Дональд Трамп был избран президентом США, а проделанные группировкой DDos-атаки оказались бесполезны. “На данный момент мы имеем этакую лайт-версию “Anonymous”, в которой группа детей пишет скрипты, проводит координированные DDos-атаки и кричит миру о том, что вносит огромный вклад в политику. Это говорит вовсе не о том, что группировка возмужала, а наоборот, сделала несколько шагов назад.

Мы все должны ждать большего.
Я скучаю по старым “Anonymous”, - Брайан Кларк, американский журналист.

Еще одна крупная атака была проведена киберальянсом украинских хактивистов - группировок FalconsFlame, RUH8, Trinity и CyberHunta. Она получила название #op256thDay, так как была проведена в День программиста, 13 сентября, в 256 день года. Целью хакеров стала информация, расположенная на ресурсах ДНР, ЛНР и России, нацеленных на обеспечение СМИ материалами для ведения информационной войны с Украиной. Часть ресурсов была полностью уничтожена, а часть скопирована на компьютеры самих хакеров и удалена с серверов атакованных ресурсов. Общее количество ресурсов, потерявших информацию в результате данной операции - 33. Также на многие из данных сайтов хактивисты внедрили видеоряд, демонстрирующий виды вооружения РФ на Донбассе.
Визитной карточкой данного альянса стали видеообращения одного из хактивистов из Львовского метро. Имея субтитры на многих языках, данный видеоматериал заимел высокую популярность в сети, благодаря чему впоследствии один из хакеров попал на телевидение, где дал интервью одному из украинских новостных каналов.

**Заключение**

 На данный момент в мире существует определенное соотношение хактивистских сил. Большая часть хактивистов работает в национальных кибервойсках стран, некоторые занимаются частной защитой компаний или программного обеспечения, еще часть - работает на хактивистские группировки наподобие “Anonymous”. В меньшинстве оказываются одиночки, которые могут появляться на отдельных операциях, но не являются участниками каких-либо союзов или объединений.
 Из-за неудачных операций, проведенных “Anonymous” против Дональда Трампа, крупнейшая хактивистская организация была обсмеяна внутри и вне сети. Исходя из этого, можно предположить, что в ближайшее время попыток изменить что-либо во внутренней или внешней политике крупных стран Европы не предвидится. Но организации на Украине скорее всего продолжат свою деятельность: КиберБеркут будет устраивать взлом правительственных сайтов парламента Украины, а ее национальные организации - оказывать защиту от этих атак и заниматься слежкой за правительством и правительственными сайтами России.
 Таким образом, можно быть практически полностью уверенными в том, что отдельные группировки не смогут вносить значимый вклад в мировую политику в ближайшие годы. Из-за усилений крупнейших киберармий мира собирать информацию и устраивать взлом внутри государства будет крайне сложно. Основная сила будет скоординирована вокруг сетевых армий различных стран, поэтому сильные хакеры будут завербованы туда. Возможно, что настанет время, неблагоприятное для отдельных хактивистов и хактивистских союзов, даже для таких сильных и многочисленных, как “Anonymous”. Но будущее у хактивизма однозначно есть. Хактивисты в будущем станут полноценной боевой единицей. Сеть уже на данный момент является отдельным полем битвы, а, значит, в будущем данная отрасль будет только прогрессировать. Уменьшение количества хакеров-одиночек поможет усилить отдельные группировки, а также киберармии стран, поэтому кибербойцы в ближайшее время будут максимально востребованы.

**Список литературы**

1. Anonymous Documentary - How Anonymous Hackers Changed the World Full Documentary
2. Anonymous - The Hacker Wars Full Documentary
3. Anonymous Documentary - The Story of the Anonymous Hacktivists Full Documentary
4. Anonymous - Behind The Mask Documentary

# Anonymous’ #OpTrump isn’t a ‘war,’ it’s a nail in the coffin of the encryption debate - thenextweb.com article

## We Are Legion: The Story of the Hacktivists - Brian Knappenberg’s movie

1. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy by Dorothy E. Denning